# THE PHILIPPINES SECOND NATIONAL RISK ASSESSMENT ON MONEY LAUNDERING AND TERRORIST FINANCING



The National Money Laundering and Terrorist Financing (ML/TF) Risk Assessment of Philippines has been conducted as a self-assessment by Philippine Authorities, using the National ML/TF Risk Assessment Tool that has been developed and provided by the World Bank. The data, statistics, and information provided and populated into National ML/TF Risk Assessment Tool templates, and any other finding, interpretation, and judgment under the scope of National Risk Assessment process completely belong to the Philippine authorities and do not reflect the views of World Bank, its Board of Executive Directors or the governments they represent. Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

# **Table of Contents**

IN	TRODUCTION	5
OI	BJECTIVES	5
NF	RA PROCESS	6
	RA WORKING GROUP	_
	RA RESEARCH AND ASSESSMENT METHODOLOGY	
LII	MITATIONS OF THE ASSESSMENT	.12
I.	OVERALL THREAT ASSESSMENT	
	THREAT ARISING FROM PREDICATE CRIMES	
	I. Tax Crimes	
	II. Smuggling	
	III. Copyright Infringement/Intellectual Property Law Violations	
	IV. Illegal Manufacture and Possession of Firearms, Ammunitions and Explosives	
	V. Environmental Crimes	
	VI. Investment Fraud and Estafa	
	VII. Violation of the Dangerous Drugs Law	
	VIII. Plunder and Violations of the Anti-Graft and Corrupt Practices Act	
	IX. Web-related Crimes	
	X. Trafficking in Persons	
	XI. Kidnapping for Ransom	
	XII. Other Unlawful Activities/ Predicate Offenses	
	1. Banks	_
	2. Money Service Businesses (MSB)	
	Designated Non-Financial Businesses and Professions (DNFBPS)	
	4. Non-Profit Organization (NPO)	
	5. Securities Sector	
	6. Insurance Sector	
	THE LEVEL OF EXTERNAL THREAT	
	OVERALL NATIONAL RISK	
	ACTION PLAN	_
	ACTION FLAN	. 51
II.	NATIONAL VULNERABILITY	. 54
	EXECUTIVE SUMMARY	
	INTRODUCTION	
	DATA AND INFORMATION COLLECTION	
	AML COMBATING CONTROLS ASSESSMENT	_
	OVERALL NATIONAL VULNERABILITY	
	ACTION PLAN	
	DANIZING SECTOR VIII NEDADILITY	101
111	. BANKING SECTOR VULNERABILITY	
	INTRODUCTION	-
	DATA AND INFORMATION COLLECTION	
	SECTOR VULNERABILITY ASSESSMENT	
		103 129
	DV-11V/IN 1 EDIN	7

IV.	SECURITIES SECTOR VULNERABILITY	131
	EXECUTIVE SUMMARY	131
	INTRODUCTION	131
	DATA AND INFORMATION COLLECTION	132
	SECTOR VULNERABILITY ASSESSMENT	
	ACTION PLAN	152
٧.	INSURANCE SECTOR VULNERABILITY	154
	INTRODUCTION	154
	DATA AND INFORMATION COLLECTION	159
	SECTOR VULNERABILITY ASSESSMENT	161
	ACTION PLAN	172
VI.	OTHER FINANCIAL INSTITUTIONS	173
	EXECUTIVE SUMMARY	173
	INTRODUCTION	173
	SECTOR VULNERABILITY ASSESSMENT	174
	A. THE NON-STOCK SAVINGS AND LOANS ASSOCIATIONS (NSSLAS)	175
	B. MONEY SERVICE BUSINESSES (MSBS)	180
	C. PAWNSHOPS (WITH COROLLARY BUSINESSES)	182
	D. LENDING AND FINANCING COMPANIES	190
	E. NON-BANK E-MONEY ISSUERS	197
	ACTION PLAN	204
VII.	. DESIGNATED NON-FINANCIAL BUSINESS AND PROFESSIONS	206
	EXECUTIVE SUMMARY	206
	DATA AND INFORMATION COLLECTION	208
	A. CASINO SECTOR	210
	INTRODUCTION 210	
	SECTOR VULNERABILITY ASSESSMENT	214
	ACTION PLAN	227
	B. LAWYERS AND NOTARIES	228
	INTRODUCTION	228
	SECTOR VULNERABILITY ASSESSMENT	229
	ACTION PLAN	236
	C. ACCOUNTANTS	236
	INTRODUCTION	236
	SECTOR VULNERABILITY ASSESSMENT	
	ACTION PLAN	244
	D. DEALERS IN PRECIOUS METALS AND STONES	245
	INTRODUCTION	245
	SECTOR VULNERABILITY ASSESSMENT	
	ACTION PLAN	
	E. COMPANY SERVICE PROVIDERS	
	INTRODUCTION	
	ACTION PLAN	
	F. CAR DEALERS	
	INTRODUCTION	
	SECTOR VULNERABILITY ASSESSMENT	
	ACTION PLAN	
	G. REAL ESTATE AGENTS (BROKERS)	

INTRODUCTION	262
SECTOR VULNERABILITY ASSESSMENT	263
ACTION PLAN	267
VIII.FINANCIAL INCLUSION PRODUCTS	268
EXECUTIVE SUMMARY	268
INTRODUCTION	269
FINANCIAL INCLUSION PRODUCTS	272
A. MICROFINANCE LOANS	272
B. MICRO-DEPOSITS	274
C. MICRO-INSURANCE	275
D. PAWNING AND REMITTANCE SERVICES OF PAWNSHOPS	277
E. E-MONEY	279
ACTION PLAN	281
IX. TERRORISM AND TERRORIST FINANCING THREAT ASSESSMENT	282
EXECUTIVE SUMMARY	
DATA AND INFORMATION COLLECTION	282
TERRORISM THREAT	285
TERRORIST FINANCING THREAT	289
TERRORIST FINANCING INVESTIGATION	
CONCLUSION	301
ACTION PLAN	301

#### **INTRODUCTION**

The National Risk Assessment (NRA) on Money Laundering (ML) and Terrorist Financing (TF) is a government-wide assessment of the overall exposure of the country to money laundering and its related predicate offenses, terrorism and terrorist financing. It is a comprehensive process of identifying and analyzing the ML/TF risks within the realm of the supervised sectors, financial institutions, and covered persons and entities under the AMLA, as amended.

Recommendation 1 of the Financial Action Task Force (FATF) Forty Recommendations requires countries to identify, assess and understand the ML/TF risks, and take actions in mitigating the risks effectively. Further, the country should apply a risk-based approach (RBA) to ensure that the mechanisms and measures to prevent ML/TF risks are commensurate to the risks and context identified.

In 2016, the Philippines concluded its First (1<sup>st</sup>) NRA covering the period 2011 - 2014. The identified ML threats are predominantly from the proceeds-generating predicate offenses such as drug trafficking, investment scam, corruption, among others. The banks, securities, remittance agencies and foreign exchange dealers are the main sectors used by criminals to channel the illegal proceeds. Recognizing this threat, the banking, securities and remittance agencies/foreign exchange dealers have imposed stricter measures and enhanced coordination with covered persons under the supervision of BSP and SEC.

The Philippines, in its effort to further strengthen its anti-money laundering and combating the financing of terrorism (AML/CFT) regime, conducted its Second (2<sup>nd</sup>) National Risk Assessment. The Anti-Money Laundering Council (AMLC), the Philippines' Financial Intelligence Unit (FIU), as the lead agency, and stakeholders from the government agencies, law enforcement agencies and private sector institutions, actively participated in this NRA.

This Report details the updated results of the process of threats, terrorism financing risk assessment and sectoral vulnerability assessments, conducted on the basis of a self-assessment by the Philippine authorities, using the National Money Laundering and Terrorist Financing Risk Assessment (NRA) Tool developed and provided by the World Bank. The Second NRA covers the period 2015-2016.

#### **OBJECTIVES**

The objectives of the Second NRA are as follows:

- a) Assess and understand the level of proceeds of crime generated in or coming into the country and the threat posed by money laundering (ML) and terrorist financing (TF);
- b) Determine the vulnerability of financial institutions and designated non-financial businesses and professions ('DNFBPs') and their products to ML and TF;
- Appreciate the most efficient way to allocate resources for the detection, prevention, investigation and prosecution of ML and its predicate crimes, and TF.
- d) Determine potential improvements to the AML/CFT regime, if necessary, spearhead the formulation or calibration of AML/CFT policies
- e) Provide information to the stakeholders and to public in order to enhance their general understanding of the AML/CFT initiatives

#### **NRA PROCESS**

The NRA process involved three stages. The first stage included several briefings and coordination meetings with law enforcement agencies, supervising agencies, government agencies, stakeholders and covered persons from February 2017 to April 2017, discussing NRA concepts, NRA tools and the assessment methodology. This was followed by NRA working group (NRAWG) meetings and data gathering discussions. Each of the working groups used the collected information/data obtained from these sectors, and populated their respective NRA tools.

The second stage required the NRA working groups to assess and analyze the collected information/data from their member-groups and institutions, re-evaluate the preliminary inputs, results and validate the AML control ratings parallel across various working groups. On 31 July - 1 August 2017, the NRA-WGs conducted a consolidation workshop to address the inconsistencies in the AML control variables assessment and identify the gaps and deficiencies present among the different sectors, such as the identification of beneficial ownership and identification infrastructure wherein the general sources of information are common across sectors.

The final stage of the NRA process included a two-day workshop held on 24-25 August 2017, which served as a venue for the final review of the NRA findings and the presentation of proposed action plan to the stakeholders.

# NATIONAL RISK ASSESSMENT WORKING GROUP (NRAWG)

National Risk Assessment Working Groups (NRAWGs) were represented by all relevant AML/CFT stakeholders from the following institutions.

Supervising Agencies	Law Enforcement Agencies and Government Agencies		
Anti-Money Laundering Council	Anti-Terrorism Council		
Bangko Sentral ng Pilipinas	Bureau of Immigration		
Insurance Commission	Bureau of Internal Revenue		
Securities and Exchange Commission	Cooperative Development Authority		
Private Stakeholders	Department of Finance		
Association of Bank Compliance Officers of the Philippines	Department of Foreign Affairs		
Association of Bank Remittance Officers, Inc.	Department of Justice		
Bankers Association of the Philippines	Department of Social Welfare and Development		
Caucus of Development NGO Networks	Department of Trade and Industry		
Cebuana Lhuillier Pawnshop	Integrated Bar of the Philippines		
Chamber of Thrift Banks	Intellectual Property Office of the Philippines		
Globe G-Cash - Globe Telecommunications	Intelligence Service Armed Forces of the Philippines		
Philippine Association of Stock Transfer Agents	Inter-Agency Council Against Trafficking		

Philippine Chamber of Mutual Benefit Associations, Inc.	National Bureau of Investigation
Philippine Insurers and Reinsurers Association, Inc.	National Intelligence Coordinating Agency
Philippine Life Insurance Association, Inc.	Office of the Ombudsman
Philippine Stock Exchange	Office of the Solicitor General
Rural Bankers Association of the Philippines	Philippine Amusement and Gaming Corporation
Smart Padala - Smart Communications	Philippine Center on Transnational Crime
Trust Officers Association of the Philippines	Philippine Deposit Insurance Corporation
	Philippine Drug Enforcement Agency
	Philippine Institute of Certified Public Accountants
	Philippine National Police – Anti-Cybercrime Group
	Philippine National Police – Anti-Kidnapping Group
	Philippine National Police – Criminal Investigation and Detection Group
	Presidential Anti-Organized Crime Commission
	Professional Regulation Commission – Board of Accountancy
	Professional Regulation Commission – Board of Real Estate Service

#### NRA RESEARCH AND ASSESSMENT METHODOLOGY

National ML vulnerability is determined by the overall sectoral money laundering (OSML) vulnerability and the national ML combating ability. In the 1<sup>st</sup> NRA, the World Bank sectoral assessment tools (WB tools) used by the NRAWGs assess the availability and presence of sectoral AML general control factors that affect the level of money laundering/terrorism financing (ML/TF) threat to the country. The WB model calculates the risk based on the identified threats and the estimated vulnerability of the selected sectors to ML/TF. The level and impact of threat for the predicate offenses, terrorism and terrorism financing, are assessed by typology analysis, sectoral threat and vulnerability to the predicate offenses and TF. The WB tool uses a combination of Bayesian network¹ and weighted average to determine the degree of dependence or correlation among the variables. For some sectors, such as the Other Financial Institutions (OFIs), Designated Non-Financial Businesses and Professions (DNFBPs) and Financial Inclusion, the AML/CFT assessment was conducted based primarily on the availability of AML enforcement mechanisms, including AML compliance, and on the products or services vulnerability of their respective WB tools. The AML controls are assessed by estimating the extent to which the AML regulations, laws, and AML process address the gaps and conform with the international standards. The AML controls used in the National Vulnerability are distinct from controls

<sup>-</sup>

<sup>&</sup>lt;sup>1</sup> Bayesian network (BN) is a type of *Probabilistic Graphical Model* used to build models from data and/or expert opinion. It is a form of conditional dependencies which can be estimated using statistical and computational methods. It combines the principles of graph theory, probability theory, computer science, and statistics.

evaluated by the other sectors, as such assess the overall sectoral impact and the country's responsiveness to ML/TF.

For the 2<sup>nd</sup> NRA process, the NRAWGs use the modified WB modules/tools (2015 WB tools). The 2015 WB tools assess the overall threat and effectiveness of the AML/CFT mechanisms in place. The 2015 WB tools also intend to identify the gaps within the existing AML systems of the sectors under assessment. The new WB tool uses two (2) approaches in assessing the impact of a certain sector to the overall sectoral money laundering (OSML) vulnerability. The new module also assesses the ability of the sectors to address cross-border threats. Under the new module, OFIs and DNFBPs sectors are now required to use the new WB tools to assess specific AML controls similar to that of the banking, securities and insurance sectors. On the other hand, the National Vulnerability NRAWG assesses the availability, quality, and the effectiveness of overall AML controls. The threat assessment and TF risk and vulnerability assessment shall employ the same design of modules used in the 1<sup>st</sup> NRA. Presented hereunder is summary of key assessment variables used in the 1<sup>st</sup> and 2<sup>nd</sup> NRA.

A. For the assessment of the vulnerability of the sectors, the following variables were used:

1 <sup>st</sup> NRA (2011-2014)	2 <sup>nd</sup> NRA (2015-2016)		
Banks, Securities, Insurance	Banks, Securities, Insurance, Other Financial		
* OFIs and DNFBPs were assessed only as	Institutions, DNFBPs		
to their products and not on their			
AML/CFT systems			
AML Laws and Regulations (preventive	Comprehensiveness of AML Legal Framework		
measures and supervision)			
Quality of AML Supervision	Effectiveness of Supervision Procedures and		
	Practices		
Market Pressure to Meet AML Standards	Level of Market Pressure to Meet AML Standards		
	(optional) <sup>2</sup>		
Commitment to Good Corporate	Availability and Effectiveness of Entry Controls		
Governance			
Penalties	Availability and Enforcement of Administrative		
	Sanctions		
Enforcement of AML Obligation	Availability and Enforcement of Criminal Sanctions		
Firm Staff Integrity	Integrity of Firms' Staff		
Firm Staff Knowledge	AML Knowledge of Firms' Staf		
Compliance Function	Effectiveness of Compliance Function		
	(Organization)		
Firms' AML Monitoring, Data Collection	Effectiveness of Suspicious Activity Monitoring		
and Record Keeping Systems	and Reporting		
Identification Infrastructure	Availability of Reliable Identification Infrastructure		
Availability of Independent Information	Availability of Independent Information Sources		
Sources			
Corporate and Trust Transparency	Availability and Access to Beneficial Ownership		
	Information		

<sup>&</sup>lt;sup>2</sup> Level of market pressure is an optional variable in the NRA assessment. The level of market pressure assesses how market forces exert pressure on management of the sector in order to have an effective AML compliance function. It addresses the pressures that exist outside of a country's legal and supervisory regimes; for instance, commercial pressure that is applied by commercial counterparts such as correspondent banks.

The 2<sup>nd</sup> NRA exercise further identifies the crosscutting risks hence, the inclusion of detailed assessment of the OFIs and DNFBPs.

B. For the assessment on national vulnerability, the following variables were used:

1 <sup>st</sup> NRA (2011-2014)	2 <sup>nd</sup> NRA (2015-2016)		
National Vulnerability	National Vulnerability		
Policy and Implementation	Quality of AML Policy and Strategy		
Criminalization of Money Laundering	Effectiveness of ML Crime Definition		
STR Data Analysis	Quality of FIU Intelligence Gathering and		
	Processing		
Capacity of Financial Crime Investigators	Capacity and Resources for Financial Crime		
	Investigations [including Asset Forfeiture (AF)]		
Integrity and Independence of Financial	Integrity and Independence of Financial Crime		
Crime Investigators	Investigators (incl. AF)		
International Cooperation in Criminal	Effectiveness of International Cooperation		
Matters			
Integrity and Independence of Financial	Integrity and Independence of Financial Crime		
Crime Prosecutors	Prosecutors (incl. AF)		
Capacity of Financial Crime Prosecutors	Capacity and Resources for Financial Crime		
	Prosecutions (incl. AF)		
Domestic Cooperation	Effectiveness of Domestic Cooperation		
Integrity and Independence of Presiding	Integrity and Independence of Judges (incl. AF)		
Officers			
Capacity of Presiding Officers	Capacity and Resources for Judicial Processes		
	(incl. AF)		
Asset Forfeiture Laws	Comprehensiveness of Asset Forfeiture Laws		
Capacity of Asset Forfeiture Investigators	Quality of Border Controls		
Integrity and Independence of Asset	Comprehensiveness of Customs Regime on Cash		
Forfeiture Investigators	and Similar Instruments		
Asset Forfeiture Orders	Effectiveness of Customs Controls on Cash and		
	Similar Instruments		
Auditing and Accounting Standards and	Availability of Independent Audit		
Practices			
Identification Infrastructure	Availability of Reliable Identification		
	Infrastructure		
Availability of Independent Information	Availability of Independent Information Sources		
Sources			
Corporate and Trust Transparency	Availability and Access to Beneficial Ownership		
T. 0: 1	Information		
Tax Disclosure	Effectiveness of Tax Enforcement		
Financial Integrity	Level of Financial Integrity		
Formalization of Economy	Level of formalization of the Economy		
Criminal Penalties			
International Cooperation in Asset			
Forfeiture			

In the 2015 World Bank model, the Sectoral ML Risk uses a correlation matrix combination of the ML threat and vulnerability of the sector under assessment. The overall ML risk is determined as a function of the overall ML risk and weighted sectoral vulnerability. The national ML risk consists of eight (8)

modules on vulnerability, including terrorism financing threat and vulnerability assessment, and one (1) module on threat risk assessment. Below is structure of the NRA tool.

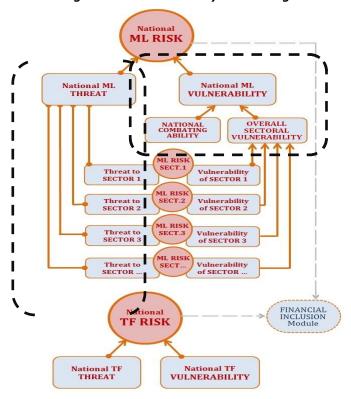


Figure 1. National Money Laundering Risk

The two major components of the assessment are the national ML threat and national ML vulnerability. The *national ML threat*<sup>3</sup> module focuses on understanding the proceeds of crimes in the country. This module also analyzes the generation, flows, and patterns of proceeds of crimes from different sector perspectives.

The national ML vulnerability<sup>4</sup> module assesses the defense mechanisms available for combating money laundering and terrorist financing. The national ML vulnerability module also takes into account the vulnerabilities of the various sectors that could be potentially abused or exploited for money laundering and terrorist financing. The national ML vulnerability is estimated as a function of the national ability to combat ML/TF and the overall ML sectoral vulnerability. The overall ML sectoral vulnerability comprises the ML vulnerability ratings of the sectors - banking, insurance, and securities, businesses and professions under the Designated Non-Financial Businesses and Professions (DNFBPs) category and the other financial institutions as assessed by the NRAWGs.

Several AML controls - or *input variables*, are evaluated as main drivers of the national ML combating ability. The input variables or AML controls, when aggregated, determine the ratings for the broader and high-level AML intermediate variables, as presented in the chart below.

<sup>&</sup>lt;sup>3</sup> "Threats" refer to the scale and characteristics of the proceeds of criminal activities or financing of terrorism in the jurisdiction

<sup>&</sup>lt;sup>4</sup> "Vulnerabilities" refer to weaknesses or gaps in a jurisdiction's defenses against ML and TF (World Bank Group, Finance & Markets. "Introduction to the National Assessment Tool." June 2015)

The overall vulnerability of the sectors under WG assessment and the deficiencies in national combating ability constitute the overall *National Money Laundering* Vulnerability score.

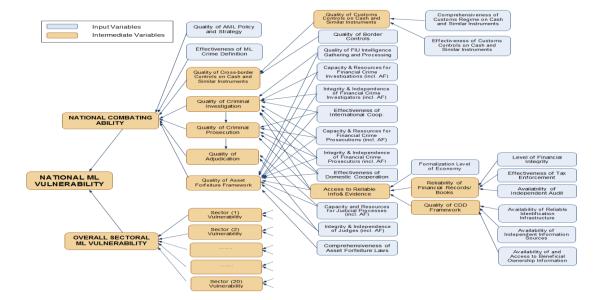
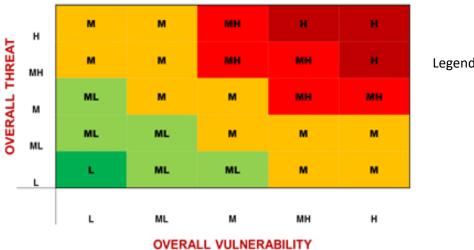


Figure 2. National Money Laundering Vulnerability

The ratings for AML controls or input variables follow a 10-point grading scale, with 1.0 being the highest and 0.1 for unavailability or absence of AML control. On the other hand, intermediate variables or high-level AML combating controls are assessed using the 5-level scale with categories Low, Medium Low, Medium, and Medium High.

The overall money laundering risk level is a function/combination of the results of the threat assessment and the vulnerability assessment, as shown in the correlation matrix:



OVERALL MONEY LAUNDERING RISK IN THE JURISDICTION

Figure 3: Overall Money Laundering Risk

Legend: L - Low

ML - Medium Low M – Medium

MH - Medium High

H - High

Quantitative and qualitative research methods are used in this NRA. The quantitative data and statistics used in the NRA are derived from periodical reports and submissions of LEAs and government agencies. Private entities, associations and covered persons have also been tapped by the sectors to provide data and information to support the NRAWGs' assessments. Electronic mails and request letters sent to several institutions, face-to-face and phone interviews were also conducted to verify the information and clarify issues.

Qualitative method using survey research was used as an additional support to the descriptive assessment of the variables. The survey employed the purposive sampling<sup>5</sup> technique in which the samples/respondents are selected on the basis of knowledge, connection and judgment in relation to ML/TF assessment.

#### LIMITATIONS OF THE ASSESSMENT

The assessment is faced by a number of limitations and challenges as follows:

Data and statistics available with some agencies are not updated. Some agencies are still in the
process of compiling and verifying 2016 data. Further, sectors, such as those under the DNFBPs,
do not maintain the data<sup>6</sup> or statistics requested by the NRAWG.

The NRAWGs resolve to use other quantifiable sources in order to obtain data necessary for the assessment. Surveys, research works, and related studies are among the sources of information.

- Dissemination of data and information sharing. Some government institutions require official clearances before the data is released.
- Proceeds generated from predicate crimes, terrorism and terrorist financing are usually not captured.

Proceeds are not collected for some predicate offenses, such as kidnapping for ransom (KFR), and therefore difficult for the NRAWG to assess the impact and extent of these crimes. In such cases, the NRAWG relies on qualitative data such as survey results, research studies made by competent authorities, and best estimates by the LEAs and government agencies.

No centralized database system. Many government institutions still maintain data manually.
 Some information such as mutual legal assistance could not be easily be accessed and verified.

Government institutions are now looking at automating or computerizing data and information.

Nonetheless, the above data limitations do not in any way invalidate the results of this assessment.

<sup>&</sup>lt;sup>5</sup> A form of non-probability sampling in which decisions concerning the individuals to be included in the sample, are based on a variety of criteria which may include specialist knowledge of the research issue, or capacity and willingness to participate in the research.

<sup>&</sup>lt;sup>6</sup> Data may include new and rejected customers, number of cross border transactions, know-your-customer/CDD violations.

#### I. OVERALL THREAT ASSESSMENT

#### THREAT ARISING FROM PREDICATE CRIMES

This assessment aims to update the National Risk Assessment covering the period 2011 to 2014 by assessing the money laundering threat faced by the Philippines for the period 2015 to 2016.

#### **EXECUTIVE SUMMARY**

The national money laundering threat level was assessed based on the prevalence of predicate offenses and the proceeds they generate, the money laundering schemes employed by criminals and the extent covered persons and products in the country's various financial sectors were used in the schemes. The money laundering threat rating has three major components: 1) threat based on predicate crimes and the proceeds they generate; 2) sectoral threat assessment, which measures the exposure of covered persons operating in the different financial sectors to criminal proceeds and money laundering; and 3) external threat assessment, which measures the exposure of the country to criminal proceeds and money laundering.

For the period covered, money laundering threat arising from the following crimes were rated <u>HIGH:</u>
1) tax crimes; 2) smuggling; 3) violation of intellectual property rights; 4) illegal manufacture and possession of firearms, ammunitions and explosives; 5) violation of environmental laws; 6) investment scams and estafa; 7) illegal drugs-related crimes; and 8) plunder and corruption-related crimes. Posing lesser threat, criminal proceeds arising from web-related crimes, illegal trafficking of persons and kidnapping for ransoms were rated <u>MEDIUM</u>. Lastly, criminal proceeds arising from other money laundering-predicate crimes were rated **LOW.** 

In the sectoral threat assessment, banks and money service businesses were identified to be the sectors primarily and widely used by criminals to launder the proceeds of their crimes. Following banks and money service business, DNFPBs, more particularly casinos, were used to launder huge amount of stolen funds. The securities and insurance sector were identified to have been used in money laundering schemes less widely.

In the external threat assessment, the threat coming from proceeds of crimes committed outside of the country's territory was assessed to be <u>HIGH</u> based on the huge amount of illicit funds involved in identified money laundering investigations, requests for information and Mutual Legal Assistance Treaty (MLAT) requests received by the AMLC from foreign jurisdictions during 2015 to 2016.

Overall, the national money laundering threat level was assessed as **HIGH**.

# DATA AND INFORMATION COLLECTION

The data used in this assessment were collected from the law enforcements authorities (LEA) which are members<sup>7</sup> of the Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Sub-

<sup>&</sup>lt;sup>7</sup> Anti-Money Laundering Council, Bangko Sentral ng Pilipinas, Bureau of Customs, Bureau of Immigration, Bureau of Internal Revenue, Bureau of Jail Management and Penology, Civil Aviation Authority of the Philippines, Cooperative Development Authority, Department of Environment and Natural Resources, Department of Finance, Department of Foreign Affairs, Department of Justice, Department of Social Welfare and Development,

committee of the National Law Enforcement Coordinating Committee (NALECC), the Office of Court Administrator of the Supreme Court and the Sandiganbayan. Data and information were gathered from the LEAs through surveys and consultations. Data available to the AMLC Secretariat pertaining to money laundering investigations also formed part of the data used in this assessment.

The challenge posed by data collection was the lack of uniformity of the data respectively maintained by the LEAs, which prevented them from providing data in the format required by the World Bank Module. This challenge was overcome by consultations with the LEAs involved. In addition, the absence of data on criminal proceeds in majority of the LEAs limited the view of the overall amount involved in the unlawful activities they respectively investigated. With respect to money laundering cases related to an unlawful activity, data on the proceeds was sourced from AMLC's cases. Comparison of data from the LEAs and the AMLC on criminal proceeds was used as basis to understand the money laundering risk posed by unlawful activities.

In conducting the threat assessment, the following factors were taken into consideration: a) number of unlawful activity investigated and prosecuted by LEAs and relevant government agencies; b) number of money laundering investigations and prosecutions, including the conduct of bank inquiry by the AMLC; c) efforts of law enforcement agencies in combating and prosecuting predicate crimes, including money laundering; d) amount of criminal proceeds involved based on LEA and AMLC data, when available; and e) amount of assets subject of freeze orders and civil forfeitures cases. In (d) and e), criminal proceeds amounting to at least PhP50,000,000.00 was set as a general threshold warranting a **HIGH** rating.

#### I. Tax Crimes

Tax evasion is not yet designated as a predicate offense to money laundering under the AMLA, as amended. Nonetheless, the FATF strongly recommends the inclusion of tax crimes as predicate offense to money laundering, as it is one of the designated categories of offenses.

## A. Background

The Bureau of Internal Revenue's (BIR) total revenue collection for CY 2015 reached PhP1.442 trillion, which represent 86.12% attainment of the target tax collection for 2015 and about 55% and 48% of the 2015 and 2016 national budgets, respectively. As claimed by the agency, the improved tax collection for 2015 can be attributed primarily to the implementation of the following programs: Run After Tax Evaders (RATE) and Oplan Kandado programs and other enforcement activities, including the Tax Compliance Verification Drive (TCVD), stocktaking operations, post-evaluation of Cash Register Machines (CRM) / Point-of-Sales Machines (POS), increased collection from delinquent accounts, and the Bureau's intensified audit program. In 2015, BIR's RATE netted 94 cases with estimated tax liabilities amounting to PhP9.71 Billion, while Oplan Kandado Program collected PhP323.95 Million and closed 259 establishments.

\_

Department of Trade and Industry, Insurance Commission, Intellectual Property Office of the Philippines, Intelligence Services Armed Forces, National Bureau of Investigation, National Intelligence Coordinating Committee, National Telecommunications Commission, Office of the Ombudsman, Office for Transportation Security, Philippine Center on Transnational Crime, Philippine Drug Enforcement Agency, PNP Anti-Cybercrime Group, PNP Anti-Kidnapping Group, Presidential Anti-Organized Crime Commission, PNP Aviation Security Group, PNP Criminal Investigation and Detection Group, PNP Directorate for Investigation and Detective Management, PNP Highway Patrol Group, PNP Intelligence Group and Securities and Exchange Commission.

<sup>&</sup>lt;sup>8</sup> https://www.bir.gov.ph/images/bir\_files/annual\_reports/annual\_report\_2015/download2015.html accessed on 14 August 2017.

#### **B.** Investigation and Prosecution of Tax Crimes

BIR provided the following data on tax evasion cases from 2005 to first quarter of 2017:

Table 1-1. Statistics on Tax Evasion Cases from the BIR

Number of cases filed with the DOJ	Number of cases prosecuted in Court	Number of convictions (cases)	Number of persons convicted	Estimated Amount involved (in Millions PhP)	Amount of adjudged in favor of BIR (in Millions PhP)
634	73	5	6	422.66	102,452.6

The Office of Court Administrator (OCA) provided statistics on violations of tax laws for the years 2015 and 2016 as follows:

Table 1-2. Statistics on Tax Evasion Cases from the Supreme Court

Tax Evasion Cases	2015	2016
Newly Filed	440	435
Pending (as of year-end)	759	632
Decided (after trial on the merits)	24	35
Decided (others)	276	208

Cases filed by the BIR with the Department of Justice (DOJ) do not necessarily result in the filing of cases before the courts. Based on the data of BIR, it appears that there are only 5 cases of convictions and 6 persons convicted despite the number of tax cases filed and pending with the courts. And in comparison with the estimated tax liabilities of PhP9.71 Billion resulting from the BIR's 2015 efforts, the amount collected as of the first quarter of 2017 was only 4.35% of said figure. The rest are awaiting the final disposition by courts.

The estimated amount of proceeds based on the data of BIR may be underestimated considering the discrepancy between the number of cases prosecuted according to the BIR and the number of cases pending according to OCA.

#### C. Conclusion

While tax crimes are not predicate offenses to money laundering, it can be seen from the data provided that the proceeds are considerable, amounting to hundreds of millions. Despite efforts of the BIR, convictions and recovery of proceeds is low. Given this, and the absence of authority of the AMLC to conduct a parallel money laundering investigation, it is inevitable to conclude that the threat posed by tax evasion to money laundering is **HIGH**.

#### II. Smuggling

Smuggling or the "practice of using illegal trade channels or fake foreign trade declarations for the purpose of evading the payment of duties and taxes, [which] inevitably causes distortions in

international trade data and in policies subsequently formulated from it remains as an important trade issue, which effectively challenges the government's political and economic authority."

The existence of a robust shadow economy parallel to the formal one creates strong demands for illicit products, which, in turn, encourages smuggling by both small time enterprising individuals and organized crime groups. Moreover, smuggling's economic incentives outweigh legal consequences, thus providing ample temptation for some law enforcers to engage in this illicit activity. As a result, amidst the government's intensive campaigns against smuggling, this crime area persists.<sup>10</sup>

# A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

Several seizures of clandestine laboratories and chemical warehouses, (accounting for 8.4 metric tons of shabu over the 2000-2006 period) placed the country 5th on a global basis. Drug manufacture is managed by transnational organized crime syndicates together with local drug groups, smuggling chemicals into the country via mislabeled shipments and setting up laboratories first in the Metro Manila area, and later as a result of enforcement actions in other regions.<sup>11</sup>

In addition, drug cultivation and smuggling have also been connected to the Abu Sayyaf Group (ASG)<sup>12</sup> as a source for funding: in 1999 Philippines security forces destroyed about 70,000 marijuana plants worth US\$10 million reportedly belonging to ASG operatives. With the death of its key leaders and arrest of its foreign supported financial officers, however, major operations have gone down in recent years.<sup>13</sup>

#### B. Current Trend in Smuggling

On 03 May 2017, The Business World Online published in its website an article entitled- *Illicit funds made up nearly a third of trade inflows in 2014—GFI*, the following information: "Dirty money likely contributed at least a fifth of trade inflows in the Philippines in 2014, a Washington-based research firm said in a report, forming part of a global trend that makes use of developing economies as a haven for ill-gotten wealth. Global Financial Integrity (GFI) said inflows of illegal wealth likely made up between 18-31% of the country's external trade that year, according to the report Illicit Financial Flows to and from Developing Countries: 2005-2014. This compares to the 14-24% average range observed among developing nations, which GFI said shows the "enormous harm" done on these economies through the trade channel. About 87% of illegal inflows come from trade misinvoicing (TM), which is done by under-declaring the value of goods and avoiding compliance, among others."<sup>14</sup>

<sup>10</sup> 2016 SOCTA, page 56

<sup>&</sup>lt;sup>9</sup> 2016 SOCTA, page 55

<sup>&</sup>lt;sup>11</sup> p.22, par. 90, 2009 Philippines MER

<sup>&</sup>lt;sup>12</sup> ASG is a militant organization that is based in the Philippines. Its mission is thought to be the establishment of a separate Islamic state in Mindanao, an island situated in the southern Philippines.

<sup>(</sup>http://www.encyclopedia.com/politics/legal-and-political-magazines/abu-sayyaf-group-asg)

<sup>&</sup>lt;sup>13</sup> p.24, par. 105, 2009 Philippines MER

 $<sup>\</sup>frac{14}{\text{http://www.bworldonline.com/content.php?section=Economy\&title=illicit-funds-made-up-nearly-a-third-of-trade-inflows-in-2014----gfi&id=144614}$ 

Table 1-3. Estimated Ranges of the Illicit Financial Flows in the Philippines
Through TM: 2005-2014

	Outflows (in millions of US Dollars)		Inflo (in millions o	
	Low	High	Low	High
2005	8,365	11,047	8,208	11,304
2006	6,430	8,372	10,697	15,040
2007	5,967 7,972		11,672	16,733
2008	5,212	6,906	14,617	22,847
2009	4,440	5,638	14,516	21,628
2010	4,018	5,368	15,231	24,451
2011	7,719	10,655	15,641	26,541
2012	3,222	4,407	18,342	30,873
2013	2,845	3,833	20,353	33,882
2014	2,596	3,549	24,336	41,628

Source: Global Financial Integrity

Figures represent 10% of the estimated ranges

Table 1-4. Trend on the Estimated Illicit Financial Flows in the Philippines
Through Trade Misinvoicing: 2005-2014

Through Trade Wishvolding: 2005-2014					
	Outflows			Infl	ows
	Low	High		Low	High
2005	100.00%	100.00%		100.00%	100.00%
2006	-23.14%	-24.21%		30.33%	33.06%
2007	-28.67%	-27.83%		42.21%	48.03%
2008	-18.95%	-17.52%		36.65%	51.91%
2009	-25.58%	-29.28%		24.36%	29.26%
2010	-22.90%	-22.26%		4.20%	7.02%
2011	73.84%	88.99%		7.75%	22.71%
2012	-19.82%	-17.92%		20.42%	26.26%
2013	-63.14%	-64.03%		30.12%	27.66%
2014	-19.42%	-19.46%		32.68%	34.84%

AMLC Secretariat's computation using the following formula: Percentage of inc/dec [Y2005(Y0) as base year]=(Y2-Y0)/Y0

The percentage of increase or decrease in the amount of outflow and inflow of illicit funds in the Philippines through TM may also be expressed in terms of graphical representation, as follows:

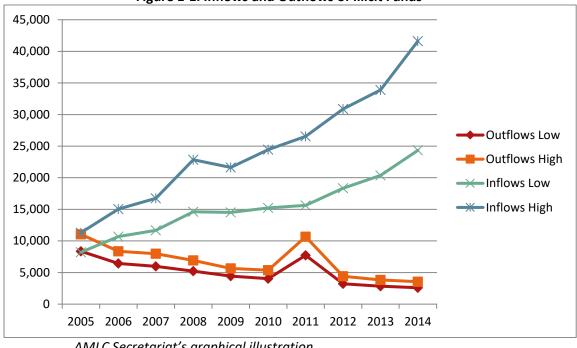


Figure 1-1. Inflows and Outflows of Illicit Funds

AMLC Secretariat's graphical illustration

The trend shows a continuous increase in the amount of illicit financial inflow through TM starting 2005 until 2014. On the other hand, the illicit financial outflow through TM within the same period demonstrates an unstable flow. Between the outflow and inflow, the amount of illicit financial inflow through TM is relatively much higher than the amount of illicit financial outflow. From 2005-2014, the outflow of illicit funds through TM shows a continuous decrease except for 2011, which registered a sharp increase equivalent to 73.84% and 88.99% for low and high ranges, respectively. For the same period, the inflow lines for both the low and high ranges in the graph show an upward slope although the average marginal increase went down towards 2010 but it gradually increased thereafter up to the end of 2014. It may be fairly inferred that illicit proceeds generated from TM within the Philippines are less likely to be transferred across the geographical border and more likely to be laundered within the domain of the Philippines. On the other hand, the influx of illicit funds sourced from TM continue to increase and may probably suggest a weak law enforcement effort regarding entry of illicit goods in the Philippines, hence, this aggravates the money laundering threat in the country arising from smuggling activities.

The prevalence of smuggling activities in the country is attributable to various factors such as geographical landscape of the country, unregulated private ports, high-seas smuggling, and legal and legislative framework.<sup>15</sup> Another contributing factor may be the reported complicity of some customs officials in smuggling activities.

Smuggling has consistently been resorted to as a means to undertake illicit drug operations. Transnational organized drugs syndicate smuggle drugs into the Philippines through mislabeled shipments and set up laboratories in coordination with local drug groups. There are intelligence reports, however, that drug syndicates have already shifted much to importation of illegal drugs through ports of entry considering the government's intensified fight against illegal drugs. In 2016 alone, at least PhP1.6 billion worth of illegal drugs were intercepted in various smuggling activities undertaken in airports and Philippine Post Office. 16 On top of this, another drug smuggling activity

<sup>15 2016</sup> SOCTA

<sup>&</sup>lt;sup>16</sup> https://www.pressreader.com/philippines/manila-bulletin/20161225/282011852018364

involving a PhP6.4 billion worth of shabu is under investigation after the cargo passed through the BOC's express lane on 23 May 2017 without having been inspected by the customs officials.<sup>17</sup>

#### C. Investigation and Prosecution of Smuggling cases

The government has been strengthening the Run After the Smugglers (RATS) Program, implemented by the Department of Finance (DOF) and Bureau of Customs (BOC), which focuses on profiling, monitoring, and building of cases for the successful prosecution of smugglers and their cohorts, including BOC personnel, importers, brokers, and other persons suspected or reported of being involved in smuggling activities.<sup>18</sup>

**Table 1-5. Anti-Smuggling Cases** 

Year	Cases handled/referred by BOC to DOJ	Cases filed in court
<b>2011</b> 69		22
2012	39	29
2013	12	4
2014	35	46
2015	10	52

Sources: 2016 SOCTA, BOC Annual Reports

At the end of 2014 alone, the smuggling cases pending before the DOJ for preliminary investigation involves a dutiable value equivalent to more than PhP56 billion, out of which PhP1.4 billion pertains to eighteen (18) rice smuggling cases. <sup>19</sup> This amount, however, represents merely about 3%-5% of the estimated ranges of illicit inflow of funds through trade misinvoicing recorded by the GFI for 2014. <sup>20</sup> It is notable that in 2014 and 2015, more cases were filed in court as compared to the number of cases handled by the BOC and referred to the DOJ for preliminary investigation. In the same year, the BOC obtained a verdict of conviction in one case it investigated.

Back in 2012, The Court of Tax Appeals (CTA) sustained the guilt of the accused for illegal importation of vehicles from South Korea who was sentenced to up to 12 years of imprisonment and payment of fine amounting to PhP8,000. The vehicles involved bear estimated taxes and duties equivalent to PhP1.8 million. The CTA also sustained the guilt of two (2) individuals indicted for illegally importing 510,000 kilograms of sugar from Singapore, which they misdeclared as 306 kilograms of soy beans. They were sentenced to be imprisoned for 2 consecutive nine-year jail terms and to pay a fine amounting to PhP20,000. They were also ordered to pay duties and taxes amounting to PhP5 million. Finally, the Regional Trial Court (RTC) of Pasay convicted an Indonesian drug-mule who arrived at the NAIA Terminal 3 from Hong Kong bringing 3.7 kilograms of shabu worth PhP29.9 million. The accused was sentenced to be imprisoned for two years and pay a fine equivalent to PhP5,000.<sup>21</sup>

#### D. Financial Investigation

Smuggling syndicate undeniably generates vast amount of criminal proceeds that undermines the economy. Trade misinvoicing disrupts efficient collection of taxes, which means a decrease in total generation of public funds and delay in the delivery of public services. For 2015-2016, the AMLC

<sup>19</sup> 2014 BOC Annual Report

<sup>&</sup>lt;sup>17</sup> http://newsinfo.inquirer.net/919298/house-body-to-conduct-own-probe-into-p6-b-drug-smuggling.

<sup>&</sup>lt;sup>18</sup> 2016 SOCTA

<sup>&</sup>lt;sup>20</sup> See Table 1-3

<sup>&</sup>lt;sup>21</sup>"Customs' Anti-Smuggling Campaign Scores", 22 October 2014, http://www.dof.gov.ph/customsngbayan/?p=8161

received referrals from other government agencies and currently building up possible money laundering cases predicated on rice smuggling and online smuggling cases.

#### E. Conclusion

The previous NRA exercise rated the money laundering threat arising from smuggling a HIGH risk based on data covering the 2011-2013 assessment periods. Such rating took into consideration the amount of income lost from evasion of custom duties, the absence or insufficiency of material records, the low number prosecution and conviction rate, and forfeiture cases.

Additional data covering 2014-2015 were gathered while data for 2016 remains unavailable. However, the additional data do not suggest any justifiable change in the rating specially so that there is substantial deviation from the trends in smuggling activities. The number of cases filed in court continues to increase as well as the inflow of funds involved in smuggling activities. Furthermore, the very low conviction rate confirms inefficiency in the enforcement and prosecution mechanism. Hence, the threat rating for this predicate offense remains **HIGH**.

#### III. Copyright Infringement/Intellectual Property Law Violations

In February 2013, Republic Act No. 10372 was signed into law, amending and updating the Intellectual Property Code of the Philippines. Three (3) other IP-related laws<sup>22</sup> were also signed that year. These laws set up the stage for the Philippines to implement a wholistic approach to IP protection and development.

#### A. Current IPR Violations Trend

The intensified campaign against IPR violations has been recognized internationally. The United States Trade Representative (USTR) Special 301 Report of 2014<sup>23</sup> removed the Philippines from the watch list based on "sustained actions that the Philippine government has undertaken to improve intellectual property rights protection and civil administrative enforcement. The Special 301 Report cites the Philippines' public-private partnership in raising IPR protection awareness as among the best practices worldwide.<sup>24</sup>

#### **B.** Investigation and Prosecution of IPR Violations

Table below summarizes the operations conducted by LEAs and the value of goods seized.

Page 20 of 300

\_

<sup>&</sup>lt;sup>22</sup>R.A. 10515 or the Anti-Cable Television and Cable Internet Act; R.A. No. 10557, The Philippine Designed Competitiveness Act of 2013; R.A. No. 10365, the Amendment to the Anti-Money Laundering Act of 2001 (including IP-Code violations as a predicate crime to money laundering).

<sup>&</sup>lt;sup>23</sup>http://www.ipophil.gov.ph/releases/2014-09-22-06-26-21/434-reforms-in-philippine-ip-regime-recognized-in-the-2016-ustr-special-301-watch-list-report <sup>24</sup> lbid.

Table 1-6. Enforcement Summary of Intellectual Property Office of the Philippines (2015 - 2016)\*

	No. Of Operations			Quant	tity	Estimated Value	
Year	Inspection	Plant Audit	Search Warrant	WSD	Pieces	Cartons/ Stacks	(PhP)
2013	2471		843	10	6,513,434	8,072	7,839,004,211.00
2014	2192		597		13,074,721	5,258	13,328,159,122.16
2015	1507		463		1,950,465	1,900	2,003,712,006.55
2016	2580		508	1	7,433,633	2,815	6,519,376,647.00

• Data sourced from IPOPHIL

Data reveals that in 2014, there was a significant increase in the seizure of pirated and counterfeit goods as the number and amount of items seized involving violations of intellectual property rights doubled the data of 2013. Because of the increased emphasis on enforcement actions during the year, coupled with significant legislative reforms,<sup>25</sup> enhanced inter-agency cooperation, and sustained engagement with the private sector, the Philippines was removed from the Watch List in the 2014 Special 301 Report.<sup>26</sup> In 2015, although there was a noted decline in the number and amount of items seized for IP violations, the Philippines remained outside the watch list in the 2015 Special 301 Report mainly because of the Philippines' effective enforcement through inter-agency cooperation.<sup>27</sup> In 2016, there was an increase in the number and amount of seized counterfeit products. The Philippines was lauded in the 2016 Special 301 Report for its initiatives in partnering to provide training with other international organizations to improve IPR protection and enforcement.<sup>28</sup>

Table 1-7 summarizes the IPO violations investigated and prosecuted by LEAs in 2015 and 2016.

Table 1-7. IPO Cases Investigated by PNP and NBI\*

	20	15	2016		
Law Enforcement Agency	No. of Cases Detected or Investigated	No. of Cases Prosecuted	No. of Cases Detected or Investigated	No. of Cases Prosecuted	
PNP	186	14	186	29	
NBI	171	47	225	65	

<sup>\*</sup>Data lifted from NBI and PNP Reports

Of the terminated cases by the National Bureau of Investigation (NBI), about 27% were recommended for prosecution. About 74% of the cases detected/investigated by the NBI in 2015 and 85% in 2016 were committed in key areas of the National Capital Region (NCR). Further, Table 1-8 shows the summary of the enforcement activities in strategic areas in 2016. These places are identified as notorious areas selling goods that infringe on intellectual property rights.

<sup>26</sup>2014 Special 301 Report

<sup>27</sup>2015 Special 301 Report

<sup>28</sup>2016 Special 301 Report

<sup>&</sup>lt;sup>25</sup> Supra, note 15

No. of Areas Raided **Period Agency** Makati St. Grand Metro 168 Quiapo Binondo Cinema Francis Greenhills Others **Total** walk Mall Square Square 44 NBI 2 10 2 30 Jan-**PNP** 27 3 21 3 Dec 237 10 1 2 **OMB** 1 220 2016 8 BOC 8 Sub-total 15 14 2 0 2 1 3 279 316 **Grand Total** 

Table 1-8. Summary of Enforcement Activities in Strategic Places\*

Table 1-9 summarizes the cases filed before the Supreme Court involving intellectual property rights violations.

IPC Violations	2011	2012	2013	2015	2016
Newly Filed	277	329	347	331	435
Pending (as of year-end)	700	737	691	831	760
Decided (after trial on the merits)	24	32	33	32	24
Decided (others)	13	165	146	196	159

Table 1-9. Statistics on IPC Violations<sup>29</sup>

Data shows that there is an increasing trend in the number of cases filed for IP violations from period 2011 to 2016. In 2016, filed cases increased by around 31% from 2015. This could be interpreted as a result of the more intensive law enforcement campaign against IP violators. Moreover, there is an increase in the number of resolved cases involving IP violations from 37 cases in 2011 to 183 cases in 2016, although an observed 20% decrease on decided cases from 2015 to 2016 was noted.

# C. Financial Investigation

Despite the increase in the number of cases filed for IP violations and the value of the goods seized, no reports or requests for financial investigation were forwarded to the AMLC for IPR violations, and there are no ML cases predicated on IPR violations.

#### D. Conclusion

In 2014, there was a significant increase in the items and amount seized in violation of the Intellectual Property Laws of the Philippines.

More effective enforcement of IPO laws was driven by legislative reforms, enhanced inter-agency cooperation, and sustained engagement with the private sector and as a result, the Philippines was removed from the Watch List in the 2014 Special 301 Report and the same status is sustained until

<sup>\*</sup>IPOPHIL Reports

<sup>&</sup>lt;sup>29</sup>Statistics from Supreme Court Office of the Court Administrator.

2016. Although there was an increase in cases filed in violation of IP Law, no money laundering investigation predicated on IPR violation has been initiated. Thus, the threat posed by IP Violations is rated **HIGH**.

# IV. Illegal Manufacture and Possession of Firearms, Ammunitions and Explosives

#### A. Current Trend

The Serious and Organized Crime Threat Assessment (SOCTA) 2016<sup>30</sup> lists local production, smuggling from other countries, and leakages and diversions from arms stockpiles of the government and arms traders as primary sources of loose firearms. Firearms acquisition is driven by self-protection, and attainment and preservation of economic and political advantages.

In the Philippines, there is a nexus of gun running with different criminal activities like robbery, assassinations, kidnapping for ransom, and illegal drug trade. Moreover, use of loose firearms increases during election periods by private army groups who are engaged in supporting and protecting, in exchange for monetary gains, moneyed and influential politicians. In the conflict zones of Mindanao, armed citizens are prevalent due to need to protect lives and properties against bandits and criminals exploiting the instability of the region. Terror groups in the region display publicly their firepower to project confidence in their struggle and to appeal disenfranchised individuals to join their cause.

Based on the report, there are around 20,000 unlicensed firearms and an estimated 500,000 more firearms with expired licenses.

#### B. Investigation and Prosecution of Illegal Possession of Firearms Cases

In 2015 and 2016, the NBI reported the following data on pertaining to their investigations on Illegal Possession of Firearm cases:

Table 1-10. Illegal Possession Cases Investigated by the NBI

2015		2016		
No. of Cases Detected or Investigated	No. of Cases Prosecuted	No. of Cases Detected or Investigated	No. of Cases Prosecuted	
60	28	62	24	

There is no data as to the amount of proceeds in illegal possession cases.

Of the illegal possession of firearms cases investigated by the NBI, around 33% and 22% were committed in the NCR on 2015 and 2016, respectively. Moreover, Regions 3 (Central Luzon), 4 (CALABARZON and MIMAROPA), 5 (Bicol Region), 6 (Western Visayas), 7 (Central Visayas), and 11 (Davao Region) registered relatively higher incidences compared to other regions. Surprisingly, there are only few cases recorded at the conflict-affected areas in Mindanao where presence of terroristic activities is prevalent because of weak law enforcement efforts and justice system and considering the security risks in the area.

\_

<sup>30</sup>SOCTA 2016

The statistics on illegal possession of firearms, ammunitions and explosives as provided by the Supreme Court's Office of the Court Administrator are as follows:

Table 1-11. Illegal Possession of Firearms, Ammunition and Explosives<sup>31</sup>

	2011	2012	2013	2015	2016
Newly Filed	4,055	4478	5198	8,071	9,270
Pending (as of year-end)	9,553	10,623	10,799	17,678	19,617
Decided (after trial on the merits)	751	897	907	1,338	1,499
Decided (others)	2,221	2,212	2,274	2,897	2,986

Data from the Supreme Court reflects a significant increase in the number of illegal possession of firearms cases filed from 4,055 in 2011 to 9,270 in 2016. The increase could be interpreted as a result of a more resolute campaign against illegal possession of firearms. Moreover, a steady increase in the number of resolved cases was noted from 2011 to 2016. During 2016, there was an increase of cases resolved from 4,235 in 2015 to 4,485, although cases pending in the Court correspondingly increased by around 11% from 17,678 in 2015 to 19,617 in 2016.

#### C. Financial Investigation

As of end of 2016, there are no money laundering cases predicated on illegal possession and manufacture of firearms, ammunition and explosives. There are also no reports or requests for financial investigation submitted to the AMLC.

#### D. Conclusion

The illegal/unlawful possession, manufacture, dealing in, acquisition or disposition of firearms, ammunition or explosives was included only as predicate crimes to money laundering in February 2013. Appropriate government agencies have not gathered information on the value of proceeds generated by these predicate crimes. Although there was a noted increase in the number of cases filed in the courts starting 2015, pending cases at year-end also correspondingly increased. The rate of decided cases is still low in 2016 and there is no material trend of increase in percentage of decided cases in relation to cases filed/pending cases as of year-end. There was no illegal/unlawful possession of firearms – related cases referred to the AMLC for investigation as of 2016. Thus, the threat rating for these crimes is **HIGH**.

#### V. Environmental Crimes

Environmental crimes, specifically violations of Sections 78 to 79 of the Revised Forestry Code, as amended (P.D. No. 705), violations of Sections 101 to 107, and 110 of Philippine Mining Act of 1995 (R.A. No. 7942), violations of Sections 27 (c), (e), (f), (g) and (i) of Wildlife Resources and Conservation Act (R.A. No. 9147), violation of Section 7 (b) of the National Caves and Cave Resources Management Act (R.A. No. 9072), and violations of Sections 86 to 106 of the Philippine Fisheries Code of 1998 (R.A. No. 8550) were made predicate offenses to money laundering in 2013.

<sup>&</sup>lt;sup>31</sup>Based on data submitted by the Office of the Supreme Court Administrator

#### A. Investigation and Prosecution of Environmental Cases

In 2016, as a testament to the threat posed by environmental crimes, the Department of Environment and Natural Resources (DENR), Department of the Interior and Local Government (DILG), Department of National Defense (DND), Department of Transportation (DOTr), Philippine National Police (PNP), Philippine Coast Guard (PCG) and the Armed Forces of the Philippines (AFP) created a task force that would go after large-scale environmental offenders, and ensure full and strict implementation of vital laws and regulations on environmental protection.

The DENR provided the following data on the number of environmental crimes which were included as predicate crimes to money laundering beginning February 2013:

Table 1-12. Environmental Crimes Statistics from the DENR

Unlawful Activities	2011	2012	2013 (Jan-June)
Violations of Sections 78 to 79 of the Revised Forestry Code	279	107	101
Violations of Sections 101 to 107, and 110 of the Philippine Mining Act	-	-	-
Violations of Sections 27 (c), (e), (f), (g) and (i) of Wildlife Resources and Conservation Act	17	16	9
Violation of Section 7(b) of National Caves and Cave Resources Management Act	No data available		ble

The DENR, NBI and PNP provided the number of environmental crimes they investigated as follows:

1. The DENR provided the following data on violations of the Revised Forestry Code as of 08 February 2017:

Table 1-13. Investigations on Violations of P.D. No. 705 by DENR

Regions	Number of Apprehensions	Cases Filed	Administrative Cases Filed	Confiscation Orders
Total	1,621	54	416	327

The estimated value of forest products apprehended as of 2017 aggregated to PhP59.4 Million with 21% of said value coming from Region 8; 19% in Region 13; 12% in Region 7; and 10% in Region 4B.

2. The DENR likewise provided the following data on violations of the Philippine Mining Act for the same period:

Table 1-14. Investigations on Violations of R.A. No. 7942 by DENR

	2015		2016		
No. of Cases Detected or Investigated	No. of Cases Prosecuted	Amount of Proceeds Confiscated (PhP)	No. of Cases Detected or Investigated	No. of Cases Prosecuted	Amount of Proceeds Confiscated (PhP)
127	18	123,751,560.00	149	65	212,717,940.00

3. The NBI investigated the following violations of R.A. Nos. 9147, 9072 and 8550 in 2015 and 2016:

Table 1-15. Environmental Crimes Investigated by NBI

Year	R.A. No. 9147	R.A. No. 9072	R.A. No. 8550
2015	3	0	0
2016	7	0	5
Total	10	0	5

4. The PNP investigated a total of 963 illegal fishing cases under R.A. No. 8550 as of 2016.

On violations of various environmental laws prosecuted in court, the OCA show the following figures for 2011 to 2013:

Table 1-16. Statistics on Environmental Laws Violations from the Supreme Court

Environmental laws violations	2011	2012	2013
Newly Filed	1,350	2,215	2,733
Pending (as of year-end)	2,543	3,373	3,693
Decided (after trial on the merits)	137	150	142
Decided (others)	465	647	724

For 2015 and 2016, the OCA provided the following statistics on cases of violations of various environmental laws pending trial in various courts:

Table 1-17. Statistics on Violations of Environmental Laws from the Supreme Court

Environmental laws violations	2015	2016			
Newly Filed	3,404	3,328			
Pending (as of year-end)	6,019	3,601			
Decided (after trial on the merits)	224	179			
Decided (others)	900	976			

#### **B.** Financial Investigation

As of end of 2016, there is no money laundering investigation predicated on violation of environmental laws. To strengthen cooperation for the possible development of cases, the AMLC and the DENR are already in the process of executing a Memorandum of Agreement to facilitate cooperation in investigating and prosecuting money laundering offenses predicated in violations of environmental laws.

#### C. Conclusion

The number of cases involving violations of P.D. No. 705, R.A. No. 7942, R.A. No. 9147, R.A. No. 9072, and R.A. No. 8550, the criminal proceeds involved in violations of P.D. No. 705 and R.A. No. 7942 alone aggregating to about PhP396 Million, and the absence of parallel money laundering investigation warrant the **HIGH** rating for the threat posed by environment crimes.

#### VI. Investment Fraud and Estafa

There are two (2) major well-known forms of investment fraud: Ponzi and Pyramid schemes. The PNP Guidelines for the Detection and Investigation of Investment Fraud differentiated the two schemes succinctly as follows:

A Ponzi scheme is built meticulously from the ground up. An unscrupulous broker begins by creating false documents, which he then uses to lure investors. The money he gathers does not go into any real investments, however, but into his own pocket. As the scheme progresses the broker secures additional investors, and uses their funds to continue to line his own bank account, as well as returning some to the initial parties to support the illusion that their investments are creating dividends. When there are no more new investors, this form of investment fraud is usually exposed.

One of the differences that make a Pyramid scheme more difficult to detect than a Ponzi scheme is the sheer number of people involved, which lends the scam credibility in the eyes of investors. Rather than recruiting investors, the perpetrator of this scam recruits more recruiters. Each investor is expected to bring more investors on board working under him, and the money is then disseminated to the levels above. This creates an organizational structure similar to a pyramid, hence the name. Since these scams lack a solid foundation in goods or services, the pyramid collapses once no new investors can be found.

The main difference between these scams is the structure. Pyramid schemes work in a top-down manner, involving multiple levels of investors. Ponzi schemes, on the other hand, have a more circular structure centered around the perpetrator of the scam, with all investors on equal, illegitimate footing.

Perpetrators of these schemes may face prosecution for the crime of estafa or violation of Republic Act No. 8799 or the Securities Regulations Code (SRC).

# A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

The 2009 Philippine MER noted "networking" or "pseudo-deposit-taking activities" or "high yield investment programs" as the prevalent illegal investment scheme in the country. The scheme generally consisted of misrepresentation that the solicitation of investments was authorized by the SEC.

#### B. Current Investment Scam/Fraud Trend

The advisories issued by the Securities and Exchange Commission (SEC) warning the public against dealing with at least 32 entities operating without license from the SEC or offering their shares for sale to the public without the required license in 2015 and 2016 mirror the observations in the 2009 Philippine MER, which makes said observations relevant to this date.

## C. Prosecution of Investment Scam and Estafa Cases

In 2015 and 2016, data from SEC showed the following figures on violations of the SRC:

	Table 1-18. SRC Violations Investigated by SEC							
Year	No. of cases detected or investigated	No. of cases prosecuted	No. of convictions (cases)	No. of persons convicted	No. of cases referred to AMLC			
2015	203	4	1	1	1			
2016	147	26	0	0	14			
TOTAL	350	30	1	1	15			

About 2% of the cases investigated by the SEC in 2015 and 18% in 2016 were prosecuted. NBI also investigated three cases of SRC violation in 2015 and one case in 2016, all allegedly committed in the NCR. The SRC violation investigated in 2016 involved criminal proceeds approximately amounting to PhP200 Million.

For the period 2009 to 2013, an average of 13,458 estafa cases were prosecuted each year according to the DOJ. In 2015 and 2016, data from the Philippine National Police (PNP) and the NBI showed the following:

Table 1-19. Estafa Cases Investigated by PNP and NBI

	201!	5	2016	
Law Enforcement Agency	No. of Cases Detected or Investigated	No. of Cases Prosecuted	No. of Cases Detected or Investigated	No. of Cases Prosecuted
PNP	6,669	2,554	4,718	1,829
NBI	2,755	660	3,314	975
Total	9,424	3,214	8,032	2,804

Of the 11,387 cases investigated by PNP for the period 2015 to 2016, about 26% in 2015 and 39% in 2016 were allegedly committed in the NCR. Similarly, out of the 6,069 cases investigated by NBI, 31% in 2015 and 40% in 2016 were allegedly committed in the NCR. Moreover, 34% of the total number of cases investigated by the two agencies were prosecuted.

From 2011 to 2013, the SEC reported that there were 393 fraud investigations related to pyramiding schemes. As of 2014, a total of 19 cases involving said schemes are pending trial before the courts for violations of the SRC while 9 complaints are pending preliminary investigation before the DOJ.

#### D. Financial Investigation

For the period 2011 to 2016, sixteen (16) money laundering cases were investigated predicated on SRC violation and estafa as follows:

Table 1-20. Fraud-related Money Laundering Investigations

Predicate Crime Involved	2011	2012	2013	2014	2015	2016
SRC Violation	-	-	-	-	-	1
Estafa/Swindling	6	5	5	10	4	1

The six (6) cases investigated in 2015 to 2016 involved criminal proceeds amounting to about PhP231 Million. In relation to the aforementioned investigations, the AMLC filed the following petitions to freeze and for civil forfeiture:

	2011	2012	2013	2014	2015	2016
Petition for the						
Issuance of Freeze	6	5	1	1	1	-
Order						
Petition for Civil	1*	2	4	1	1	1
Forfeiture	1	2	4	1	1	1
Money Laundering					2	ı
<b>Total Cases</b>	7	7	5		4	1
Amount of proceeds	PhP.265	PhP33.71	PhP233.3	PhP.559	PhP9.98	PhP.863
subject of forfeiture	USD.0010	USD.0006	2USD.707	USD.0000	USD.024	
proceedings	GBP .007			9 EUR.101		
(in millions)						

Table 1-21. Freeze and Confiscation

In one case predicated on the crime of estafa, the court rendered partial judgment in favor of the government in the amount of PhP481,317.93.

#### E. Conclusion

The foregoing statistics show a decreasing trend of investigations involving estafa and SRC violation and minimal money laundering investigations predicated on both crimes. Nonetheless, the number of estafa cases and SRC violations, taken together, remains significantly high. In addition, the number of money laundering cases predicated on the two crimes remains minimal. In fact, the amount of criminal proceeds involved in the six (6) money laundering investigations in 2015 and 2016 translates to only 3% of the total amount of criminal proceeds in said crimes. The foregoing justify the retention of **HIGH** rating for the threat posed by fraud.

#### VII. Violation of the Dangerous Drugs Law<sup>32</sup>

Production, trade and consumption of illegal drugs continue to be a major concern in the Philippines.

Drug trafficking poses a major role in the proliferation of illegal drugs in the country. Due to its strategic location and vast and porous shorelines, the Philippines is a choice as a trans-shipment point, through its various airports and seaports, for the distribution of illegal drugs by local and international syndicates. Among these international syndicates are the African Drug Syndicates, Chinese Drug Syndicates and Mexican Sinaloa Drug Syndicate. They use local drug groups to facilitate domestic distribution and employ displaced Overseas Filipino Workers and willing individuals as "mules" in transporting drugs overseas.<sup>33</sup>

The manufacture and cultivation of illegal drugs in the country is manifested through the discovery and subsequent dismantling of clandestine shabu laboratories and eradication of marijuana plantation

<sup>\*</sup>One petition for the issuance of freeze order resulted in the filing of petition of civil forfeiture.

<sup>&</sup>lt;sup>32</sup>Information and data are provided by the Philippine Drug Enforcement Agency (PDEA).

<sup>&</sup>lt;sup>33</sup>Philippine Drug Enforcement Authority 2016 Annual Report.

sites. Big time drug traffickers use unassuming facilities that houses the clandestine laboratories in order to conceal their activities during production.

Drug syndicates continue to innovate strategies to easily, conveniently and safely transport illegal drugs. Trafficking of illegal drugs ultimately goes to the street level markets and ends to the economically or socially disadvantaged.

Law enforcement efforts challenge the international and local distribution of illegal drugs through anti-drug operations conducted. In 2016, the Philippine Drug Enforcement Agency (PDEA) and other LEAs conducted 34,077 anti-drug operations nationwide, resulting in the arrest of 18,056 drug personalities and the seizure of PHP18 billion worth of drugs<sup>34</sup>.

# A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

The 2009 MER states that the country is a significant producer, transit point and consumer country of crystal methamphetamine (locally referred to as "shabu"). Drug manufacture is managed by transnational organized crime syndicates together with local drug groups by smuggling chemicals and setting up laboratories in the country.

# B. Current Drug Trafficking Trend

The relentless anti-illegal drug campaign by the government resulted in the seizure of various dangerous drugs, controlled precursors and essential chemicals (CPECs), and other non-drug evidence. The drugs seized during 2016 were valued at about PhP18 billion or an increase of about 232% of the value of seized drug in 2015. Table 1-22 shows the summary of seized drugs and CPECs seized from 2011 to 2016.

145.0 1	rable 1 22: Brags and Cr 203 30:204		
Year	Value in Pesos (in Millions)		
2011	4,669.13		
2012	2,530.52		
2013	5,439.37		
2014	6,182.62		
2015	5,417.40		
2016	18,009.48		

Table 1-22. Drugs and CPECs Seized35

Drug-related operations conducted nationwide in 2016 showed that shabu is still the main drug of choice in the Philippines representing around 66% of the total value of drugs and CPECs seized or 94.93% of the illegal drugs seized. Table 1-23 shows the summary of dangerous drugs and CPECs seized for the year 2016.

-

<sup>&</sup>lt;sup>34</sup>Ibid

<sup>&</sup>lt;sup>35</sup> Data lifted from PDEA Annual Reports from 2011 to 2016.

Table 1-23. Summary of Drugs and CPECs seized in 2016<sup>36</sup>

Particulars	Value in Peso (in Millions)	Percentage of Total Value of Drugs Seized	
Shabu (including liquid shabu)	11,889.66	66.02%	
Marijuana	5,735.90	31.85%	
Cocaine	324.05	1.80%	
Ecstasy	35.84	0.20%	
Other Drugs and CPECs	24.03	0.13%	
Total	18,009.48	100%	

Marijuana remains to be the second most abused illegal drugs in 2016 with 31.85% of the total value of drugs seized.

Notably during 2016, shabu seizure by law enforcement efforts was the highest. Table 1-24 shows the historical data of shabu seizure from 2011 to 2016.

Table 1-24. Shabu Seizures from 2011 to 2016

Table 1 24. Shaba Selzares from 2011 to 2010		
Year	Volume (kg) or (L)	
2010	63 kg	
2011	254 kg	
2012	112 kg	
2013	837 kg	
2014*	718.47 kg / 17.58L	
2015	607.77 kg	
2016*	2,214.14 kg / 1,806.42 L	

<sup>\*</sup>includes liquid shabu

As of December 2016, a total of 19,717 or about 47% of the 42,036 total barangays<sup>37</sup> are affected by the drug menace. The NCR is still the most affected with 99.94% of the region's 1,706 barangays are affected.

Table 1- 25. Barangays Affected by the Campaign Against Illegal Drugs

Year	Affected	Unaffected
	Barangays	Barangays
2015	11,321	30,715
2016	19,717	22,319

Compared to 2015, there was an increase of about 74% affected barangays in 2016. This is amid the intensified drug operations by the law enforcement units. The increase in statistics however does not

<sup>&</sup>lt;sup>36</sup> Data lifted from PDEA Annual Report 2016

<sup>&</sup>lt;sup>37</sup> A barangay is the smallest administrative division in the Philippines and is the native Filipino term for a village, district or ward (<a href="https://en.wikipedia.org/wiki/Barangay">https://en.wikipedia.org/wiki/Barangay</a>)

necessarily mean worsening drug situation in the country but may be due to underreporting of data in previous years.

#### C. Drug-Related Arrests and Investigation

Since the assumption of Rodrigo Roa Duterte to the presidency in 2016, law enforcement became more focused on crime suppression especially on illegal drugs. Upon his marching order, law enforcement efforts to curb the drug problem doubled, registering the highest number of anti-drug operations conducted since 2011.

Table 1-26 shows the summary of drug operations and arrests from 2011 to 2016.

<u>ie 1-20. Juli</u>	e 1-20. Summary of Drug Operations and Am				
Year	No. Drug Operations	No. of Persons Arrested			
2011	12,269	10,636			
2012	9,885	10,159			
2013	11,474	9,162			
2014	16,939	13,792			
2015	25,041	19,432			
2016	34,077	28,056			

Table 1-26. Summary of Drug Operations and Arrests

Data shows that 50,567 drug operations were conducted from 2011 to 2014. In 2015, a remarkable 47.83% increase in drug operations was recorded from the 16,939 operations in 2014. A drastic increase in drug operations was also observed during 2016 whereby a record high 34,077 operations in a 6-year period was registered. Total drug operation on the two-year period 2015 and 2016 totaled to 59,118.

Most of the drug operations during 2016 were buy-bust operations totaling to 21,655. 305 operations were considered high-impact operations involving dismantling of clandestine laboratories and chemical warehouses, eradication of marijuana sites and interdiction operations in major ports. Table 1-27 shows the types of operations conducted by law enforcement during 2016.

In 2016, about 67% of the persons arrested were drug pushers and 27% were drug possessors and users. 112 foreigners were arrested for drug related offenses, dominated by Chinese nationals at 39.29% of the total foreign nationals arrested.

Correspondingly, the number of drug personalities arrested significantly increased as a result of intensified anti-illegal drug operations conducted. A total of 49,389 drug violators were arrested from 2011 to 2014. The biggest number of arrests were recorded in 2015 with 19,432 and 2016 with 28,056 persons arrested, totaling to 47,488 arrests. This translated to an increase by 40.89% and 44.38% in 2015 and 2016, respectively, of arrested persons.

Table 1-27. Operations conducted by LEAs in 2016

Type of Operation	Total
Buy-bust	21,655
Search Warrant	4,498
Test-Buy	3,486

Casing/Surveillance	2,703
Inflagrante Delicto	769
Checkpoint	219
Search Incidental to Lawful Arrest	178
Warrant of Arrest	151
Routinary Inspection	130
Marijuana Eradication	113
Interdiction	90
Seizure of Drugs Incidental to Lawful Search	47
Recovery of Dangerous Drugs/CPECs	36
Controlled Delivery	2
Total	34,077

A significant number of minors are engaged and utilized in illicit drug use, sale and trafficking. Year 2016 recorded the highest incidence of drug apprehension involving minors since 2003, with 376 minors apprehended during anti-drug operations and turned over to Social Workers for support, assistance and rehabilitation.<sup>38</sup>

# D. Prosecution of Illegal Drugs Cases

Data from the PDEA reveals that 119,786 drug related cases were lodged against different personalities. The highest recorded number of cases filed by LEAs was in 2015 and 2016.

Table 1-28. Operations vs. Cases Filed

Year	No. of Operations	No. of Cases Filed
2011	12,269	12,627
2012	9,985	12,532
2013	11,474	10,502
2014	16,939	17,619
2015	25,041	30,282
2016	34,077	36,224

A more or less 20% increase in the number of cases filed against drug personalities was registered in 2016 compare to 2015. A significant increase of the cases filed was recorded upon the assumption of President Duterte during the 2<sup>nd</sup> quarter of 2016.

The PDEA incessantly monitors the status of filed cases in the different courts. Data reveals that conviction achieved on filed cases is low. Table 1-29 shows the summary of status of resolved cases from 2002 to 2016.

-

<sup>382016</sup> PDEA Annual Report

No. of No. of Resolved No. of Conviction Dismissal Acquittal Year **Convictions** Cases Cases Rate Rate Acquittal Rate (Cases) Dismissed 2002 -14,087 17.48% 26.71% 43.64% 2012 2013 28 160 41 26% 91 57% 17% 2014 3,301 636 19% 903 27% 1,762 54% 2015 3,030 631 21% 685 23% 1714 57% 2016 22% 24% 54%

Table 1-29. Summary of Status of Resolved Cases by the Courts

In 2015, out of 30,282 cases filed, only 3,030 were resolved, with 631 convictions, 685 dismissed cases and 1,714 acquittals. In 2016, the conviction, dismissal and acquittal rates of 2015 were more or less maintained. PDEA asserts the challenges that hinder personalities from being penalized under the law as follows: a) insufficiency of evidence or lack of probable cause, b) irregularity or illegality of arrest, search and seizures, and c) failure to comply with the technical provisions of the Drug Law.

Table 1-30 shows data obtained from the courts through the Supreme Court's Office of the Court Administrator (SC-OCA) on drug-related cases filed with the courts nationwide.

Table 1-30. Drug Related Cases Filed in Courts

	Table 1-30. Drug Related Cases Tiled III Courts				
Year	Newly Filed	Pending Cases as of Year-End	Decided Cases on the Merits	Decided Others	
2011	17,899	66,242	7,832	4,251	
2012	19,908	73,466	7,069	4,803	
2013	21,959	73,041	6,839	4,584	
2015	53,481	138,368	9,015	7,146	
2016	88,280	186,538	10,486	9,581	

The data shows that there is a steady increase in cases newly filed in different courts, with the highest cases filed on 2015 and 2016 totaling to 141,761 cases. Correspondingly, pending cases as of yearend in said years increased also dramatically. The piling up of undecided cases may be due to relatively low rate of deciding filed cases over the years. Because of this, just several days after President Duterte assumed office, the Supreme Court designated an additional 240 courts to hear, try and decide cases filed in violation of the Dangerous Drugs Act.<sup>39</sup> However, with the present volume of caseloads of the different drug courts and procedural requirements in hearing and deciding cases, the effects of the additional courts in disposing of drug cases may not be felt immediately.

#### E. Financial Investigation

PDEA, other relevant government agencies and the AMLC collaborated in tracing the proceeds of drugrelated crimes. This resulted in the filing of criminal charges for violations of the Dangerous Drugs Act and for violations of the AMLA, and the freezing, asset preservation and forfeiture of the proceeds of the crime.

<sup>&</sup>lt;sup>39</sup> "PDEA lauds SC for additional 240 RTCs to handle drug cases nationwide," Philippine Information Agency, September 20, 2016, accessed July 25, 2017, http://news.pia.gov.ph/article/view/2131474293253/-pdea-lauds-sc-for-additional-240-rtcs-to-handle-drug-cases-nationwide

Table 1-31 shows the total preserved assets of drug personalities from 2003 to 2016.

Table 1-31. Total Preserved Assets of Drug Personalities from 2003 to 2016.<sup>40</sup>

Particulars	Amount				
Cash	PhP 489,722,345.78				
Foreign Currency	USD 402,311.22				
	CNY 3,016.76				
Other Assets	68 vehicles				
	4 Firearms				
	28 Parcel of Land				

Table 1-32 shows the number of money laundering cases from 2011 to 2016.

Table 1-32. Cases filed under the AMLA, as amended

Table 1-52. cases med under the AMEA, as amended								
Particulars	2011	2012	2013	2014	2015	2016		
Number of drug-related	3	1	2	5	7	12		
cases subject to Inquiry								
and/or Freeze by AMLC								
Number of criminal cases	17,899	19,908	21,959	17,619	53,481	88,280		
filed for Violation of the								
Dangerous Drugs Act								
prosecuted								
Number of cases filed for	-	3	1	-	1	1		
Violation of the AMLA								
Amount of proceeds	PhP163.69	PhP55.49	PhP64.97	PhP29.77	PhP55.98	PhP6.18		
subject of forfeiture	US\$.181				USD.026*			
proceedings (in millions)	(PhP7.7)				(PhP1.32)			
	CNY.003							
	(PhP.022)							
	Total =							
	PhP171.38							

<sup>\*</sup>as per BSP Website, Exchange Rate: USD=PhP50.698

In 2015, drug-related financial investigations conducted by the AMLC upon referral by LEAs were for violations committed in the NCR. In 2016, investigated cases by the AMLC came from all regions in the Philippines.

From 2011 to 2014, there were 11 drug-related cases which were subjects of freeze and inquiry orders. AMLC received 5 drug-related cases in 2015 and 7 cases in 2016 for financial investigation. Of these, 4 cases in 2015 and 6 cases in 2016 were issued freeze orders on respective bank accounts and properties. The total amount of assets frozen are PhP62,924,530.68 and PhP204,089,294.80, in 2015 and 2016, respectively.

In 2015, there were five (5) civil forfeiture cases pending in courts involving PhP57,306,898.76 worth of various assets while in 2016, there were two (2) civil forfeiture cases filed involving PhP6,182,343.26 worth of various assets. Moreover, in 2016, the court granted the petition by the AMLC to forfeit in favor of the government various properties totaling to PhP10,269,987.67 (RP v. Li Lan Yan, et. al).

-

<sup>&</sup>lt;sup>40</sup>PDEA Annual Report 2016

The AMLC filed one (1) money-laundering case in 2015 and one (1) in 2016, both predicated on Violation of the Comprehensive Drugs Act of 2001.

#### F. Conclusion

It is seen that the fight against the drug problem in the grassroots was strengthened due to increased law enforcement capacity as evidenced by the significant increase in the number of operations against drug trafficking, number of drug cases filed and the value of seizure and confiscations beginning 2015. However, due to these, there is a significant increase in the number of pending drug cases in the courts. Although efforts for additional judicial manpower has been set up in order to sufficiently help in deciding the increasing number of drug related cases, the unclogging of the dockets may not be felt immediately. The conviction rate was seen to be steadily low because of operational lapses in the conduct of drug operations.

In the same vein, although the money laundering investigations predicated on illegal drug cases increased in 2015 and 2016, the same is only about 0.01% of the drug-related cases filed in court in the same period. Moreover, the illegal proceeds from drugs subject of civil forfeiture only amount to about 0.27% of the value of the drugs confiscated in 2015 to 2016. In consideration of the foregoing, the threat posed by the cases of violations of the Comprehensive Dangerous Drugs Act is rated <u>HIGH</u>.

## VIII. Plunder and Violations of the Anti-Graft and Corrupt Practices Act<sup>41</sup>

The Philippines got a score of 35 in the 2016 Corruption Perceptions Index released by global antigraft watchdog Transparency International (TI), same as its score in the 2015 report. But its ranking worsened to 101st out of 176 countries, compared to 95th place out of 168 in 2015. In 2014, the Philippines was ranked 85th out of 175 countries, with a score of 38.

## A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

As observed in the 2009 MER, corruption in the country is widespread and generates substantial illegal proceeds. Corruption in revenue-generating agencies takes a heavy toll on the economy.

#### B. Current Plunder and Graft and Corruption Trend

It is estimated that 20% of the Philippines' yearly national budget is lost to corruption.<sup>42</sup> Following the same pattern and based on the 2015 (PhP2.6 Trillion) and 2016 (PhP3 Trillion) national budgets, about PhP520 to PhP600 Billion were lost to corruption in 2015 and 2016.

The Philippine Revised Penal Code, R.A. No. 3019 or the Anti-Graft and Corrupt Practices Act, R.A. No. 7080 defining and penalizing Plunder<sup>43</sup>, and R.A. No. 6713 or the Code of Conduct and Ethical

<sup>&</sup>lt;sup>41</sup>Violations of Section 3 par. B, C, E, G, H, and I of Republic Act No. 3019 (Anti-Graft and Corrupt Practices Act), as amended, and Plunder under Republic Act No. 7080, as amended, are predicate crimes to ML.

<sup>&</sup>lt;sup>42</sup>Developing a Corruption-intolerant Society (<u>www.ph.undp.org</u>).

<sup>&</sup>lt;sup>43</sup> Under Section 2 of RA No. 7080, as amended, Any public officer who, by himself or in connivance with members of his family, relatives by affinity or consanguinity, business associates, subordinates or other persons, amasses, accumulates or acquires ill-gotten wealth through a combination or series of overt criminal acts as described in Section 1 (d) hereof in the aggregate amount or total value of at least Fifty million pesos (P50,000,000.00) shall be guilty of the crime of plunder and shall be punished by reclusion perpetua to death.

Standards for Public Officials and Employees are the prevailing laws aimed to combat corruption in the country. The Office of the Ombudsman, as the primary agency, and the National Bureau of Investigation are tasked to investigate and prosecute graft and corruption cases involving public officials. Cases against high-ranking officials are brought before the Sandiganbayan, a special anti-corruption court, while cases against low-ranking officials are filed before regional trial courts for trial.

## C. Investigation and Prosecution of Plunder and Graft and Corruption Cases

For the same period, the NBI conducted investigations on the following number of corruption-related cases:

1	Table 1-33. Corruption-related Cases investigated by the NBI							
Year	Plunder	Violation of R.A. No. 3019	Bribery	Malversation				
2015	3	107	1	4				
2016	0	02	1	11				

Table 1-33. Corruption-related Cases Investigated by the NBI

35% of the cases investigated by the NBI involving violation of R.A. No. 3019 in 2015 and 41% of the same cases in 2016 were allegedly committed in the National Capital Region (NCR). Two of the three plunder cases investigated in 2015 and the four bribery cases investigated in 2016 were likewise allegedly committed in the NCR.

In the same years, 2015 and 2016, the statistics of the corruption-related cases prosecuted by the Office of the Ombudsman and the resulting convictions are as follows:

		2015			2016			
Unlawful Activity	No. of Cases Prosecuted (newly filed)	No. of Convictions (newly filed)	No. of Persons Convicted	No. of Cases Prosecuted (newly filed)	No. of Convictions (newly filed)	No. of Persons Convicted		
Plunder	2	0	0	0	0	0		
Violation of R.A. No. 3019	137	24	73	378	62	146		
Bribery	10	1	1	8	3	3		
Malversation	42	21	42	288	29	34		

Table 1-34. Corruption-related cases Prosecuted by the Office of the Ombudsman

For the period 2011 to 2016, cases pending trial before the Sandiganbayan involving high-ranking government officials are as follows:

Table 1-35. Corruption-related cases filed before the Sandiganbayan

Year	Plunder	R.A. No. 3019	Bribery*	Malversation*
2011	1	223	-	-
2012	1	194	-	-
2013	-	521	-	-

Any person who participated with the said public officer in the commission of an offense contributing to the crime of plunder shall likewise be punished for such offense.

2014	14	234	-	-
2015	6	154	10	49
2016	-	402	8	390

<sup>\*</sup>Data for the period 2011 to 2014 was not included in the NRA for said years.

The total workload of cases being heard before the Sandiganbayan as of 31 December 2016 is as follows:

Table 1-36. Cases Heard before the Sandiganbayan

Plunder	R.A. No. 3019	Bribery*	Malversation*
8	2,187	33	863

As of 2016, about PhP689.7 Million is involved in the cases for forfeiture of illicit funds pending before the Sandiganbayan. Out of said amount, about PhP15.7 Million was ordered forfeited in favor of the government in 2016.

#### D. Financial Investigation

From 2011 to 2016, the AMLC conducted the following ML investigations predicated on corruption-related cases:

**Table 1-37. Corruption-Related Money Laundering Investigations** 

Predicate Crime Involved	2011	2012	2013	2014	2015	2016
Violation of R.A. No. 3019	1*	1	4**	9***	11	2
Plunder		-	1	1	1*	1
Bribery						
Malversation						
Total	1	1	5	10	12	3

<sup>\*</sup>The investigation involved both the two predicate crimes of graft and corruption, and plunder.

Ten (10) out of the twelve (12) money laundering cases being investigated by the AMLC in 2015 and two (2) out of the three (3) cases in 2016 are related to the alleged unlawful appropriation and use of the Priority Development Funds (PDAF) funds of subject lawmakers.

Based on the aforesaid investigations, the AMLC filed the following actions:

Table 1-38. Freeze and Confiscation

	2011	2012	2013	2014	2015	2016
Petition for the	1	1	2**	-	1	-
Issuance of Freeze						
Order						
Petition for Civil	1*		-	2	2	-
Forfeiture						
<b>Total Cases</b>	2	1	2	2	3	-
Amount of proceeds	PhP274.24	PhP56.81	PhP18.45	PhP380.85	PhP203.62	
subject of forfeiture	USD1.77	USD.374	USD.055	USD.697	***	
proceedings	EUR.006				USD.385	-
(in millions)						

<sup>\*\*</sup>Three (3) investigations involved the predicate crime of plunder.

<sup>\*\*\*</sup>Six (6) investigations involved the predicate crime of plunder.

All the 15 money laundering cases investigated by the AMLC in 2015 and 2016 involve corruption proceeds approximately amounting to PhP750 Million. For the same period, corruption proceeds subject of civil forfeiture amount to PhP223 Million in funds and properties, but AMLC records show that as of 31 December 2016, about PhP1 Billion in funds and properties are the subject of civil forfeiture cases related to corruption.

The AMLC, the Office of the Ombudsman and the NBI continue to work together in investigating and prosecuting corruption-related cases and money laundering cases predicated on corruption through exchange of information and continued coordination pursuant to the respective Memoranda of Agreements between the AMLC and the Office of the Ombudsman, and the AMLC and NBI.

#### E. Conclusion

The foregoing data on the corruption-related cases investigated and prosecuted for the period 2011 to 2016 show no increasing trend, but the figures remain significantly high. As to the amount of corruption proceeds, about PhP689.7 Million and PhP750 Million are involved in the cases for forfeiture of illicit funds pending before the Sandiganbayan and money laundering investigations of the AMLC, respectively. Moreover, insofar as the 15 money laundering cases are concerned, only 30% of the proceeds of these cases are subject to civil forfeiture. The foregoing considerations provide reasonable bases to retain the <a href="HIGH">HIGH</a> rating of the threat posed by plunder and other corruption-related cases.

#### IX. Web-related Crimes

While violation of the Electronic Commerce Act of 2000 (R.A. No. 8792) was made a predicate offense to money laundering in 2013, cybercrimes under the Cybercrime Prevention Act of 2012 (R.A. No. 10175) have not yet been designated as predicate offense to money laundering.

#### A. Investigation and Prosecution of Web-related Crimes

The NBI investigated the following number of violations of the E-Commerce Act:

Table 1-39. Violations of E-Commerce Act investigated by NBI

Year	Investigated	Prosecuted
2015	9	4
2016	6	-

In addition, the NBI investigated and recommended for prosecution the following violations of the R.A. No. 10175:

Table 1-40. Cybercrime Complaints Received by NBI

20:	15	2016		
Investigated Prosecuted		Investigated Prosecute		
1,123	45	2,005	101	

<sup>\*</sup>Only one case was involved. A petition for civil forfeiture was filed before the expiration of the freeze order issued against the subject properties.

<sup>\*\*</sup>The petition for civil forfeiture was filed in 2014.

<sup>\*\*\*</sup>Includes assessed value of real estate properties and vehicles.

The Anti-Cybercrime Group (ACG) of the PNP received a total of 150 complaints in 2013 relating to violation of R.A. No. 10175, broken down as follows:

Table 1-41. Cybercrime Complaints Received by ACG

Year	No. of Complaints
2013	150
2014	544
2015	1,098
2016	1,937

## **B.** Financial Investigation

For the period 2015 to 2016, there are two cases investigated by the AMLC predicated on violation of R.A. No. 8792, including one of the biggest money laundering case investigated by the AMLC.

Sometime in February 2016, a computer hacking incident was reported resulting in the loss of over US\$80.8 Million from the Bangladesh Bank's account with the Federal Reserve Bank of New York (FRB-NY). It was reported that fraudulent SWIFT Payment Instructions were issued on 04 February 2016 to FRB-NY with instructions to transfer money to a Philippine bank through the latter's correspondent banks in the United States.

On 15 February 2016, the Governor of Bangladesh bank sought assistance from the Bangko Sentral ng Pilipinas (BSP) Governor to trace, freeze and recover the transferred funds. The matter was referred to the AMLC, which is also chaired by the BSP Governor. The AMLC Secretariat conducted an investigation and confirmed that the funds were indeed transferred to accounts in a Philippine bank which were opened using spurious and fake identity documents. Investigation disclosed that a money remitter facilitated the transfer of funds of approximately US\$80.8 Million or PhP3.8 Billion from the questionable bank accounts to the bank accounts of: (a) a casino; (b) a casino junket operator; and (c) an inexistent individual.

On 01 March 2016, upon petition by the AMLC, the Court of Appeals issued a freeze order on the known bank accounts of the recipients of the stolen funds. One of the funds' recipients, a casino junket operator, volunteered to return approximately US\$15 Million to the government of Bangladesh through its embassy in Manila.

On 18 April 2016, the AMLC filed a Petition for Civil Forfeiture before the Regional Trial Court in Manila for the recovery of the stolen funds including the US\$15 Million that was voluntarily returned. Insofar as the surrendered funds, upon motion of the AMLC, an Order of Partial Judgment was issued by the court on 07 July 2016.

On 16 September 2016, the court allowed the Bangladesh government, through the Philippine Department of Justice, to intervene in the civil forfeiture case and file a claim on the forfeited US\$15 million in funds. The funds were eventually released in favor of the Bangladesh government on 10 November 2016.

From 11 March 2017 to 27 April 2017, the AMLC filed criminal complaints for money laundering, predicated on the violation of the e-commerce law, i.e. hacking, against the bank official, several John Does and the owners of the money remittance company. On 18 November 2016, an additional complaint for money laundering was filed against the senior officials of the Philippine bank which received the stolen funds.

Considering that violation of R.A. No. 10175 is not yet a predicate offense to money laundering, there is likewise no money laundering investigation done predicated thereon.

#### C. Conclusion

Although the country was taken by surprise by the attack against a central bank, the amount stolen and use of established financial institutions abroad and in the country to divert the stolen funds, the case also highlighted the readiness and capacity of law enforcement authorities to act promptly and appropriately in the aftermath of such an attack, as well as coordination efforts of agencies concerned, both local and foreign. All taken together, a **MEDIUM** rating for the threat posed by web-related crimes is justified.

#### X. Trafficking in Persons

## A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

In 2008, the US Department of State (US-DOS) report the Philippines as part of the "Tier 2"<sup>44</sup> group of countries with respect to the scope and nature of the phenomenon. While compared to 2001 the country has remained in the same Tier, across 2004-2005 the situation had been deteriorating, with the Philippines being demoted from Tier 2 to Tier 2's "watch list". The last three years have seen the country back again into Tier 2, but several elements suggest that it is vulnerable to human trafficking.<sup>45</sup>

## **B.** Current Trend in Trafficking in Persons

In June 2016, the US-DOS has reported that the Government of the Philippines fully meets the minimum standards for the elimination of trafficking. The report mentioned that the government convicted 42 traffickers, including five for online child sex trafficking and two for forced labor. Although pervasive corruption undermined efforts to combat trafficking, the government convicted two immigration officers and charged five officials allegedly complicit in trafficking. On this strength, the Philippines was removed from the Tier 2 List and included in the Tier 1 List. The Philippine government is now considered to have fully met the US Trafficking Victims Protection Act's (TVPA) minimum standards.

According to the 2016 SOCTA, the Department of Social Welfare and Development (DSWD) claimed that the following are the usual nature of human trafficking complaints they receive: offer of high-paying jobs abroad; use of fake visas, marriage certificates, and other spurious travel documents to facilitate exit from the country; and, the enticement of parents to allow their young daughters to leave the province and work in Manila as domestic helpers, with promises of huge salaries, but then they end up doing jobs other than what was promised.<sup>47</sup>

Consolidated statistics sourced from PNP and NBI indicate that there were at least 859 trafficking cases filed from 2010 to 2015. It can be gleaned from both the PNP and NBI data that there was a downward trend of trafficking cases from 2011 (with 193 cases combined) to 2014 (with only 128 cases).

<sup>46</sup> P.307, Trafficking in Persons Report, June 2016, US-Department of State,

<sup>&</sup>lt;sup>44</sup> Tier 2 countries are Countries whose governments do not fully meet the TVPA's minimum standards, but are making significant efforts to bring themselves into compliance with those standards.

<sup>&</sup>lt;sup>45</sup> P.23, par. 99, 2009 Philippines MER

<sup>&</sup>lt;sup>47</sup>2016 SOCTA citingUnited Nations Office on Drugs and Crime, Human Trafficking Report 2015, accessed April 2, 2016, https:// www.unodc.orgfunodc/en/human·trafficking/faqs.html. International Labour Organization, Profits and Poverty: The Economic of Force Labour, May 20, 2014, accessed April 02, 2014

Moreover, 2015 likewise recorded a lower number of TIP cases, with the PNP-Criminal Investigation and Detection Group (CIDG) reporting eight cases from January to July; 22 for the PNP Women and Children Protection Center (WCPC) from, June to December; and, the NBI with 29 cases for the first' semester of the year. It should be noted that the WCPC assumed CIDG's jurisdiction over TIP cases starting June2015, as per National Police Commission (NAPOLCOM) Resolution No. 2014-441, signed on January 23,2015.<sup>48</sup>

Furthermore, of the TIP cases handled by the NBI in 2015 and 2016, more than 85% were committed in the NCR, followed by Regions III and VII.

Finally, the 2016 Global Slavery Index estimates that 45.8 million people are subject to some form of modern slavery in the world today. Based on the ranking of 167 countries with estimated prevalence of modern slavery the Philippines ranked 33<sup>rd</sup>, which is a slightly improved rating from its previous rank (29<sup>th</sup>) in 2014.<sup>49</sup>

## C. Investigation and Prosecution of TIP cases

According to the 2016 SOCTA, as to the prosecutorial part of the intensified government efforts, on 7 December 2015, Inter-Agency Council Against Trafficking (IACAT) reported that there were already 197 convictions with 220 convicted personalities from 2010-2015. The increase of convictions from 2010 may be due to the issuance of DOJ Circular No. 57, which orders the prioritization of the resolution of trafficking cases and thwart any deferral in the prosecution of such cases.

Table 2 121 Consolidated Hamber of the Gases Hamarica by the fitt and test							
Year	Number of TIP Cases handled by PNP and NBI	Number of Convictions	Number of Persons Convicted				
2011	193	25	32				
2012	194	27	32				
2013	133	27	37				
2014	128	55	57				
2015	59	45	46				
TOTAL	707	179	204				

Table 1-42. Consolidated Number of TIP cases Handled by the PNP and NBI

While the number of TIP cases handled by the PNP and NBI in 2015 is merely 36% of the average annual number of cases handled in 2011-2014<sup>50</sup>, the prosecution efforts managed to obtain verdicts of conviction yielding to 134% of the average annual number of convictions in 2011-2014.

#### D. Financial Investigation

For the period 2015-2016, the AMLC was able to file a petition for civil forfeiture of illicit funds arising from trafficking in persons amounting to approximately PhP11.4 Million. The filing of the civil forfeiture and other ML-related cases were initiated following the cooperation and coordination between the AMLC and other LEAs concerned, as well as in part request for assistance from a foreign jurisdiction. The domestic cooperation also resulted in the arrest and indictment of perpetrators for violation of the Anti-Trafficking in Persons Law.

-

<sup>&</sup>lt;sup>48</sup> 2016 SOCTA

<sup>&</sup>lt;sup>49</sup> www.globalslaveryindex.org

<sup>&</sup>lt;sup>50</sup> The average annual number of TIP cases handled by the PNP and NBI in 2011-2014 is equivalent to 162.

#### E. Conclusion

Considering the high number of convictions in 2015 equivalent to 134% of the average annual number of convictions in 2011-2014, as well as the upgrade of the Philippines from Tier 2 to Tier 1 category in a review exercise conducted by the US-DOS, implying that the Philippines have fully met all the minimum standards for the elimination of trafficking plus the improvement in the ranking of the Philippines in a study conducted by the Global Slavery Index, the threat of human trafficking is downgraded to **MEDIUM**.

#### XI. **Kidnapping for Ransom**

## A. 2<sup>nd</sup> Mutual Evaluation Report (2009 MER)

Kidnapping is a serious issue in the Philippines. The crime is used both as a source for income for criminal groups, and as a source for funds by armed groups acting against the government. Renegade elements of the Moro Islamic Liberation Front (MILF) and members of the Abu Sayyaf Group (ASG) have often engaged in kidnapping to fund operations and general logistical expenses.<sup>51</sup>

#### Current Trend in Kidnapping for Ransom (KFR)

Based on the Global Kidnap Review 2016<sup>52</sup>, the NYA International Crisis Prevention and Response<sup>53</sup> classified the Philippines as "High Threat Country" and was considered as the Southeast Asia's top kidnapping hotspot. Moreover, the Review mentioned that the Philippines' kidnap threat extends nationwide with higher threats apparent in Manila as well as in Mindanao and Sulu. Insurgent and extremist groups such as the ASG and New People's Army use kidnappings to achieve political motives or fund terrorist operations. While the vast majority of kidnap victims are domestic nationals, the ASG particularly targets foreign nationals for substantial ransom payments.

The scope of the threat assessment on kidnapping for ransom, however, does not include kidnapping committed by the ASG and other local threat groups. This is assessed separately under Chapter IX, Terrorism and Terrorism Financing Threats.

## C. Investigation and Prosecution of KFR Cases

Based on the data provided by the PNP-DIDM, Regions 13, CAR, 8 and 3 had the most number of KFR incidents for the period 2015-2016. On the other hand, the PNP-AKG had investigated thirty-one (31) KFR cases from 2014-2016 involving a total estimated proceeds equivalent to PhP26.5 million pesos.

Table 1-43 illustrates the number of KFR cases handled and investigated, and prosecuted by the PNP from 2012-2016.

Table 1-43. KFR Cases reported by the PNP-AKG

OFFENSE		YE	AR	
Kidnapping for Ransom Under Article 267 of Act no.3815	2014	2015	2016	TOTAL
No. of Cases Reported & Investigated	9	11	11	31

<sup>&</sup>lt;sup>51</sup> P.23, par.97, 2009 Philippines MER

<sup>&</sup>lt;sup>52</sup>w<u>ww.nyainternational.com</u>

<sup>&</sup>lt;sup>53</sup> NYA International is a leading global risk and crisis management consultancy. It produces a range of monthly, quarterly and incident-specific situation reports covering both land-based and maritime security events.

No. of Cases Prosecuted	6	9	9	24
No. of Convictions(Cases)	0	1	0	1
No. of Persons Convicted	0	3	0	3
Estimated Proceeds Involved in the	12.57	46.99	26 AFMillion	26.51
Crime (Ransom Paid)	Million	Million	26.45Million	Million

Source: PNP-AKG

It appears that from 2014-2016, 77% of the total number of KFR cases investigated were filed for prosecution and only 4% of which have resulted into subsequent conviction. Most of the cases are either pending for trial or otherwise submitted for resolution by the court.

#### D. Financial Investigation

In July 2016, the AMLC obtained a verdict of conviction against an accountholder in whose bank account was deposited the ransom money from Tokyo, Japan and facilitated the offense of money laundering by knowingly transacting the proceeds of the unlawful activity of KFR through daily withdrawals. It appeared that the funds originated from the family of the victim. The money laundering investigations led to the filing of a civil forfeiture proceedings amounting to PhP2.6 Million.

#### E. Conclusion

The statistical data provided by some of the concerned agencies are incomplete for it did not provide the number of KFR cases handled in some regions. Nevertheless, the prevalence of KFR is undeniable and apparently would involve substantial amount of ransom money. However, taking into consideration the good number of cases elevated for prosecution and the recent conviction for laundering proceeds derived from KFR, this predicate offense is rated **MEDIUM**.

#### XII. Other Unlawful Activities/ Predicate Offenses

## A. Investigation and Prosecution of Other Unlawful Activities

The NBI provided the following data on the following crimes:

Table 1-44. Cases reported by the NBI

Table 1 : it dates reported by the res						
Unlawful Activities	20	)15	2016			
Offiawful Activities	Investigated	Prosecuted	Investigated	Prosecuted		
Violation of Migrant Workers and Overseas Filipinos Act (R.A. 8042)	4	38	21	29		
Qualified Theft	235	79	185	64		
Arson	23	2	20	3		
Carnapping	100	30	103	24		
Gambling and Betting	107	60	51	30		
Frauds and Illegal Exaction	429	15	403	18		
Robbery and Extortion	311	59	247	44		
Murder	627	136	625	118		
Forgeries and Counterfeiting	56	2	43	4		
Violation of the Anti-Fencing Law (P.D. 1612)	4	1	-	-		

Violation of the Anti-Photo and Video Voyeurism Act (R.A. 9995)	73	3	156	8
Violation of the Anti-Child Pornography Act (R.A. 9775)	4	-	8	1
Violation of R.A. 7610 (Child Abuse)	193	77	175	58

Additionally, the PNP provided the following data on arson, carnapping, hijacking, jueteng and masiao for the years 2014 to 2016.

Table 1-45. Cases reported by the PNP

	201	2014		2015		2016	
Unlawful Activity	No. of Cases Investigated	No. of Cases Prosecuted	No. of Cases Investigated	No. of Cases Prosecuted	No. of Cases Investigated	No. of Cases Prosecuted	
Destructive							
Arson	4	0	4	0	14	3	
Carnapping	8,916	956	3,247	539	8,188	1,604	
Hijacking	24	1	21	5	7	2	
Jueteng and							
Masiao	655	655	1,028	1,028	1,341	1,341	

#### **B.** Financial Investigation

Financial investigation resulted to the following:

- a. Freezing of bank deposits amounting to PhP3,761,046.12 in the case predicated on illegal recruitment;
- b. Filing of a money laundering complaint against the alleged perpetrator of money laundering in the case predicated on qualified theft; and
- c. Conviction for 29 counts of money laundering with imposition of PhP1.5 Million penalty in another case predicated on qualified theft

#### C. Conclusion

Taken individually, the number of investigations involving the foregoing crimes is less significant. Also, the foregoing crimes, by their nature, do not produce significant proceeds. In fact, in the money laundering cases investigated by the AMLC predicated on illegal recruitment and qualified theft identified above, the criminal proceeds involved totaled to PhP5.2 Million. As such, the foregoing offenses, individually, is rated **LOW**.

## **SECTOR THREAT ANALYSIS**

For the period 2015 to 2016, the AMLC investigated forty-nine (49) money laundering cases, which served as the bases in assessing sectoral treat. These money laundering cases are predicated on nineteen (19) illegal drug cases, fifteen (15) corruption-related cases, five (5) estafa cases, four (4) trafficking in persons cases, two (2) cases involving qualified theft, and one (1) case each involving kidnapping, illegal recruitment, violation of the e-Commerce Act, and violation of the SRC.

#### 1. Banks

As of 2016, 82% of the covered persons registered with the AMLC and 98% of the covered and suspicious transaction reports received by the AMLC come from institutions supervised by the Bangko Sentral ng Pilipinas. All the 49 money laundering cases investigated by the AMLC involving about PhP5.9 Billion used bank accounts in the money laundering scheme.

Common to the 19 cases involving illegal drugs is the use of banks to launder proceeds of illegal drug trade by depositing the same to different bank accounts to facilitate payment or for temporary safekeeping. In said 19 money laundering cases, about 929 bank accounts in 17 universal and commercial banks, 3 thrift banks, 4 rural banks, and 3 savings and loan associations were used to launder an estimated amount of PhP950 Million proceeds of illegal drug trade.

In the 15 money laundering cases predicated on corruption-related cases, 377 bank accounts were used to divert public funds approximately amounting to PhP750 Million from the government coffers to the hands of corrupt public officials and their cohorts by scheming to have public funds deposited and transferred to bank accounts of controlled dummies and later withdrawing the same. Said accounts were opened and maintained in 18 universal and commercial banks and one thrift bank.

The proceeds of the five estafa cases mentioned above approximately amounting to PhP231 Million were laundered using 38 bank accounts in six universal and commercial bank accounts. The scheme varies as follows: a) deposit and withdrawal of checks drawn payable to a government agency to and from the personal account of one of the subjects; b) deposit of funds to one bank account, transfer to another and subsequent withdrawal of the funds; c) creation of dummy corporations appearing to be dealing with one another obtained loans based on fraudulent documents and proceeds of the scheme are wire transferred to bank accounts in the Philippines; d) funds obtained from investors are deposited to bank accounts, pooled therein and used to pay investors following a *ponzi* scheme; and e) bank uses its own funds to cover the amount of the check drawn payable to the bank itself to accommodate the borrowers who issued the checks as payment for loans.

In the four cases involving illegal trafficking of persons, victims were forced to engage in sexual acts producing photos and video footages that were later on uploaded in various websites. Viewers pay to see the photos and videos and payments were made through fund transfers. Proceeds of the four cases approximately aggregated to PhP20.2 Million were coursed through 12 bank accounts in one universal bank, one thrift bank, and two rural banks.

Approximately PhP11 Million were laundered using 25 bank accounts maintained in six universal and commercial banks and one rural bank in the two cases of qualified theft investigated by the AMLC.

In one of the biggest case of money laundering, unauthorized SWIFT Payment Instructions from Bangladesh Bank approximately amounting to PhP3.8 Billion were cleared and credited to four dummy accounts in one of the biggest universal banks in the country. Investigation disclosed that a money remitter facilitated the transfer of said funds to the bank accounts of a casino, casino junket operators and inexistent individuals. Investigation covered 39 bank accounts in five universal and commercial banks. Officers of one of the universal banks involved are currently facing charges of money laundering before the DOJ.

In the kidnapping case, approximately PhP2.6 Million was laundered through remittance of said funds using two bank accounts maintained in two universal banks. In the illegal recruitment case, approximately PhP112,000.00 was deposited and transacted using six bank accounts in two universal banks. And, in the SRC violation case, PhP200 Million was used to perpetuate market price

manipulation using 40 bank accounts in 6 universal and commercial banks and one thrift bank in effecting payments and settlements of trading transactions.

In the foregoing cases, approximately PhP5.9 Billion was laundered using over 1,500 bank accounts in 21 universal and commercial banks, 4 thrift banks, and 6 rural banks. Currently, bank deposits aggregating PhP822,635,461.00 are the subject of several civil forfeiture cases.

In 141 requests for information (RFIs) from counterpart FIUs and 12 MLAT requests from foreign jurisdictions, over PhP500 Billion were allegedly coursed through bank accounts.

It must be noted, however, that the amount of PhP5.9 Billion criminal proceeds from the 49 money laundering cases investigated by the AMLC in 2015 and 2016 translates to only .056% of the total demand deposits or .042% of the total assets of the banking industry in 2016. Further, the PhP500 Billion criminal proceeds involved in the 141 RFIs from counterpart FIUs and 12 MLAT requests from foreign jurisdictions received by the AMLC in 2015 and 2016 translates to only 4.7% of the total demand deposits or 3.6% of the total assets of the banking industry in 2016.

Nonetheless, although the criminal proceeds involved in the money laundering cases and related predicate offenses translate to a minimal percentage of the total assets of the banking industry, the cases clearly showed that continuous use of banking products and facilities and money service businesses in laundering proceeds of unlawful activities; hence, the threat rating for banks and money service businesses remains **HIGH.** 

## 2. Money Service Businesses (MSB)

Perpetrators of illegal drug trades investigated by the AMLC used 15 remittance companies and foreign exchange dealers, maintaining about 12 bank accounts, to facilitate movements of funds intended as payments for the illegal drugs. In the same manner, perpetrators of illegal sex trade through the web, as investigated by the AMLC, used two remittance companies to pay for access on the sex-oriented photos and videos uploaded on the web by criminals. And, in the case of the Bangladesh Bank heist, the transfer of PhP3.8 Billion from the dummy bank accounts to casinos, junket operators, and inexistent persons was facilitated by three remittance and foreign exchange companies. Officers of the remittance company are now facing charges for money laundering before the DOJ.

In 141 requests for information from counterpart FIUs and 12 MLAT requests from foreign jurisdictions, over PhP90 Billion Pesos were allegedly coursed through money service remittance businesses.

The foregoing showed how MSBs were used extensively to move illicit funds warranting a **HIGH** rating.

## 3. Designated Non-Financial Businesses and Professions (DNFBPS)

For the period 2015 to 2016, no dealers in precious stones and metals, lawyers and accountants were detected to be involved in money laundering cases. No covered or suspicious transaction reports were received from the sector. Neither did financial investigations resulted to any finding pointing to the sector to have been used to launder criminal proceeds. There is however and evident lack of data with respect to the said businesses and professions as they remain unregulated for AML purposes even if they are included as covered persons since 2013. Hence, no compliance checking has been conducted, nor were there any covered or suspicious transactions filed by the said business and professions.

With respect to the real estate sector, about PhP55 Million worth of real estate properties are currently the subject of civil forfeiture cases, which indicates that purchase of real properties have been used by criminals to launder criminal proceeds.

Focusing on casinos, about PhP3.8 Billion stolen funds ended up with two casinos and one junket operator as follows: a) about PhP1.36 million was transferred through intra-bank fund transfer to one casino; b) about PhP1 Billion was transferred to another casino through inter-bank fund transfer; and c) about PhP1.44Billion was delivered in cash and in tranches by a remittance company to a junket operator. Identified junket operators who received part of the stolen funds were charged of money laundering offenses before the DOJ.

Considering the amount of criminal proceeds that were laundered through DNFPBs, more particularly, casinos and casino junket operators and the absence of clear regulations on DNFPBs during this time that allowed casinos to be used to perpetrate the crime and prevented authorities to follow the flow of the stolen funds for recovery, the threat rating for DNFPBs is **HIGH**.

## 4. Non-Profit Organization (NPO)

In the twelve (12) corruption-predicated money laundering cases investigated by the AMLC in 2015 to 2016, 21 non-government organizations were used as dummies to funnel about PhP420 Million government funds in favor of criminals. Further, intelligence information shows that NPOs are being used in financing terrorist activities. Furthermore, no uniform regulation governing the operations of no-profit organizations is in place, necessitating an in-depth study to determine extent of vulnerability of the sector to money laundering and terrorist financing. Considering the foregoing, the threat rating for NPO is **HIGH**.

#### 5. Securities Sector

As of 2016, only 12% of the registered covered persons with the AMLC and only 1.47% of the covered and suspicious reports come from the securities sector.

As of 2016, the SEC investigated a total of 743 cases involving violations of the SRC, including pyramiding scheme. In one case investigated for laundering of proceeds of violation of the SRC involving about PhP200 Million, 41 accounts in eight broker-dealers were used to perpetrate market price manipulation. The mastermind funded the trading of shares of his own corporation and used dummy accounts with broker-dealers to control the purchases and sales of the shares, thereby achieving artificial trading activity and driving the price of the stocks higher.

In another case, predicated on plunder, the subjects used the securities industry to hide proceeds of their unlawful activity. Shares of stocks worth PhP44,116,578.66 is currently the subject of civil forfeiture proceedings.

The total criminal proceeds identified to have been laundered through the securities industry translate to about .0023% of the total assets of the security industry in 2015.

Although investment-related scams seem to continue to proliferate, the extent the security industry and securities products used in money laundering is not widespread; hence, the threat rating for the Securities sector is **MEDIUM**.

#### 6. Insurance Sector

As of 2016, only 6% of the registered covered persons with the AMLC and only 0.53% of the covered and suspicious reports come from the insurance sector.

In three cases predicated on illegal drugs and one case predicated on estafa, insurance products offered by at least three insurance companies were used to hide the proceeds of their unlawful activity. Close to PhP3 Million is currently subject of civil forfeiture proceedings. This figure is only about .0023% of the total assets of the insurance industry in 2015. Considering the limited use of the insurance industry and insurance products in laundering criminal proceeds, the threat rating for the insurance sector is **MEDIUM**.

#### THE LEVEL OF EXTERNAL THREAT

It is a declared policy of the State to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity, among others. Accordingly, the State extends cooperation in transnational investigations and prosecutions of persons involved in money laundering activities wherever committed. Undeniably, any attempt to transfer criminal proceeds generated abroad into the territory of the Philippines would augment money laundering threats in the country.

#### **Proceeds from Abroad**

In 2015 and 2016, the AMLC received a total of one hundred fifty-three (153) requests for information and assistance from other jurisdictions, including twelve (12) requests for mutual legal assistance. The requests basically contain allegations that illicit funds derived from various offenses committed within the respective territorial jurisdictions of the requesting countries were transferred or probably transferred, in whole or in part, in the Philippines.

In 2015 and 2016, about 35% and 28%, respectively, of the requests are related to various forms of fraud as the source of criminal proceeds. The following table shows topmost offenses as subject of requests.

Table 1-46. Topmost Offenses as Subject of Requests

		2015		2016		
Number of		68		85	) )	
requests received	Offenses	Number of requests	%	Offenses	Number of requests	%
Most number of	Fraud	24	35%	Fraud	24	28%
offenses involved	Drugs	8	12%	Scam	3	4%
	Tax Evasion	5	7%	Terrorism	3	4%
				Theft	3	4%
				Underground Banking	3	4%

On the other hand, the requests received in 2015 involve illicit funds amounting to more than PhP13 billion and in 2016, more than PhP595 billion. In 2015, 72% of the criminal proceeds were generated from fictional entrepreneurship and tax evasion, while in 2016, 85% of the illicit funds were proceeds of fraud. The tables below show the topmost offenses as sources of illicit funds from abroad.

Table 1-47. Topmost Offenses as Sources of Illicit Funds

	2015			20	16	
Total amount	PhP13	Billion		PhP595	billion	
of illicit funds	Offenses	Offenses Amount (PhP) %		Offenses	Amount (PhP)	%
Topmost offenses as sources of	Fictional Entrepreneurship , Tax Evasion	9.6 billion	72%	Fraud	508 billion	85%
illicit funds	Fraud	2.5 billion	18%	Narcotics	75 billion	13%
	Investment Scam	4.15 million	5%	Embezzlement Of Private Funds	5 billion	1%

**Table 1-48. Source Countries of the Illicit Funds** 

	2015			2016			
Total amount		PhP13 billion		Pl	PhP595 billion		
Total amount of illicit funds	Country	Amount (PhP)	%	Country	Amount (PhP)	%	
Top countries	Kazakhstan	9.6 billion	72%	Indonesia	75 billion	13%	
of origin	USA	2.3 billion	17%	USA	6 billion	1.06%	
	Belgium, HongKong	590 million	4%	Switzerland	5 billion	0.84%	

In 2015 and 2016, the United States of America (USA) has consistently been one of the topmost sources of illicit funds from abroad accounting for 17% and 1.06% of the illicit funds flowing to the Philippine, for 2015 and 2016, respectively. The following table shows the topmost countries of origin of illicit funds and the amount of proceeds involved.

With these identified countries of origin, the proceeds were derived from the following offenses:

Table 1-49. Countries of Origin of the Proceeds

		2015				.6
Total		PhP13 bil	lion		PhP595	billion
amount of illicit funds	Country	Offense	Amount (PhP)	Country	Offense	Amount (PhP)
Top countries of origin	Kazakhstan	Fictional entrepreneurshi p, tax evasion	9.6 billion	Indonesia	Hijacking/ KFR	1 million
	USA	Bribery, graft	5 million		Hacking of bank accounts	126 thousand
		Drugs	255.4 million	USA	Drugs	75 billion
		Fraud	2 billion		Fraud	533 million
	Belgium,	Investment	590 million	Switzerland	Theft	5.25 million
	HongKong	scam			Tax cases	153 million
					Money Laundering	112 million
					Embezzlement of private funds	5 billion

The transactions of these criminal proceeds were predominantly undertaken by abusing the vulnerabilities of various financial sectors. In 2015 and 2016, about 98% and 70%, respectively, of the sectors involved in the inflow of illicit funds include banks. Money remittance businesses and securities trading participants were also among those mostly resorted financial sectors.

In spite of strict banking regulations, it appears that 90% and 85% of the inflow of dirty money in 2015 and 2016, respectively, were transferred or otherwise transacted using bank accounts and other products offered by the banking industry. The remaining 10% to 15% was coursed through remittance agents and foreign exchange dealers. The banking sector appears to have been more exploited as compared to remittance agents and foreign exchange dealers owing to the volume of dirty money involved and the wider selections of financial products and services offered by banks.

## A. International Rankings

In 2014, "The Basel AML Index-Country risk ranking" overall score of the Philippines is 6.39 (from [0] low to [10] high risk), which is a Medium High risk country for money laundering/terrorist financing. The rating slightly improved in 2015 and 2016 garnering 6.4 and 6.31 ratings, respectively. The Basel AML Index assesses countries' adherence to AML/CTF standards, their perceived level of public corruption, financial transparency, political financing, judicial strength and other relevant indicators. By combining these various data sources, the Basel AML Index score represents a country's overall risk level or vulnerability regarding money laundering and terrorist financing.

#### **B.** Financial Investigation

Within the assessment period, the AMLC investigated money laundering cases involving proceeds allegedly derived from estafa, trafficking in persons, kidnapping for ransom and violation of E-Commerce Act cases sourced from abroad. These cases involve a total amount of more than PhP902 Million of illicit funds from other jurisdictions. About 53% of this total amount or PhP481 millions relate to estafa case and has been ordered by the court forfeited upon petition filed by the AMLC. On the other hand, the court promulgated a verdict of conviction in a money laundering complaint filed by the AMLC against persons who facilitated the transaction of ransom money.

Considering the number of RFI and MLAT requests and the amount involved in the requests approximately aggregating to PhP608 Billion point to the inevitable conclusion that the Philippines faces <u>HIGH</u> external treat to be used as venue for money laundering.

#### **OVERALL NATIONAL RISK**

All the foregoing showed the prevalence of predicate offenses and the proceeds they generate, the money laundering schemes employed by criminals and the extent covered persons and products and services in the country's various financial sectors were used in the schemes. Accordingly, the national money laundering threat is assessed as **HIGH**.

## **ACTION PLAN**

The result of the assessment show that the risk posed by crimes involving illegal drug trade, corruption, fraud, smuggling, IPL violations, violations of environmental laws, violations of the e-Commerce Act and cybercrimes, illegal manufacture and possession of ammunitions and firearms and kidnapping for ransom is high. Accordingly, there is a need for a closer coordination and cooperation

between the AMLC and the respective LEAs authorized to investigate and/or prosecute said unlawful activities. In addition, LEAs involved in the risk assessment must be encouraged to maintain statistics specifically needed in conducting the threat analysis to eliminate the challenge in data collection faced in the previous and current assessment. Thus, the following actions are recommended:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Obtain commitment of relevant government agencies to collect data as to proceeds of crimes involved in their respective agencies.  Frequent bilateral coordinationworkshop between AMLC and other relevant LEAs to accomplish the following, among others:  a. Execute/Revisit MOA;  b. Update on applicable laws and relevant work procedures;  c. Appoint technical focal persons;  d. Establish AML Desk;	AMLC BIR BOC IPOPHIL PNP-CIDG DENR SEC PDEA OMB		January 2018 onwards  September 2017: I.SEC II.OMB III.PDEA October 2017: BOC
e. Strategic referral of cases to AMLC for possible money laundering	NBI DOJ PNP-AKG		November 2017: CIDG
investigation; f. Inventory, update of status and strategize the handling of cases;	PAGCOR		November 2017: NBI
g. Synthesize the gathering of data requirements, specially the proceeds of crime;			Other agencies- January 2018 onwards
h. And other relevant matters.			5.1144143
Initial coordination-workshop			

The sectoral threat assessment likewise showed that the sectors involving banks and other financial institutions supervised by the BSP and DNFPBs are the more prevalent venues used by criminals to launder criminal proceeds warranting **HIGH** ratings, respectively. Based on the same assessment, the Securities and Insurance Sector have been used as venues for money laundering in limited terms; hence, the **MEDIUM** rating. Moreover, the threat coming from proceeds of crimes committed outside of the country's territory was rated **HIGH**. The foregoing ratings may be attributed to the use of the products and institutions in said sectors in laundering criminal proceeds, both from internal and external sources, in the money laundering schemes of criminals identified above. To aid in forestalling possible repetitions of these schemes, the following courses of actions are recommended:

ACTION PLAN	PRIMARY AGENCY	TIMELINE
Require covered persons to conduct enhanced profiling of clients focused on: a) beneficial ownership and legal existence; b) transaction patterns in the same account and in various related accounts; and c) financial capacity and relations of parties to transactions involving huge amounts of funds.  Require covered persons to closely monitor and conduct enhanced due diligence on accounts holders whose accounts exhibit the following behavior or patterns: a) use of bank account as temporary repository of huge amounts of funds or as a pass-thru account; and b) deposit and immediate withdrawal of huge amounts of funds in cash.  Provide a venue for covered persons and supervising authorities to share observed money laundering trends and typologies.  Study how to facilitate sharing of client information among covered persons across the different sectors, subject to prevailing rules on confidentiality.	AMLC BSP SEC IC PAGCOR CEZA APECO	First Quarter of 2018
Conduct an in-depth study/risk assessment to determine vulnerability of the NPO sector to money laundering and terrorist financing.	AMLC, SEC, DWSD, PCNC, CDA	December 2017

#### II. NATIONAL VULNERABILITY

#### **EXECUTIVE SUMMARY**

The threat of money laundering (ML) and terrorism financing (TF) has drawn importance and understanding globally. As the threats and its opportunities are being identified, the vulnerability to money laundering continues to increase thereby affecting the country's ability to combat it. There are many anti-money laundering (AML) controls that contribute to the combating ability of a country against money laundering and terrorist financing. Some of the controls have direct impact while others depend on the existence of other ML combating controls. For example, in order to determine the quality of CDD framework, the AML controls or factors *Availability of Reliable Identification Structure, Independent Information Sources, Access to Beneficial Ownership Information must be first assessed and rated.* 

The AMLC, Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), and the Insurance Commission (IC), and other competent authorities and agencies recognize that sustained and continuing efforts are needed to further improve effectiveness in the implementation of the AML/CFT rules and regulations. The AMLC, BSP, SEC, and IC need to address the gaps identified in sector vulnerability assessments particularly in the enforcement of AML/CFT rules on their respective supervised covered persons. This will require the adoption of a more effective AML monitoring systems and mechanisms and further enhancements on the customer due diligence (CDD) frameworks, focusing more on the availability of independent information sources and more reliable identification infrastructure. While the country has yet to implement a national identification system, the supervisors BSP, SEC, IC and the AMLC, and covered persons rely on available Independent information sources such as credit bureaus, and identification infrastructure systems (LTO ID, Postal ID, PRC ID systems, among others) in the conduct of verifying historical and transactional patterns of their clients.

Tax records and information on the management, control and beneficial interests in corporations are still not currently readily available to the regulator and to AML-regulated entities.

Further, not all customs officials stationed at various ports monitor and submit information on cases pertaining to smuggling of goods, arms, etc., including smuggling of cash, precious metals and stones. The AMLCS, so far receives referrals from other LEAs, insofar as investigation for ML is concerned. Records also show that customs office stationed in NAIA regularly submit customs declaration forms to the AMLC. Other major airports like those in Cebu and Davao do not, rendering the government incapable of coming up with reliable data on the amount of cash being declared, their sources and destination and nationalities of those who do so.

#### **INTRODUCTION**

In 2016 alone, the country faced major threats of money laundering (ML) and terrorism financing (TF) predicated from high-profile offenses such as drug trafficking, kidnap for ransom, violations of the E-Commerce Act, and terrorism. The penetration of these threats tested the capability of the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) systems of financial institutions (FIs) and designated non-financial businesses and professions (DNFBPS) to deter these risks.

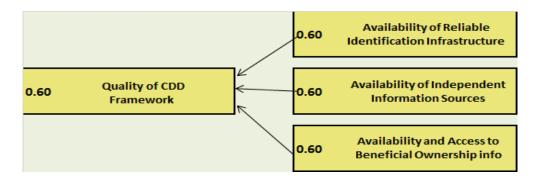
The growing threat of ML/TF has gained recognition and understanding in both domestic and international context. In order to effectively combat this threat, there is a need to identify the weaknesses and gap's in the country's ability to combat ML/TF and identify the vulnerability of the different sectors. This Section intends to assess our national vulnerability to ML/TF, with respect to

ability of the different sectors under this assessment to combat the same. This will enable the country to prioritize actions that will improve the national combating ability by strengthening AML controls at the national level.

In the previous NRA, one of the major concerns was the level of informal economy<sup>54</sup>. The Office of the President's issuance of the Executive Order (EO) No. 208 on 02 June 2016 to create the Financial Inclusion Steering Committee (FISC)<sup>55</sup> intends to address the need of the low income sector. The FISC, as the governing body, shall (i) provide strategic direction, guidance and oversight in the NSFI implementation which was developed through a consultative process; and (ii) serve as a pillar for public and private sector stakeholders to systematically accelerate financial inclusion in the Philippines.

Another factor that needs to be addressed in the previous NRA is the analysis of Suspicious Transaction Report (STR) data. The number of quality STRs referred to the Compliance and Investigation Group, the investigative arm of the AMLC Secretariat, is another aspect that needs be to be improved upon. In the 2<sup>nd</sup> NRA, the focus is on the quality of FIU intelligence gathering which includes the assessment of effectiveness of triggering and supporting ML/TF investigation through the collection, analysis and dissemination of STRs and CTRs deemed suspicious. In the 2009 MER, one of the deficiencies noted was the inadequate number of STRS submitted by covered persons other than banks. Considering the data from the previous NRA and 2nd NRA, the number of STRs reported by covered persons other than banks, particularly the money services businesses and those covered persons under the Securities and Insurance sectors, increased. This is primarily due to the regulatory issuances and continuous training conducted by the AMLCS and supervising agencies, BSP, SEC and IC.

The national vulnerability aims to look at the AML combating factors that contribute to the vulnerability of a country. Some factors directly create impact (input variables) while others depend on the existence of other factors (intermediate variables). For example, in order to determine the quality of CDD framework, the AML controls or factors *Availability of Reliable Identification Structure, Independent Information Sources, Access to Beneficial Ownership Information*<sup>56</sup> must be first assessed and rated.



<sup>&</sup>lt;sup>54</sup> Formalization of the economy specifically concerns the level of informal economy ranked 2<sup>nd</sup> in terms of priority in the previous NRA.

The FISC consists of: (i) Bangko Sentral ng Pilipinas; (ii) Commission on Filipino Overseas; (iii) Department of Agrarian Reform; (iv) Department of Budget and Management; (v) Department of Education; (vi) Department of Finance; (vii) Department of Science and Technology; (viii) Department of Social Welfare and Development; (ix) Department of Trade and Industry; (x) Insurance Commission; (xi) National Economic Development Authority; (xii) Philippine Deposit Insurance Corporation; (xiii) Philippine Statistics Authority; and (xiv) Securities and Exchange Commission.

<sup>&</sup>lt;sup>56</sup> The AML factors are described in the succeeding pages.

Below is the summary of AML combating controls assessed through this NRA.

**Table 2-1. Summary of AML Controls** 

AML Combating Controls AML General Controls Rate					
AIVIE COMBACING CONCIONS	Quality of AML Policy and Strategy	Medium High			
	Effectiveness of ML Crime Definition	High			
Reliability of Financial	Level of Financial Integrity	High			
Records/Books	Effectiveness of Tax Enforcement	Medium			
(Medium)	Availability of Independent Audit	High			
	Availability of Reliable Identification Infrastructure	Medium High			
Quality of CDD Framework (Medium High)	Availability of Independent Information Sources	Medium High			
	Availability and Access to Beneficial Ownership Information	Medium High			
Accessibility to Reliable	Quality of CDD Framework	Medium High			
Information and Evidence	Reliability of Financial Records and Books	Medium			
(Medium)	Level of Formalization of the Economy	Medium			
Quality of Customs Controls on Cash and	Comprehensiveness of Customs Regime on Cash and Similar Instruments	Medium			
Similar Instruments (Medium)	Effectiveness of Customs Controls on Cash and Similar Instruments	Medium			
Quality of Cross-Border Controls on Cash and Similar Instruments	Quality of Customs Controls on Cash and Similar Instruments	Medium			
(Medium)	Quality of Border Controls	Medium			
	Quality of FIU Intelligence Gathering and Processing	Medium			
	Capacity and Resources for Financial Crime Investigations	Medium High			
Quality of Criminal	Integrity and Independence of Financial Crime Investigators	High			
Quality of Criminal Investigation (Medium High)	Capacity and Resources for Financial Crimes Prosecutions	Medium High			
	Integrity and Independence of Financial	High			
	Accessibility of Reliable Information and Evidence	Medium			
	Effectiveness of Domestic Cooperation	High			
	Effectiveness of International Cooperation	High			
Quality of Criminal	Quality of Criminal Investigation	Medium High			
Prosecution (Medium High)	Capacity and Resources for Financial Crimes Prosecutions	Medium High			

	Integrity and Independence of Financial Crimes Prosecutors	High			
	Accessibility of Reliable Information and Evidence	Medium			
	Effectiveness of Domestic Cooperation	High			
	Effectiveness of International Cooperation	High			
	Quality of Criminal Prosecution	Medium High			
Quality of Adjudication (Medium High)	Capacity and Resources for Judicial Processes	Medium High			
	Integrity and Independence of Judges	Medium High			
	Quality of FIU Intelligence Gathering and Processing	Medium			
	Capacity and Resources for Financial Crime Investigations	Medium High			
	Integrity and Independence of Financial Crime Investigators	High			
	Capacity and Resources for Financial Crimes Prosecutions	Medium High			
Quality of Asset Forfeiture Framework	Integrity and Independence of Financial Crimes Prosecutors	High			
(Medium)	Capacity and Resources for Judicial Processes	Medium High			
	Integrity and Independence of Judges	Medium High			
	Comprehensiveness of Asset Forfeiture Laws	High			
	Accessibility of Reliable Information and Evidence	Medium			
	Effectiveness of Domestic Cooperation	High			
	High				
National ML Combating Ab	Medium High				
Overall Sector Vulnerability	Medium High Medium				
National ML Vulnerability	National ML Vulnerability				

#### **DATA AND INFORMATION COLLECTION**

Data/information required for the assessment are collected from LEAs' and AMLC's databases, periodical reports, publications, research papers, annual reports, and survey results. Descriptive statistics and survey research analysis are used in the assessment of the variables.

Descriptive research is used as the primary tool in the assessment of the variables. The descriptive aspect provides the historical narrative and experience of the FIU and members of the NRAWGs. Survey research method is used as an additional support to the descriptive assessment of the

variables. The survey employs the purposive sampling<sup>57</sup> technique in which the samples/respondents are selected on the basis of knowledge, connection and judgment in relation to money laundering and terrorist financing investigation. The instrument also uses a Likert categorical scale to measure the respondents' or the members' attitude towards the factors consistent to the initial analysis of the variables.

#### AML COMBATING CONTROLS ASSESSMENT

**Quality of AML Policy and Strategy** 

**Medium High** 

The quality of AML policy and strategy is one of the key factors that determine the national ML combating ability<sup>58</sup>. It assesses whether the country has or effectively implements its national AML policy and strategy based on risk assessment conducted with all relevant government agencies and private sector participants. Financial Institutions, non-financial institutions and designated non-financial businesses and professions (DNFBPS) should also undertake their own money laundering risk assessments and implement measures to prevent or mitigate the identified risks.

As stated in Section 2 of Republic Act No. 9160, or the Anti-Money Laundering Act (AMLA) of 2001, as amended, it is the policy of the State to protect and preserve the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity. The AMLC ensures that the covered persons and stakeholders act in accordance with the mandate and objectives of the AMLA to combat money laundering, its related predicate offenses, and terrorist financing. The AMLA was also amended several times in 2003, 2012, 2013 and 2017, to make it compliant with the international AML/CFT standards.

The AMLC, as the government agency tasked to implement the AMLA, together with its Secretariat, has been responsible for developing policies and measures to combat ML/TF. From 2003 to 2016, the AMLC has issued twenty-three (23) resolutions on AML regulations to be adopted by covered persons (CPs). Most of the resolutions focus on the obligations of covered persons under the AMLA, as amended, primarily on the reporting of CTRs/STRs<sup>59</sup> and registration<sup>60</sup> with the AMLC. The AMLC has also issued four (4) resolutions on Terrorist Financing for CPs to apply measures and enhanced due diligence, and direct the freezing of properties or funds without delay, including related accounts, of the designated terrorist individuals and entities named in several sanctions lists pursuant to the United Nations Security Council (UNSC) resolutions.

<sup>&</sup>lt;sup>57</sup> A form of non-probability sampling in which decisions concerning the individuals to be included in the sample, are based on a variety of criteria which may include specialist knowledge of the research issue, or capacity and willingness to participate in the research.

<sup>&</sup>lt;sup>58</sup> The National ML combating ability assesses the country's effectiveness to prosecute and penalize instances of money laundering offenses and forfeit the proceeds and instrumentalities of the predicate crimes or unlawful activities.

<sup>&</sup>lt;sup>59</sup> Resolution No. 61, 2 August 2016, on New CTR-STR Period; Resolution No.5, 20 January 2016 and Resolution No. 43, 20 May 2014, on Multiple Transaction under one STR; Resolutions No. 10, 10-A and 10-B, 24 January 2013, on Deferred Reporting of "No/Low" Risk Covered Transaction; Resolution No. 59, 1 June 2005, on Suspicious Transaction Indicators or Red flags; Resolution No. 410, 3 September 2004, Requiring covered institution to determine the true identity of the owner subject of a covered transaction or suspicious transaction.
<sup>60</sup> Resolution No. 34, 4 May 2016, List of Money Service Business Registered with AMLC as of 03 May 2016

On 21 September 2016, the Revised Implementing Rules and Regulations (RIRRs) was approved. The new RIRRs of the AMLA, as amended, took effect on 9 August 2017. Salient features of the RIRRs include the use of biometrics as additional CDD requirement for individual and corporate signatories, the use of passport or alien certificate of registration as default identification document for foreign nationals. It also allows deferment of face to face for low risk customers, through the use the facility of Information and Communication Technology (ICT) but Know-Your-Customer (KYC) documents should be in possession of the covered persons prior to the scheduled face to face and that the entire process should be documented. Suspicious transaction report can be filed if the covered person reasonably believes that the conduct of enhanced due diligence will tip-off the customer.

Further, the AMLC closely coordinates with the supervisory authorities in the crafting and implementation of AML policies, and capacity building of the regulators. The AMLC has adopted mechanisms to strengthen its coordination with the law enforcement agencies, government agencies, supervisory authorities, CPs and private stakeholders, in the conduct of ML/TF investigation.

In 2014, the AMLC spearheaded the conduct of the First Philippine National Risk Assessment - a government-wide activity geared towards identification of ML/TF risks and the implementation of relevant policies, laws, regulations and other measures to improve the AML/CFT regime consistent with the risk and context of the jurisdiction. The 1<sup>st</sup> NRA, which covered the period 2011-2014, enabled the different sectors to identify and address deficiencies in their AML/CFT Regime. Among the identified deficiencies were on the supervision of stand-alone MSBs and the non-coverage of casinos as covered persons under the AMLA. The BSP has since issued regulations to address deficiencies of stand-alone MSBs<sup>61</sup> and casinos are now covered persons under the AMLA.

Despite the absence of an AML National policy and strategy, the AMLC and its Secretariat, along with the supervising agencies, BSP, SEC and IC, are committed to ensure that: (1) policy, coordination and cooperation among all stakeholders are in line in understanding and mitigating ML/TF risks, (2) the financial system shall not be used as money laundering site for the proceeds of crime, (3) proceeds of crime are detected and forfeited and shall not be used to further finance criminal activities, and (4) launderers and criminals are sanctioned and prosecuted. Further, the AMLC ensures that measures and policies are imposed to strengthen the AML/CFT regime.

Effectiveness of ML Crime Definition High

The ML crime definition is effective if the country has defined the money laundering offense comprehensively and it is possible to enforce and obtain convictions based on this law. It also looks into whether the penalties are proportionate and dissuasive.

On 15 February 2013, Republic Act No. 10365 which further amended R.A. No. 9160, or the Anti-Money Laundering Act of (AMLA) 2001, was signed into law. The law fully criminalized money laundering<sup>63</sup> in compliance with FATF Recommendation 3 (old Recommendation 1) by stating in particular the specific overt acts constituting the crime of money laundering. The latest law also

<sup>&</sup>lt;sup>61</sup> To be discussed in detail under Chapter 6, Other Financial Institutions

<sup>&</sup>lt;sup>62</sup> On 14 July 2017, President Rodrigo Duterte signed Republic Act No. 10927, or An Act Designating Casinos as Covered Persons under the Republic Act No. 9160, otherwise known as the AMLA, as amended. The law took effect on 29 July 2017.

<sup>&</sup>lt;sup>63</sup>Section 4, AMLA, as amended.

increased the number of predicate crimes<sup>64</sup> to money laundering which now covers nineteen (19) out of the twenty-one (21) designated categories of offenses under the FATF Revised Forty Recommendations (2012). The amendment to the definition of money laundering now covers almost all elements of the Vienna and Palermo conventions including the ancillary offense of conspiracy to commit money laundering. The latest amendment notwithstanding, tax crimes are still not included as a predicate crime to ML. There are ongoing efforts to include tax crimes as predicate crimes to ML.

On 14 July 2017, Republic Act No. 10927 was signed into law. This law classifies casinos, including internet and ship-based casinos, as covered persons under the AMLA. This would significantly dissuade criminals from using casinos to launder their criminal proceeds.

To ensure effective compliance with the AMLA, as amended, and prevent the Philippine financial system and DNBPS from being used in money laundering activities, cases must be timely filed and effectively prosecuted. Members of the NRAWGs, comprising of senior officials and designated representatives of LEAs, were of the opinion that criminal penalties provided under the AMLA, as amended, are appropriately severe. Table below shows a Summary of Criminal Penalties under the AMLA.

**Table 2-2. Criminal Penalties** 

ML Violation/ Particulars	Penalty imposed			
Money laundering [Sections 4 (a), (b), (c), (d)]  Money laundering is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity: (a) transacts said monetary instrument or property; (b) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property; (c) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property (d) attempts or conspires to commit money laundering offenses referred to in paragraphs (a), (b) or (c);	Imprisonment from seven (7) to fourteen (14) years and a fine of not less than Three Million Philippine Pesos (PhP3,000,000.00) but not more than twice the value of the monetary instrument or property involved in the offense			
Money laundering [Sections 4 (e) and (f)]  Money laundering is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:  (e) aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (a), (b) or (c) above; and  (f) performs or fails to perform any act as a result of which he facilitates the offense of money	Imprisonment from four (4) to seven (7) years and a fine of not less than One Million Five Hundred Thousand Philippine Pesos (PhP1,500,000.00) but not more than Three Million Philippine Pesos (PhP3,000,000.00)			

<sup>&</sup>lt;sup>64</sup>Section 3(i), AMLA, as amended.

-

laundering referred to in paragraphs (a), (b) or (c) above.	
Money laundering Section 4 (2 <sup>nd</sup> Par.)  Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required under this Act to be reported to the Anti-Money Laundering Council (AMLC), fails to do so.  Failure to keep records under Section 9b.  Record Keeping. — All records of all transactions of covered institutions shall be maintained and safely stored for five (5) years from the dates of transactions. With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least five (5) years from the dates when they were closed.	Imprisonment from six (6) months to four (4) years or a fine of not less than One Hundred Thousand Philippine Pesos (PhP100,000.00) but not more than Five Hundred Thousand Philippine Pesos (PhP500,000.00), or both.  Imprisonment from six (6) months to one (1) year or a fine of not less than One hundred thousand Philippine pesos (PhP100,000.00) but not more than Five hundred thousand Philippine pesos (PhP500,000.00).
Section 14(c) of the AMLA  Malicious Reporting. Any person who, with malice, or in bad faith, report or files a completely unwarranted or false information relative to money laundering transaction against any person;  Provided, that the offender is not entitled to avail the benefits of the Probation Law.	Imprisonment from six (6) months to four (4) years or a fine of not less than One Hundred Thousand Philippine Pesos (PhP100,000.00) but not more than Five Hundred Thousand Philippine Pesos (PhP500,000.00)
Section 14(d) of the AMLA Breach of Confidentiality	Imprisonment from three (3) to eight (8) years and a fine of not less than Five Hundred thousand Philippine Pesos (PhP 500,000.00) but not more than One Million Philippine pesos (PhP 1,000,000.00) shall be imposed on a person convicted for a violation under Section 9(c).
Section 14(e) of the AMLA Penalties for Knowingly Participating in the Commission of Money Laundering.	Imprisonment from four (4) to seven (7) years and a fine corresponding to not more than two hundred percent (200%) of the value of the monetary instrument or property laundered shall be imposed upon the covered person, its directors, officers or personnel who knowingly participated in the commission of the crime of money laundering

2016 Revised Implementing Rules and Regulations

From 2001 – 2014, only four ML convictions were secured by the AMLC. Two (2) of those convicted were found guilty of laundering proceeds from estafa (swindling) cases while the remaining two (2) persons were found guilty of laundering the proceeds from a Kidnap for Ransom (KFR) case. The Regional Trial Court (RTC) imposed penalties of imprisonment and fine against all four (4) persons convicted of various ML offenses. One of the persons convicted applied for probation and was granted

the same since penalty imposed on him qualified the grant of probation under the law.<sup>65</sup> He was sentenced to serve a maximum term of imprisonment of not more than six (6) years.

From 2015 to 2016, the AMLC investigated forty-nine (49) ML cases<sup>66</sup>. However, the AMLC was only able to secure (1) conviction for ML against an individual engaged in KFR of a Japanese National in Cebu City in 2003. He was sentenced to 7-14 years of imprisonment and a fine of Php3.0 million. The amount represented the proceeds he allegedly received as KFR proceeds. In 2017, an accountant was convicted for money laundering for embezzlement of more than PhP3.7 million from three (3) corporations. The proceeds of theft were deposited to the account of the husband. Below is the summary of convictions and penalties imposed.

Table 2-3. Summary of Convictions and Penalties Imposed

Table 2 of Sammary of Contributions and Females Imposed						
PARTICULARS	YEAR CONVICTED	PENALTY IMPOSED				
ML Conviction No. 1 - facilitating the						
transaction of the proceeds of estafa	2006	Imprisonment: 6 years				
(swindling) under Section 4(b) of the AMLA, as amended		Fine: PhP1.5 Million				
ML Conviction No. 2 - transacting the proceeds		Imprisonment: 7 to 13 years				
of estafa (swindling) under Section 4(a) of the	2013	Fine: PhP34 Million				
AMLA, as amended						
ML Conviction No. 3 - transacting the proceeds	2012	Imprisonment: 8 years				
of Kidnapping for Ransom (KFR) under Section	2013	Fine: PhP500,000				
4(a) of the AMLA, as amended						
ML Conviction No. 4 - transacting the proceeds	201.4	Imprisonment: 8 years				
of KFR under Section 4(a) of the AMLA, as amended	2014	Fine: PhP500,000				
ML Conviction No. 5 - transacting the proceeds						
of KFR under Section 4(a) of the AMLA, as	2016	Imprisonment: 7-14 years				
amended	2010	Fine: PhP 3,000,000				
ML Conviction No. 6 – depositing the proceeds		Imprisonment: 4-5 years (for				
from Qualified Theft under Section 4(a) of the	2017	each of the 29 counts but not				
AMLA, as amended		to exceed 15 years)				
7 Will i, as amenaea		Fine: PhP1,500,000				

The seemingly low conviction rate may be attributed to the clogged dockets of the courts, particularly the Regional Trial Courts (RTCs) where criminal cases for money laundering are filed. RTCs typically handle hundreds, if not thousands, of criminal cases in a given year. In order to decongest the court dockets, the Supreme Court approved on 25 April 2017 the Revised Guidelines for Continuous Trial of Criminal Cases. The said Guidelines took effect on 1 September 2017 and are expected to streamline the criminal litigation process by introducing significant reforms to existing trial procedures such as simplifying the form and timing of presentation of the witnesses.

<sup>&</sup>lt;sup>65</sup> Presidential Decree No. 968, as amended.

Section 9. *Disqualified Offenders*. The benefits of this Decree shall not be extended to those:

<sup>(</sup>a) sentenced to serve a maximum term of imprisonment of more than six years; x x x

<sup>&</sup>lt;sup>66</sup> The 49 cases were predicated on 19 illegal drug cases, 15 corruption-related cases, 5 estafa cases, 4 trafficking in persons cases, 2 cases on qualified theft, and 1 case each involving kidnapping, illegal recruitment, violation of the E-Commerce Act, and violation of the SRC.

Quality of CDD Framework (Medium High)	Availability of Reliable Identification Infrastructure	Medium High
	Availability of Independent Information Sources	Medium High
	Availability and Access to Beneficial Ownership	Medium
	Information	High

The Quality of CDD framework assesses whether the country has the legal, institutional and technical framework to identify and verify the identities of natural and legal persons, and to store the identification records. The use of this information shall facilitate authorized parties for AML purposes. The quality of CDD framework is determined through the assessment of the availability and reliability of identification infrastructure, independent information sources and accessibility to beneficial ownership information.

Section 9 of the AMLA, as amended, requires covered persons to establish and record the true identity of its clients based on official documents. Covered persons should likewise maintain a system of verifying the true identity of their clients. In case the client is a corporation, the covered person is required to create a system of verifying their legal existence and organizational structure.

## Reliable Identification Infrastructure

A reliable identification infrastructure, which is rated MEDIUM HIGH - the same rating as in the previous NRA, must be in place to prevent the use of fake documents and fictitious identification.

The Philippines has more than twenty (20) identification documents issued by the government and regulating agencies. These identification documents (i.e. driver's license system, passport system, social security system) are used by citizens to facilitate dealings with the government and private entities, including banks and other financial institutions.

The establishment of national identification system has been subject of heated debates for years. With the recent threats on national security, the debate has shifted in favor of the establishment of a national ID system. Lawmakers have recognized the need for a unified ID through House Bill No.6221, or the act establishing the Filipino Identification System or FilSys, which was approved on its third and final Reading in September 2017. The unified ID will serve as the official ID of a Filipino citizen which can be used in all dealings with the government offices and private entities.

The executive department, in the past years, also attempted to establish a reliable identification system, with a nationwide scope. Executive Order No. 420, series of 2005 and Executive Order No. 420, series of 2008 required all government agencies and government owned and controlled corporations (GOCCs) to streamline and harmonize their ID systems and adopt a unified multi-purpose identification (UMID)<sup>67</sup> system.

<sup>67</sup> The objectives of the UMID are:

- 1. To reduce costs and thereby lessen the financial burden on both the government and the public brought about by the use of multiple ID cards and the maintenance of redundant database containing the same or related information
- 2. To ensure greater convenience for those transacting business with the government and those availing of government services;
- 3. To facilitate private businesses and promote the wider use of the unified ID card as provided under this executive order;
- 4. To enhance the integrity and reliability of government-issued ID cards; and
- 5. To facilitate access to and delivery of quality and effective government service.

The UMID is supposed to cover the Government Service Insurance System (GSIS), Social Security System (SSS), Pag-IBIG and Philhealth are the first to adopt the UMID card system. These agencies conduct CDD procedures, and the UMID is equipped with biometric data of the holder. Further to the UMID, other government efforts set-up facilities that allow immediate verification of identification documents.

Though the Philippines is yet to implement a national ID system, various efforts have been made by the SAs to establish the true and full identity of clients. The BSP, SEC and IC have issued rules and regulations requiring CPs to obtain the prescribed minimum information and validating the same from official documents, such as government-issued IDs. Moreover, financial institutions are required to adopt a risk-based process of identifying their clients.

A survey of some ID systems in the Philippines would show that issuing government agencies have also provided mechanisms to verify authenticity of IDs they have issued.

Table 2-4. Identification Verification System

ruble 2 4 ruchtmouton vermedulon bystem						
ID System	Features of the ID	Means of Verification				
Integrated Bar of the	The new IBP ID has Quick	QR code scanning via Mobile				
Philippines ID (for Lawyers)	Response (QR) code embedded	Application				
Land Transportation Office (LTO) Driver's License	<ul><li> Has security hologram</li><li> Contains holographic image</li></ul>	SMS verification via LTO database; however, only the LTO number and date of expiration				
Professional Regulation Commission	Various professional licenses	Online verification by conducting database search on the license number and/or name				
Philippine Postal Corp. – Postal ID	<ul> <li>Has QR code embedded</li> <li>With Security hologram</li> <li>Contains holographic image</li> <li>Ultraviolet ink</li> </ul>	QR code scanning via Mobile Application				

In July 2017, the Department of Labor and Employment launched the new identification card for Overseas Filipino Workers (OFW). The OFW ID (also called iDOLE) shall be used as universal identification document by OFWs for all government transactions.

Despite efforts to ensure the validity of ID, there's still a number of cases involving fictitious identification or fraudulent IDs. The table below shows the number of suspicious transaction reports filed by CPs on clients not properly identified due to the use of fake IDs, false identity and identity theft.

1<sup>st</sup> NRA 2<sup>nd</sup> NRA **Suspicious Transaction Total** 2011 2013 2014 2015 2016 Reports 2012 Reason in the narrative field: Client is not properly identified due to: (1) identity theft; (2) forged documents; (3) no documents submitted to 497 978 801 1720 6360 1184 1180 support claim; (4) multiple identities; (5) non-existent business/address; (6) discrepancies in KYC documents; (7) fictitious ID docs

Table 2-5. STRs on Fictitious Identification

The STRs filed for fictitious identification were generally reported by commercial banks. These STRs constitute only about 0.8%-1% of the total STRs filed every year. It can then be surmised that CPs, in general, implement stringent KYC/CDD on their clients.

## **Independent Information Sources**

Covered persons rely on client's financial and historical information from available sources shared by the credit bureaus and media reports.

#### 1. The Bankers Association of the Philippines' Credit Bureau (BAP Credit Bureau)

The BAP Credit Bureau, which was established in 1990 by the Bankers' Association of the Philippines (BAP), is a computerized credit information exchange institution which facilitates the exchange of credit information among its member banks and provides credit information services to all its members. This assists the member banks in identifying individual and corporate borrowers with negative ratings and bad loan reputations.

#### 2. Credit Information System

Republic Act No. 9150 or the Credit Information System Act of 2008 (CISA Law) established the credit information system (CIS) in the Philippines. It addresses the need to build a centralized, comprehensive and reliable credit information system that is accessible to all financial institutions. Section 5 of the same Act allows the creation of Credit Information Corporation (CIC), for primary purpose of: (1) to act as a central registry or central repository of credit information; (2) to receive and consolidate *basic credit data*<sup>68</sup>; and (3) to provide access to reliable, standardized information on credit history and financial condition of borrowers. Banks, quasi-banks, their subsidiaries and affiliates, life insurance companies, credit card companies and other entities that provide credit

<sup>&</sup>lt;sup>68</sup> Basic Credit Data" refers to positive and negative information provided by a borrower to a submitting entity in connection with the application for and availment of a credit facility and any information on the borrower's creditworthiness in the possession of the submitting entity and other factual and objective information related or relevant thereto in the submitting entity's data files or that of other sources of information: Provided, that in the absence of a written waiver duly accomplished by the borrower, basic credit data shall exclude confidential information on bank deposits and/or clients funds under Republic Act No. 1405 (Law on Secrecy of Bank Deposits), Republic Act No. 6426 (The Foreign Currency Deposit Act), Republic Act No. 8791 (The General Banking Law of 2000), Republic Act No. 9160 (Anti-Money Laundering Law) and their amendatory laws.

facilities are required to participate and submit basic credit data and updates thereon on a regular basis to Credit Information Corporation.

The efficient operations and services of a CIS are expected to improve the overall availability of credit, particularly to micro-, small- and medium-scale enterprises. The CIS is also expected to reduce the financial institutions' over-all credit risk, contributing to a healthier and stable financial system.

#### 3. The CIBI Information Inc. (CIBI)

Another credit bureau, the CIBI Information, Inc. (CIBI) (formerly known as Credit Information Bureau, Inc.) is also a provider of information to businesses and individuals. The said company provides reports to accredited agencies, industry partners and even private professionals. It also validates and collects any available information using sources from both private and government institutions such as SEC, DTI, BSP, Land Transportation Office (LTO); schools, colleges, universities and other educational institutions.

**Availability of independent and reliable information sources**, previously rated as **MEDIUM** in the previous NRA, is rated **Medium High** in the 2<sup>nd</sup> NRA. This is because, aside from the availability of the systems described above, the financial institutions diligently adhere to the regulations issued by the BSP, SEC and IC. The existing regulations mandate financial institutions to verify and validate the minimum information obtained from their clients as part of customer acceptance and identification process. Higher level of validation is implemented for clients that pose higher risks. FIs rely on the authenticated official documents issued by government, utility bills, accounts and credit card statement, income statement, and other government issued documents to validate the information of their clients. Other financial institutions issue membership cards with unique identifiers to facilitate verification of the identities of their clients.

## **Beneficial Ownership Information**

FATF Recommendations 24 and 25 require countries to take measures to prevent the use of legal persons and arrangements for money laundering and terrorist financing. Competent authorities should have access and be able to obtain adequate, accurate and current information on the beneficial ownership and control of the companies and other legal persons, such as incorporators of. One mechanism that can be considered is the availability of a central database on corporations including the beneficial interests and owners.

The SEC is the main repository for information on the structure, management, control, and beneficial ownership in corporations, trusts, and similar vehicles. Juridical persons are required to file this information upon creation, and yearly thereafter. Aside from this, Section 18 of the Securities and Regulation Code (SRC) requires any person who acquires directly or indirectly the beneficial ownership of more than five (5%) of a class of equity securities/share to submit a sworn statement to the SEC disclosing information<sup>69</sup> on the beneficial owner of the shares. In this case, information on the structure, management, control and beneficial ownership are primarily obtained by the covered persons from their clients. These representations however are required to be supported by relevant documents, such as Certificate of Registration, Articles of Incorporation, Certificate of Partnership, General Information Sheet, and other identification documents incorporators, stockholders and officers of the corporation. In case the shareholder is a foreign entity, the covered persons are required to implement additional measures in order to identify the ultimate beneficial owners or

<sup>&</sup>lt;sup>69</sup> personal background, identity, residence and citizenship, nature of such beneficial ownership, purpose of acquisition, and details pertaining to the contract of acquisition.

natural persons with controlling interest to the foreign entity. To date, there were no reports on financial institutions being sanctioned for failure to identify the beneficial owner.

Covered persons have instituted their own mechanisms to obtain beneficial ownership information prior to establishing business relationship. SAs, in turn, verify during AML examination whether said information are obtained during account opening. Covered persons, regulators and authorities also use the SEC i-View database, for any information on corporations and partnerships, the Cooperative Development Authority (CDA) for cooperatives, and Department of Trade and Industry (DTI) for sole proprietorship. The existing facility however provides for limited information only. Identifying the ultimate beneficial owner may require repeated queries with the relevant authority, which can possibly delay the verification process.

Reliability of Financial	Availability of Independent Audit	High
Records/Books	Effectiveness of Tax Enforcement	Medium
(Medium)	Level of Financial Integrity	High

The reliability of financial records/books looks at whether ML investigators can rely on the financial records/books to trace the flow of proceeds of crime in money laundering cases.

#### **Availability of Independent Audit**

Currently, there is no Philippine regulatory body that currently audits the work of auditors. External auditors are not being assessed for the quality of their work. Such scenario poses challenges to various stakeholders in the accountancy and auditing industry, including, among others, the regulators, companies being audited, and the CPA practitioners.

## Initiatives from the Philippine Professional Regulatory Board of Accountancy

The Philippine Professional Regulatory Board of Accountancy (BOA), which is the government regulatory body that supervises the accountancy profession, has adopted an external audit Quality Assurance Review (QAR) Program to meet its oversight duties of looking into the quality of audit of financial statements. Relative thereto, the Professional Regulation Commission (PRC), upon the recommendation of the BOA, approved a resolution in 2009, entitled "Adoption of the Rules and Regulations [RR] for the Implementation by the BOA of the QAR Program." This RR was subsequently revised in 2010.

In December 2015, the BOA passed a resolution endorsing for approval by the PRC the adoption of the "Revised RR for the Conduct by the BOA of Oversight into the Quality of Audits of FS and Operations of CPA Practitioners."

#### Initiatives from the Philippine SEC

Insofar as the Philippine SEC is concerned, it currently performs regular evaluation of audited FS of companies, majority of whom are listed in the stock exchange and other companies or entities vested with public interest. Furthermore, as part of the accreditation process of external auditors, the SEC reviews the audited FS of the auditor's selected clients. These reviews aim to ascertain the compliance of the reporting companies with their financial reporting requirements. Administrative penalties/sanctions will be imposed on both the reporting company and its external auditors should there be any significant or material financial reporting lapses found.

Recently, the SEC has been working on the revision of its Rules on Financial Statements Reporting that include, among others, the implementation of its own QAR System of External Auditors accredited by it. Thus, aside from performing its primary regulatory function of registered corporations, the SEC will now also review the quality of audit of the external auditors.

To sum up, the eventual implementation of the BOA of its QAR Program and the final approval of the SEC of the revisions to its current rules to incorporate its own QAR System are crucial tools to increase financial transparency and ensure that proper and reliable accounting records and financial statements are available.

#### **Effectiveness of Tax Enforcement**

The effectiveness of tax enforcement assesses whether the tax laws are enforced fully, fairly, and consistently, through regulatory enforcement. This includes tax inspection, and criminal and civil litigation in order to promote voluntary compliance with the tax laws. The effective performance and implementation of tax enforcement is to promote and maintain public confidence in the integrity of the tax system.

The National Internal Revenue Code of 1997 (NIRC)<sup>70</sup> requires individuals<sup>71</sup> and corporations<sup>72</sup> to file annual Income Tax Returns (ITRs) with the Bureau of Internal Revenue (BIR). In relation to this, the BIR Commissioner is authorized by law to **obtain information, and to summon, examine, and take testimony of persons** in order to: (i) ascertain the correctness of any return; (ii) make a return when none has been made; (iii) determine the liability of any person for any internal revenue tax; (iv) collect any such liability; or (v) evaluate tax compliance.<sup>73</sup>

<sup>71</sup> Section 51 of the NIRC requires the following to file ITRs: (a) Every Filipino citizen residing in the Philippines; (b) Every Filipino citizen residing outside the Philippines, on his income from sources within the Philippines; (c) Every alien residing in the Philippines, on income derived from sources within the Philippines; and (d) Every nonresident alien engaged in trade or business or in the exercise of profession in the Philippines.

(a) To examine any book, paper, record, or other data which may be relevant or material to such inquiry;

- (b) To obtain on a regular basis from any person other than the person whose internal revenue tax liability is subject to audit or investigation, or from any office or officer of the national and local governments, government agencies and instrumentalities, including the Bangko Sentral ng Pilipinas and governmentowned or -controlled corporations, any information such as, but not limited to, costs and volume of production, receipts or sales and gross incomes of taxpayers, and the names, addresses, and financial statements of corporations, mutual fund companies, insurance companies, regional operating headquarters of multinational companies, joint accounts, associations, joint ventures of consortia and registered partnerships, and their members;
- (c) To summon the person liable for tax or required to file a return, or any officer or employee of such person, or any person having possession, custody, or care of the books of accounts and other accounting records containing entries relating to the business of the person liable for tax, or any other person, to appear before the Commissioner or his duly authorized representative at a time and place specified in the summons and to produce such books, papers, records, or other data, and to give testimony;
- (d) To take such testimony of the person concerned, under oath, as may be relevant or material to such inquiry; and
- (e) To cause revenue officers and employees to make a canvass from time to time of any revenue district or region and inquire after and concerning all persons therein who may be liable to pay any internal

<sup>&</sup>lt;sup>70</sup> Republic Act No. 8424, as amended.

<sup>&</sup>lt;sup>72</sup> Section 52 of the NIRC requires every corporation, except foreign corporations not engaged in trade or business in the Philippines, to file a true and accurate quarterly income tax return, as well as a final or adjustment return for the taxable year.

<sup>&</sup>lt;sup>73</sup> Section 5, NIRC

Access by LEAs to tax information, particularly Income Tax Returns (ITR), however, is very limited. ITRs can be open for inspection only upon order of the President of the Philippines, subject to the rules and regulations prescribed by the Secretary of Finance, and upon recommendation of the Commissioner.<sup>74</sup> Hence, ITRs and other tax information are confidential in nature and may not be readily available for the investigation of predicate crimes and ML and TF offenses.

In relation to the Philippines' compliance with Article 26 of the OECD's Model Tax Convention, the Exchange of Information on Tax Matters Act of 2009<sup>75</sup> allows the BIR to exchange information on tax matters with foreign tax authorities. The said law amended the NIRC to help combat international tax evasion and avoidance and to help address tax concerns that affect international trade and investment.

The BIR has filed cases in relation to tax evasion and other tax crimes. Below is summary of statistics on violations of tax laws handled by the BIR.

Table 2-6. Statistics off Tax Evasion by the bir			
Type of Cases	BIR (2015 to 1st Quarter of 2017)		
Number of cases filed with the DOJ	634		
Number of cases prosecuted in Court	73		
Number of convictions (cases)	5		
Number of persons convicted	6		
Estimated Amount involved (in Millions PhP)	422.66		
Amount of adjudged in favor of BIR (in Millions PhP)	102,452.6		

Table 2-6. Statistics on Tax Evasion by the BIR

Tax evasion is not a predicate offense to money laundering under the AMLA, as amended. As it is one of the designated category of offenses to ML, the AMLC supported several bills (in 2010, 2012 and 2016<sup>76</sup>) including Sections 254 (attempt to evade or defeat tax) and 255 (failure to file return, supply correct and accurate information, pay tax, withhold) of the NIRC among the list of predicate crimes to ML.

#### **Level of Financial Integrity**

The level of financial integrity focuses on the quality of business and professional ethics and tax transparency in the country. It is rated one notch higher compared to the previous NRA.

Latest Assessment of Corporate Governance (CG) Practices in the Philippines:<sup>77</sup>

1. From the Asian Corporate Governance Association (ACGA):

The table below shows that there was a slight progress in the Philippines' CG scores for 2014 relative to 2010. On the other hand, significant improvements in CG can be observed in other Asian countries, such as Malaysia, Thailand and India. Thus, the Philippines is faced with the challenge of improving its

<sup>75</sup> Republic Act No. 10021.

revenue tax, and all persons owning or having the care, management or possession of any object with respect to which a tax is imposed.

<sup>&</sup>lt;sup>74</sup> Section 71 of the NIRC.

<sup>&</sup>lt;sup>76</sup> Senate Bill 1256, filed under the 17<sup>th</sup> Congress, is still pending before the Senate

<sup>&</sup>lt;sup>77</sup> http://www.sec.gov.ph/wp-content/uploads/2015/01/SEC\_Corporate\_Governance\_Blueprint\_Oct\_29\_2015.pdf

CG scores compared to its neighboring countries in order to make investing in the Philippines more attractive.

Asian Corporate Governance Association Corporate Governance Watch Market Scores 2014 vs 2012 vs 2010

Rank	Market	2010	2012	2014	Change fr 2012	Change fr 2010
1	Singapore	67	69	65	-4	-2
2	Hong Kong	65	66	64	-2	-1
3	Thailand	55	58	60	+2	+5
4	Japan	57	55	58	+3	+1
5	Malaysia	52	55	58	+3	+6
6	Taiwan	55	53	56	+3	+1
7	India	49	51	54	+3	+5
8	Korea	45	49	49	+0	+4
9	China	49	45	45	+0	-4
10	Philippines	37	41	40	-1	+3
11	Indonesia	40	37	39	+2	-1

Based on the breakdown of the Philippines' CG scores for 2012 and 2014 (shown below), the Philippines gained points in CG rules/practices and CG culture as there were notable CG reforms and improvements in investors' relations of companies. However, the Philippines has yet to make significant improvements in disclosing and implementing a regime of effective enforcement and of quality accounting/auditing practices. Some of these sought after improvements relate to takeovers and related party transactions (RPTs).

# Asian Corporate Governance Association The Philippine Category Scores 2014 vs 2012

	2012	2014	Change
Corporate Governance Rules/Practices	35	40	+5
Enforcement	25	18	-7
Policy & Regulatory Environment	44	42	-2
International Generally Accepted Accounting Principles	73	65	-8
Corporate Governance Culture	29	33	+4

2. From the Organization for Economic Co-operation and Development (OECD) Reform Priorities in Asia:

Serious governance problems in Asian countries, including the Philippines, were noted in the "Asian Roundtable 2003 White Paper on Corporate Governance" to wit:

- i. concentrated ownership structure;
- ii. prevalent Related Party Transactions; and
- iii. lack of independence of Boards of Directors.

Relative to the above, six reform priorities were identified:

- a. Public and private-sector institutions should continue to make the business case for the value of good CG among companies, board members, gatekeepers, shareholders and other interested parties, such as professional associations;
- b. All jurisdictions should strive for active, visible and effective enforcement of CG laws and regulations. Regulatory, investigative and enforcement institutions should be adequately resourced, credible and accountable, and work closely and effectively with other domestic and external institutions. They should be supported by a credible and efficient judicial system;
- c. The quality of disclosure should be enhanced and made in a timely and transparent manner. Jurisdictions should promote the adoption of emerging good practices for non-financial disclosure. Asian Roundtable jurisdictions should continue the process of full convergence with international standards and practices for accounting and audit. The implementation and monitoring of audit and accounting standards should be overseen by bodies independent of the profession;
- d. Board performance needs to be improved by appropriate further training and board evaluations. The board nomination process should be transparent and include full disclosure about prospective board members, including their qualifications, with emphasis on the selection of qualified candidates. Boards of Directors (Board) must improve their participation in strategic planning, monitoring of internal control and risk oversight systems. Boards should ensure independent reviews of transactions involving managers, directors, controlling shareholders and other insiders;
- e. The legal and regulatory framework should ensure that non-controlling shareholders are adequately protected from expropriation by insiders and controlling shareholders. Gatekeepers such as external auditors, rating agencies, advisors, and intermediaries should be able to inform and advise shareholders free of conflicts of interest; and
- f. Shareholder engagement should be encouraged and facilitated, in particular, by institutional investors.

## 3. Based on the World Economic Forum (WEF) Report:

The table below shows that the Philippines has continually improved its ranking from 2010 to 2014 when it rose from 85th to 52nd rank. Serious efforts should be promoted and sustained to improve and align CG practices in the Philippines with the global CG standards to make Philippine companies more competitive in the global economy.

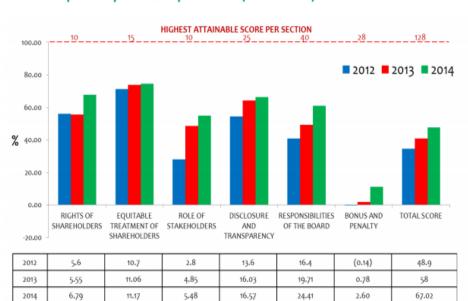
World Economic Forum Competitiveness Report (2010 - 2014)

	2010	2011	2012	2013	2014	Тор
TOTAL NUMBER OF COUNTRIES	139	142	144	148	144	
Philippine Ranking	85 <sup>th</sup>	75 <sup>th</sup>	65 <sup>th</sup>	59 <sup>th</sup>	52 <sup>nd</sup>	
CORPORATE GOVERNANCE RANKINGS	90 (65%)					55 (38%)
Ethical Behavior of Firms	129	118	87	69	49	34%
Strength of Investors' Protection	109	111	110	107	105	73%
Protection of Minority Shareholders' Interests	80	84	57	47	45	31%
Strength of Auditing and Reporting Standards	75	62	41	38	48	33%
Efficacy of Corporate Boards	56	52	51	48	29	20%

4. Based on the 2014 ASEAN Corporate Governance Scorecard (ACGS):

From 2012 when the ACGS was first adopted, there is a positive trend in improving ACGS scores of Philippine Publicly-Listed Corporation's (PLCs). This reflects a deeper commitment to sound CG practices through the concerted effort of regulators and PLCs. The average CG scores of the top 100 Philippine PLCs by market capitalization rose from 58 points in 2013 to 67.02 points in 2014 (as shown in the table below). Also, of the five governance categories, the most dramatic improvement in average scores on a year-on-year basis was in the Rights of Shareholders (6.79 points in 2014 compared with 5.55 points in 2013) and the Bonus Section (2.6 points in 2014 compared to 0.78 point in 2013).

Notwithstanding the fact that there are still many things that need to be done to raise the scores in all categories, special attention should be given to Role of Stakeholders in CG (5.48 points in 2014, maximum point is 10) and Responsibilities of the Board (24.41 points in 2014, maximum points is 40) as compared with Equitable Treatment of Shareholders (11.17 points in 2014, maximum points is 15) and Disclosure and Transparency (16.57 points in 2014, maximum points is 25).



ASEAN Corporate Governance Scorecard Average Scores of Top 100 Philippine Publicly-Listed Companies by Market Capitalization (2012 – 2014)

Accessibility to Reliable	Formalization of Level of the Economy	Medium
Information and Evidence (Medium)	Reliability of Financial Records/Books	Medium
	Quality of CDD Framework	Medium High

Accessibility to reliable information and evidence looks at whether the country has the ability to ensure that accurate financial and identification data is available and, where appropriate, accessible to authorized agencies involved in the investigation and prosecution of money laundering/terrorist financing.

The AML combating controls, (1) *reliability of financial records/books* and (2) *quality of CDD framework* are assessed in the previous sections. The AML factors used in the assessment of these

combating controls are based on the ability of the ML/TF investigators to identify and verify the identification of persons and entities and trace the proceeds of unlawful activities.

## Formalization of the Level of the Economy

Formalization of level of the economy assesses the degree by which the economy is formalized, and if there is a significant level of informal economic activity in the country.

## Bangko Sentral ng Pilipinas' (BSP) Financial Inclusion Initiatives

The BSP continued to lead the implementation of the National Strategy for Financial Inclusion (NSFI). The Office of the President issued Executive Order (EO) No. 208 on 02 June 2016 to create the Financial Inclusion Steering Committee (FISC)<sup>78</sup>, the governing body that: (i) provides strategic direction, guidance and oversight in the NSFI implementation which was developed through a consultative process; and (ii) serves as a pillar for public and private sector stakeholders to systematically accelerate financial inclusion in the Philippines. The EO's issuance marks another breakthrough in the effort to establish a financial system that benefits all Filipinos, specifically the unbanked and underserved, and thereby contribute to inclusive growth and development.

The BSP further enhanced the financial inclusion regulatory environment through policies<sup>79</sup> that promote financial access to targeted sectors. Other initiatives of the BSP directed at financial inclusion are the following:

- **1. BSP's Financial Inclusion Reports -** The BSP continuously publishes regular reports on financial inclusion to sustain past efforts in support of evident-based policy making; to wit:
  - a. Financial Inclusion in the Philippines. A semestral publication that aims to increase public awareness and appreciation of the BSP's initiatives in financial inclusion, themes and topics related to financial inclusion, and new developments and emerging issues in both domestic and global contexts.
  - b. Report on the State of Financial Inclusion in the Philippines. An annual report that provides an update on the various financial inclusion initiatives of the BSP and the general state of financial inclusion in the Philippines using data from supervisory reports. This is annually updated and upgraded to include a growing number of financial inclusion indicators.

The BSP also established a web-based search facility that will allow users to identify banks and other financial institutions in their respective areas. This searchable directory allows the public to find accessible financial institutions as potential sources of products and services. The public may contact financial institutions directly to make inquiries, and possibly facilitate the start of beneficial banking relationship.

<sup>&</sup>lt;sup>78</sup> The FISC consists of: (i) Bangko Sentral ng Pilipinas; (ii) Commission on Filipino Overseas; (iii) Department of Agrarian Reform; (iv) Department of Budget and Management; (v) Department of Education; (vi) Department of Finance; (vii) Department of Science and Technology; (viii) Department of Social Welfare and Development; (ix) Department of Trade and Industry; (x) Insurance Commission; (xi) National Economic Development Authority; (xii) Philippine Deposit Insurance Corporation; (xiii) Philippine Statistics Authority; and (xiv) Securities and Exchange Commission.

<sup>&</sup>lt;sup>79</sup> BSP Circular 901 (dated 29 January 2016), amending Sec. X151 of the Manual of Regulation for Banks (MORB); BSP Circular 908 (dated 14 March 2016) Agricultural Value Chain Financing (AVCF) Framework; Circular 929 (dated 28 October 2016) -Allows the conversion of micro-finance-oriented thrift or rural banks (or branches) to regular bank (or branches).

- 2. BSP Economic and Financial Learning Program The BSP implemented different component programs of the Economic and Financial Learning Program (EFLP) which is in line with the thrust to develop a citizenry that is well-informed in economics and finance. In 2016, there were 42 learning sessions with 55,000 participants reached nationwide.
- 3. BSP's Financial Learning Module for the Unbanked The BSP collaborated with the Department of Social Welfare and Development (DSWD) in developing a simplified financial learning module specially-made to the unique profile of unbanked segments like the participants of the Pantawid Pamilyang Pilipino Program (Pantawid) and Sustainable Livelihood Program (SLP). The module will be integrated in the Family Development Session (FDS) modules being delivered to all Pantawid and SLP participants. The impact of this module is significant considering the number of Pantawid and SLP beneficiaries and their households.
- **4. BSP's Financial Empowerment Seminars** This covers topics on credit cards, savings consciousness, consumer protection, fraud and scams and investment products. In 2016, a total of twenty-one (21) FES were conducted in various areas reaching a total of 2,951 which is 140% above target.
- **5. Financial Education Expo** -This aims to instill awareness about the availability and accessibility of financial education programs to all Filipinos, increase personal financial consciousness on the values and benefits of being financially empowered, and orient the public about available financial tools that can help promote their financial well-being.
- **6. BSP's Financial Inclusion Fridays** -This learning event aims to familiarize BSP employees with financial inclusion concepts, the BSP's role in financial inclusion and ongoing initiatives.
- **7. Financial Education Through Social Media -** This is a cost-efficient way of expanding public awareness on financial education and consumer protection through the BSP Facebook page.
- **8. BSP's Establishment of a Credit Surety Fund** On 6 February 2016, Republic Act No. 10744, otherwise known as the "Credit Surety Fund (CSF) Cooperative Act of 2015," was enacted. It provides for the creation and organization of CSF cooperatives to manage and administer credit surety funds and enhance the accessibility of micro, small and medium entrepreneurs, cooperatives and non-government organizations to the credit facility of banks.

BSP's CSF Program is a credit enhancement scheme which aims to increase the credit worthiness of micro, small and medium enterprises (MSMEs) that are experiencing difficulty in obtaining loans from banks due to lack of acceptable collateral, credit knowledge and credit track record.

The formalization of the level of economy has improved to **MEDIUM** from medium low in the previous NRA, primarily due to the financial inclusion initiatives of the government that address the needs of the target sector - the unbanked and underserved.

Quality of Customs Controls on Cash and	Comprehensiveness of Customs Regime on Cash and Similar Instruments	Medium
Similar Instruments (Medium)	Effectiveness of Customs Controls on Cash and Similar Instruments	Medium

The quality of customs controls on cash, and other similar instruments looks at whether the country has a comprehensive and well-designed legal and regulatory framework, whether it enforces the customs laws and regulations effectively, and whether it can actually detect and deter any attempt for unauthorized transportation of cash, negotiable instruments and precious metals and stones.

The BSP mandates<sup>80</sup> travelers passing through international airports and seaports to make cross border declarations of local or foreign currencies brought in or out of the country beyond the identified thresholds. Any person, who brings into or takes out of the Philippines foreign currency, as well as other foreign currency-denominated bearer monetary instruments, in excess of USD10,000 or its equivalent is required to declare the same in writing and to furnish information on the source and purpose of the transport of such currency or monetary instrument. Likewise, a person may import or export, or bring with him into or take out of the country, or electronically transfer, legal tender Philippine notes and coins, checks, money order and other bills of exchange drawn in pesos against banks operating in the Philippines in an amount not exceeding PHP50,000 without prior authorization by the BSP. Amounts in excess of said limit without prior written authorization from the BSP can be confiscated and subject to forfeiture proceedings by the Bureau of Customs and subject the offender to criminal prosecution.

The Office of Transportation Security (OTS) assists the BOC in the detection undeclared currencies. OTS personnel have attended trainings and are able to detect through x-ray machines bulk cash hidden in luggage of passengers.

However, not all airports and seaports submit cross border declaration reports to the AMLC, with only NAIA regularly submitting cross border declaration forms to the AMLC. For the period 2014-2016, only 2,346 foreign currency declarations were submitted to the AMLC.

Table 2–7. Statistics on Foreign Currency Declarations

rable = 7. Granous on Foreign Carrency Deciarations					
Year	Incoming Passengers	Outgoing Passengers	Total		
2014	490	377	867		
2015	519	458	977		
2016	32	470	502		
Total	1,041	1,305	2,346		

The decline in the number of declarations submitted to the AMLC indicate lack of enforcement of the requirements of cross-border declarations. This is a source of vulnerability as government may be unable to monitor cash smuggling. This also hampers efforts of the government to come with up with reliable data on the amount of cash being declared, their sources and destination and nationalities of those who do so.

<sup>&</sup>lt;sup>80</sup> Section 4 of the BSP Manual of Regulations on Foreign Exchange Transactions, as amended by Circular No. 794 dated 18 April 2013 and Circular No. 874 dated 8 April 2015; and Circular No. 922 dated 23 August 2016

Reminders to declare excess cash are also lacking in international airports and seaports. The BOC has coordinated with the AMLC and BSP to increase visibility of reminders to accomplish and submit cross border declarations

Quality of Cross-border Controls on Cash and Similar	Quality of Border Controls	Medium
Instruments (Medium)	Quality of Customs Controls on Cash and Similar Instruments	Medium

The Quality of Cross Border Controls is assessed based on the quality of border control mechanisms and the country's legal and regulatory framework to deter unauthorized transportation of cash, negotiable instruments and precious metals and stones.

The vast maritime borders of the Philippine archipelago make it difficult for the already resourcestricken Philippine Coast Guard and Bureau of Customs to monitor all possible entry and exit points into the country. This is especially true in Southern Philippines near the Malaysian and Indonesian borders, which has been exploited by smugglers (cash, goods and persons) and other criminal elements.

As seen in Chapter 1, Threat Assessment, the predicate crime of smuggling<sup>81</sup> is rated high, with the estimated illicit financial flows in the Philippines ranging from USD2.6 million to USD41.6 million from 2005 – 2014.<sup>82</sup> The high level of informal economy parallel to the formal one creates a strong demand for producing illicit products by both small time enterprising individuals and organized crime groups. The economic incentives from these illicit activities overshadow legal consequences, thus encouraging businesses to engage in such crimes.

Porous borders in the Southern Philippines has also been exploited by terrorist elements, as can be seen in Chapter 9, Terrorism and Terrorism Financing Threats. A local terrorist organization used the seas in the region, even crossing over to international waters, to perpetuate its kidnapping activities. It is also suspected that ransom money for some kidnap victims are carried through the borders. There are also anecdotal information of terrorist and threat groups carrying out smuggling activities (drugs, rice, other goods, persons) in the Southern Philippine regions.

The *quality of customs controls on cash and similar instruments* is another AML combating control. As discussed above, customs controls on cash and similar instruments are not strictly enforced. Efforts are currently being made to strengthen the legal framework and enforcement of cross border declarations.

\_

<sup>&</sup>lt;sup>81</sup> Smuggling as a "practice of using illegal trade channels or fake foreign trade declarations for the purpose of evading the payment of duties and taxes, [which] inevitably causes distortions in international trade data and in policies subsequently formulated from it remains as an important trade issue, which effectively challenges the government's political and economic authority."

<sup>82</sup> Global Financial Integrity, 2015

Quality of Criminal Investigation (Medium High)	Quality of FIU Intelligence Gathering and Processing	Medium
	Capacity and Resources for Financial Crime Investigations	Medium High
	Integrity and Independence of Financial Crime Investigators	High
	Capacity and Resources for Financial Crimes Prosecutions	Medium High
	Integrity and Independence of Financial Crimes Prosecutors	High
	Accessibility of Reliable Information and Evidence	Medium
	Effectiveness of Domestic Cooperation	High
	Effectiveness of International Cooperation	High

Quality of criminal investigation depends on the ability and integrity of the law enforcement agencies to appropriately initiate and conduct investigations of alleged money laundering offenses. The AMLC is the government agency tasked to implement the Anti-Money Laundering Act, as amended. It has the power to investigate suspicious transactions and covered transactions deemed suspicious after an investigation by AMLC, money laundering activities, and other violations of this Act;<sup>83</sup> and to cause the filing of complaints with the DOJ or the Ombudsman for the prosecution of money laundering offenses.<sup>84</sup>

## **Quality of FIU Intelligence Gathering and Processing**

The AMLC, and its Secretariat, would be able to carry out its functions effectively when it (1) has adequate capacity and resources, and (2) has the independence and autonomy to perform its activities without fear or favor. The AMLC shall act unanimously in the discharge of its functions.

# A. AMLC Registration and Reporting of Covered and Suspicious Transactions

Covered Persons are required to submit covered transaction reports (CTRs) and suspicious transaction reports (STRs) within five (5) days from date of transaction.<sup>85</sup> The CTRs and STRs are submitted in a secured format via *web portal* and lodged in the AMLC database for analysis. The Financial Intelligence Analysis Staff (FIAS) of the AMLC Secretariat is the primary unit tasked to collect and analyze all the STRs and CTRs deemed suspicious and submit their analysis reports to the Compliance Investigation Group (CIG) for further investigation. The CIG acts as the law enforcement of the AMLC Secretariat.

As of 31 December 2016, the AMLC has received 526,190<sup>86</sup> STRs and 470,644,693 electronic CTRs. The graphs below show the trend in covered and suspicious transaction reporting from 2004 to 2016.

\_

<sup>83</sup> Section 7(5), Republic Act No. 9160, as amended

<sup>84</sup> Section 7(4), Republic Act No. 9160, as amended

<sup>&</sup>lt;sup>85</sup> AMLC Resolution No. 61, dated 20 July 2016.

<sup>&</sup>lt;sup>86</sup> AMLC Annual Reports

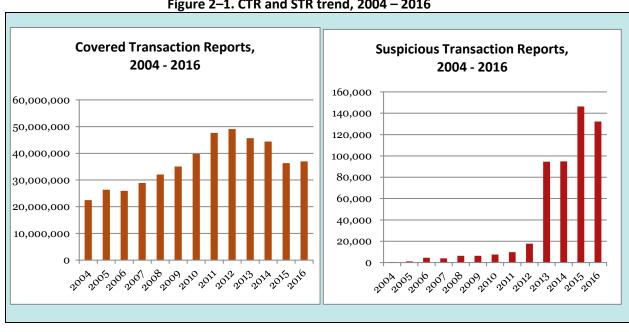


Figure 2–1. CTR and STR trend, 2004 – 2016

For the period 2011 to 2016, the AMLC received 495,656 STRs which accounted for 94.26% of the total STRs filed since 2004. On the other hand, CTRs filed within the same period accounted for 55.26% of the total CTRs. The bulk of these reports, or about 99%, were filed by BSP-supervised covered persons, mostly from the banks.

In the 1st NRA, the number of CPs reporting to AMLC registered a 31.83% increase across all sectors. This is particularly due to the issuances of the BSP Circular 706, series of 2011 and AMLC Resolution 10-A, Series of 2013, which mandated CPs to strictly comply with the AMLA.

As of 2016, the number of CPs reporting CTRs/STRs increased by 9% from 1,168 CPs in 2014 to 1,272 CPs, particularly from the Money Service Businesses (MSBs), Rural Banks, Insurance Companies and Financing Companies. Table 2-8 shows the number of covered persons reporting CTRs/STRs to AMLC.

Table 2–8. Covered Persons Reporting to AMLC

		1 0					
SA	Total Covered Persons Submitting Reports						
Year	2011	2012	2013	2014 <sup>87</sup>		2015	2016
BSP	824	863	890	930		957*	1006*
IC	57	58	64	72		76	77
SEC	59	66	76	166		183	189
Total	940	987	1,030	1,168		1,216	1,272

Note: The statistics on BSP-supervised institutions include those CPs that underwent merger and those ceased to operate in 2015 and 2016.

<sup>&</sup>lt;sup>87</sup> NRA Report 2015, STR Data Analysis

For BSP-Supervised CPs, 98% of the entities that registered in 2015-2016 came from MSBs (i.e. FX dealers, money changers, remittance agents, pawnshops). This is primarily due to BSP Circular No. 93888, Series of 2016, requiring pawnshops to strictly comply with the AMLA and its RIRRs. In April 2016, the BSP also issued Memorandum M-2016-004 which requires banks to conduct risk management when dealing with MSBs. Under this Memorandum, banks should require MSBs to submit proof of AMLC registration to comply with reporting obligations. Pursuant to this memorandum, the AMLC issued Resolution No. 34, Series of 201689, which indicates the revised registration procedure for MSBs.

Figure 2-2 shows the 6-year comparative data between the BSP-supervised CPs registered and reporting to AMLC.

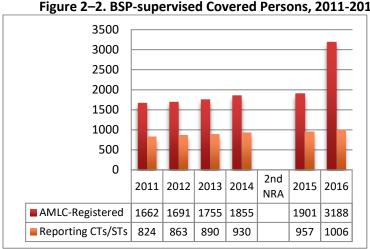


Figure 2–2. BSP-supervised Covered Persons, 2011-2016

For the period 2011-2016, registration of IC-supervised CPs, particularly insurance companies, increased. The diagram below shows the number of IC-supervised CPs<sup>90</sup> registered and reporting covered and suspicious transactions (CTs/STs) to AMLC.

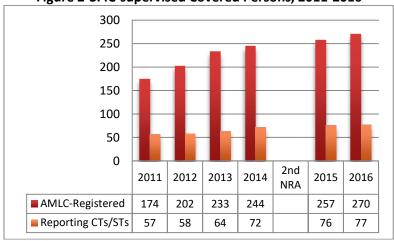


Figure 2-3. IC-supervised Covered Persons, 2011-2016

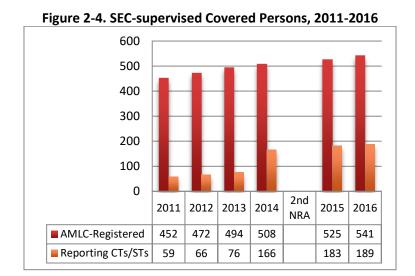
<sup>&</sup>lt;sup>88</sup> BSP Circular No. 938, Series of 2016 on Amendments to the Manual of Regulations for Non-Bank Financial Institutions MORNFBI) - Pawnshops (P) Regulations, Section 4191.P Anti-money laundering regulations

<sup>&</sup>lt;sup>89</sup> AMLC Resolution 34, Series of 2016, was approved on April 29, 2016.

<sup>&</sup>lt;sup>90</sup> The statistics include covered persons that currently are in *inactive* status with the AMLC and those CPs that were not granted certificates of authority to operate by the Insurance Commission. Source of data, AMLC database.

In 2015, the IC created an AML department that oversees AML compliance of IC-supervised CPs. The 10.66% increase in the number of CPs registered with AMLC can be attributed to the efforts of the Insurance Commission to ensure compliance of IC-CPs with the AML/CFT requirements through the issuance of guidelines and circulars. The above data also includes reclassification of Pre-need companies from SEC-supervised to IC-supervised. On the other hand, no Health Maintenance Organizations (HMOs)<sup>91</sup> have registered with AMLC since its inclusion as Covered Persons under IC in 2015.

Most of the SEC-supervised CPs that registered with AMLC in 2015 and 2016 are financing companies and mutual fund/investment companies. The 6.5% increase in the number of CPs registered with AMLC can be attributed to the issuance SEC Memorandum Circular No. 19, Series of 2014 which pertains to the submission of the Anti-Money Laundering Operating and Compliance Form for financing and lending companies. The SEC also issued SEC Memorandum Circular No. 10, Series of 2013, which amended the General Information Sheet (GIS) to include page 1-A pursuant to the AMLA. In 2015, the SEC issued the Revised Implementing Rules and Regulation of the Securities Regulation Code requiring all SEC-supervised institutions to comply with the requirements of the SEC and the AMLA, where applicable.



## **B.** Analysis of Suspicious Transaction and Covered Transaction Reports

From 2014-2016, about 98% of the total CTRs and STRs were submitted by covered persons supervised by the BSP, particularly from the banking sector. This is primarily due to the AML systems in place and ongoing monitoring by banks. BSP has imposed regulations to effectively detect and alert banks' attention on transactions, including account movements, that may qualify either as covered transactions or suspicious transactions. Universal and commercial banks are likewise required to adopt electronic AML systems capable of monitoring risks associated with ML/TF. 92

Tables 2-9 and 2-10. Covered Transaction Report (CTR) and Suspicious Transaction Report (STR) per Supervising Agency (SA)

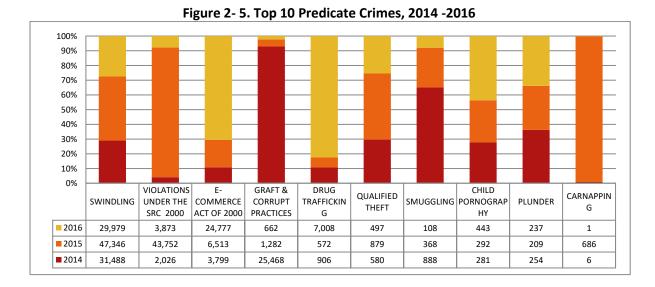
<sup>&</sup>lt;sup>91</sup> Executive Order No. 192 signed 12 November 2015 by President Benigno S. Aquino III transferred the regulation and supervision of Health Maintenance Organizations from the Department of Health to Insurance Commission.

<sup>&</sup>lt;sup>92</sup> With reference to NRA banking sector *Effectiveness of Suspicious Activity Monitoring and Reporting* 

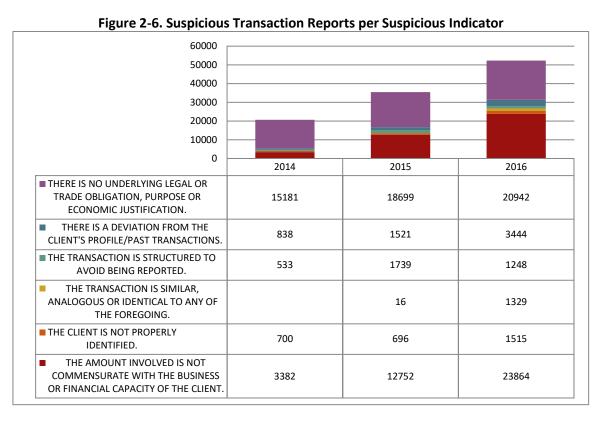
	Ta	able 2-9. CTRs	Ta	ble 2-10. ST	Rs	
SA	2014	2015	2016	2014	2015	2016
BSP	43,804,450	35,657,724	36,187,391	94,483	145,861	129,678
IC	84,258	68,889	58,907	364	467	697
SEC	493,111	595,451	735,152	92	70	1,931
Total	44,381,819	36,322,064	36,981,450	94,939	146,398	132,306

As the CTR and STR trend (figure2-1), grew at an increasing rate, the AMLC recognizes the need to conduct risk assessment and prioritization of STRs and data mining analysis on CTRs. Since 2011, the STRs are being classified based on their unlawful activities and suspicious indicators under Sec. 3.b of the AMLA, as amended, and according to their level of prioritization. If the STR warrants further investigation, the analyst conducts preliminary assessment using available database resources, such as AMLC Search Engine, World-Check, SEC i-View, and other open source websites. The preliminary STR analysis reports are submitted to the CIG, the investigative arm of the AMLC, for case building.

Most of the STRs referred to the CIG in 2014 were related to the *pyramiding and pork barrel scams* that were under AMLC investigation since 2013. In 2015, the AMLC received 146,398 STRs, the bulk of which were reported in relation to an investment scam involving several entities for allegedly selling unregistered securities (gold) to the public. While in 2016, the bulk of the 132,306 STRs were filed under Swindling and violations of the Electronic Commerce Act of 2000, accounting for 22.66% and 18.73%, respectively. 35,150 STRs or 25.79% of the total STRs. STRs under these categories were related to disputed/unauthorized online transactions, counterfeit cards and ATM skimming. Below is the graphical trend of the top 10 predicate crimes or unlawful activities based on STRs filed by CPs from 2014 – 2016.



A notable increase was also observed for STRs filed on *Other suspicious or red flag indicators* under Section 3(b-1) of the AMLA, as amended. Most of the STRs submitted under the indicators specified therein pertained to the involvement of officials and entities in pork barrel scam, illegal drugs, graft, terrorism and violations of the E-Commerce Act of 2000.



The FIAS staff are conducting STR analysis, on top of their other equally important functions such as strategic analysis, data mining and operational/tactical analysis<sup>93</sup>. As of June 2017, the FIAS has referred 43% of the STRs to the CIG. The low referrals of STRs to the CIG, can be attributed to the increasing number of STRs, as well as requests for information (RFIs) from law enforcement agencies and foreign counterparts. On the average, each analyst is required to act on 800 STRs per month, in addition to the RFIs received from the LEAs and foreign counterparts. For every RFI, the analyst spends on the average at least two (2) working days to collect and analyze transactions of the subjects. In some RFIs, particularly those involving *multiple subjects* and/or *sophisticated ML schemes* (*such as boiler room operations, securities fraud, market manipulation)*, data collection and analysis on the transactions may entail not less than five (5) days. Due to the limited number of analysts, the FIAS acts predominantly on the requests for database information from LEAs and foreign counterparts. It is the presumption that the information needed by the LEAs and foreign FIUs are necessary in the conduct of their ongoing investigations. In order to address the low STR referrals and long turnaround time, the AMLC may need to revisit the prioritization and classification procedure for both the STRs and requests for information.

## C. STRATEGIC ANALYSIS on STRs and CTRs

Pursuant to Section 7(7) of the AMLA, as amended, and FATF Recommendation 29, the Financial Intelligence Analysis Staff (FIAS) conducted a strategic analysis on the cross border investment fraud

<sup>&</sup>lt;sup>93</sup> One of the major functions of the FIAS is to provide support to the investigative unit of the AMLCS, the CIG, by acting on their requests for database information on subjects under ML/TF investigation.

in the Philippines from 2010 to 2014. The FIAS used descriptive and quantitative techniques in determining the extent cross-border investment fraud<sup>94</sup> in the Philippines. The study used data from the AMLC database, search requests from LEAs, and ESW (Egmont Secure Web) requests for the same period.

Based on the STRs and other requests received by the AMLC from foreign counterparts, the Philippines appears as a destination of the proceeds of investment fraud, particularly those from boiler room, recovery room, and advance fee fraud. Analysis on the STRs and CTRs shows that Makati, Pasig, Quezon City, Cebu, Butuan, Paranaque City and Cavite are among the top locations of beneficiaries of the proceeds from fraud. On the other hand, Canada, Singapore Germany and USA are some of the source countries of remittances from the presumed victims or suspected criminal associates. Other countries that were identified as sources of remittances are presented in the illustration below.



Figure No. 2-7. Source Country of Remittances/ Proceeds from Cross-Border Investment Fraud

Common schemes of this type of fraud, based on the STRs, are the use of investment advisors, business process outsourcing/call center businesses and retail trading of goods. These companies receive the international remittances from victims located in different jurisdictions. The amounts are then immediately withdrawn in cash. Information gathered by the reporting banks from these companies as to the purposes of the remittances and withdrawals include: (1) the funds are intended to finance activities<sup>95</sup> of foreign nationals; (2) funds to be used to purchase properties in the Phils.; and (3) as payment for business expenses.

The results of the study may be used by the AMLCS, LEAs, and other state agencies to determine money laundering vulnerabilities of cross-border investment fraud, and to enhance their knowledge and understanding on the methods used to defraud their victims. It may also help establish policies and goals for AMLC, or more broadly for other entities within the AML/CFT regime.

In February 2017, the FIAS started their second strategic analysis on STR data quality. The FIAS looks into the quality of the STRs submitted by the CPs in 2016 using the mandatory data fields defined under the AMLC Reporting Procedure. The quality of STRs is measured through the completeness of information provided in the STRs which the FIAS and CIG can use in their analysis and investigation of possible money laundering offense. Results show that about 31% of the STRs do not have information on the subject of suspicion, 49% show inconsistencies and lack clarity in the narrative fields, and 56%

<sup>&</sup>lt;sup>94</sup> 2015 Strategic Analysis Report on Cross-border Investment Fraud posted on the AMLC website in 2016.

<sup>&</sup>lt;sup>95</sup> Activities such as business expense, travel allowance, casino and gambling activities, purchase of properties, etc.

were filed by the presumed transacting branch of the subject of the STR. The results of the study may serve as a means of feedback mechanism to covered persons to address the deficiencies in the transaction reporting.

#### **D. DATA MINING ANALYSIS**

CTRs are being analyzed through the conduct of data mining. For 2016, the FIAS referred three (3) data mining analysis reports to the CIG for further assessment. The data mining reports targeted potential subjects of investigation for fraud, particularly those engaged in boiler room, recovery room and advance fee fraud. The FIAS looked into more or less 100,000 CTRs resulting from the criteria set by the FIAS to obtain reports on entities with profile and transaction pattern similar to those involved in investment fraud.

Strategic analysis and data mining are not regularly being conducted by the FIAS due to the mounting requests for information and STRs received by the AMLC. Moreover, for these types of analysis which require higher statistical and data modeling software and applications, the FIAS analysts employ a mix of automated and manual data treatment and statistical techniques which may entail a longer period to produce the intelligence/analysis reports.

The AMLC shares the processed information and intelligence reports to LEAs, supervising agencies and foreign counterparts pursuant to the provisions set forth in the Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with these agencies. To date, the AMLC has 25 MOAs and 40 MOUs with different LEAs, SAs and FIUs.

The processed information from CTRs and STRs are used by the CIG in the conduct of gathering additional documents for investigation of subjects and related accounts and associates.

Based on the foregoing, the quality of FIU intelligence gathering is rated MEDIUM.

## Capacity and Resources for Financial Crime Investigations

One of the primary functions of the AMLC is to initiate investigations of covered and suspicious transactions, money laundering activities and other violations under the AMLA, as amended. The AMLC is assisted by a Secretariat in the conduct of its functions.

The Compliance and Investigation Group (CIG) is specifically tasked to handle money laundering/terrorism financing (ML/TF) investigations in the AMLC Secretariat There are seven (7) subgroups comprising the CIG with each subgroup concentrating on specific predicate crimes defined under the AMLA, as amended. Rather than have a "general-function-unit" that investigates a variety of offenses, dedicated subgroups, usually composed of three (3) financial investigators, are specifically tasked to handle the investigation of particular financial crimes.

The key functions of the CIG are as follows:

- (a) Investigate suspicious transactions, covered transactions deemed suspicious, money laundering activities and other violations of the AMLA, as amended;
- (b) Investigate terrorism financing activities and other violations of the Terrorism Financing (TF) Suppression Act;

- (c) Act on request for investigation or request for information from domestic law enforcement and other agencies of the government and requests for assistance of other jurisdictions and international organizations;
- (d) Gather evidence for the purpose of establishing probable cause required in the filing of petitions for freeze orders, applications for bank inquiry, civil forfeiture cases and criminal complaints for money laundering; and
- (e) Conduct administrative investigation on violations by covered persons of the AMLA, as amended, and its RIRRs.

The current plantilla of the CIG is composed of twenty-three (23) positions. The group is headed by one (1) Deputy Director assisted by seven (7) subgroup heads exercising supervision over two (2) to three (3) financial investigators. The conduct of financial investigations for ML/TF activities constitutes the bulk of the work of CIG personnel.

Each CIG financial investigator typically handles an average of thirty-five (35) ML/TF cases a year based on the Suspicious Transaction Reports (STRs) and requests for information and referrals from Philippine and international law enforcement agencies. These cases range from a few number of subjects, accounts or transactions, to those involving dozens of respondents, hundreds of accounts and complex transactions. An investigator would typically require approximately 55 to 165 man-hours to probe a small case. On the other hand, the more complex cases would require approximately 165 to 625 man-hours of investigation. Most of the time allotted to investigation is consumed by gathering bank and financial information from covered persons, case conferences with relevant law enforcement and other government agencies, analyzing the financial transactions, preparing the investigation report, and testifying in the ML/TF cases.

At present, the CIG has eight (8) investigation teams to deal with high-profile cases particularly those involving plunder, graft and corruption, and large-scale swindling. These high-profile cases take up a considerable amount of time and effort for CIG investigators inasmuch as these are cases of public-interest where asset recovery and successful prosecution is essential to ensure that the perpetrators of the ML/TF activity are held accountable. For instance, the Bangladesh Bank investigation team, composed of nine (9) investigators has spent, to date, a total of approximately 624 man-hours in the investigation of the case since February 2016.

The current roster of CIG investigators is composed of experienced accountants and lawyers possessing specialized knowledge and technical expertise in AMLA laws, rules, regulations and procedures.

Table 2-11. CIG Profile, 2011 - 2016

Field of Expertise/Educational	2011-2014	2015-2016
Background	Complement	Complement
Certified Public Accountant (CPA)	4	4
Certified Public Accountant and Lawyer	4	6
Lawyer	5	5
CPA and Forensic Accountant	1	2
Financial Expert from Law Enforcement	3	2
Agency		
Total	17	19

Managerial positions in the CIG are occupied by individuals with the expertise necessary to analyze significant volumes of financial, banking, business and accounting transactions as well as the experience in gathering business and financial intelligence, identifying complex illegal schemes,

following the money trail and using investigative techniques to effectively prosecute the case. Similarly, they are competent in guiding and honing the skills of intermediate and junior financial investigators. They are also qualified to represent the AMLC in different committees, special assignments and meetings with other offices/agencies. Other functions performed by CIG investigators:

- 1. Represent AMLC in Inter-Agency Meetings
- 2. Conduct AMLA Lectures
- 3. Attend to Queries and/or Requests for Clarifications/Reports on Possible Unlawful Activity or ML Offenses

The ML/TF investigators regularly attend training conducted by the Secretariat and LEAs to keep them abreast with the recent trends and schemes on money laundering and terrorism financing.

**Table 2-12: Number of Trainings for AMLC** 

	Year	2011	2012	2013	2014	2015	2016	Total
ML/TF; Asset tracking/	asset	11	9	6	12	8	13	59
forfeiture trainings								

With the scope of the CIG's responsibilities widened (to deal with financing of terrorism in addition to money laundering and related predicate offenses) and range of reporting entities expanded to include DNFBPs (dealers in precious metals and stones, company service providers, legal and accounting professionals), CIG needs the additional manpower and resources to strengthen its basic core functions in the area of ML/TF financial investigations.

## <u>Integrity and Independence of Financial Crime Investigators</u>

The AMLC's current structure insulates the agency from undue influence and pressure from personalities subject of its investigations, especially from government officials who are suspected of having committed plunder, graft and corruption. It is not attached to any other government agency in the Philippines. Its day-to-day operations and investigations are not subject to review/approval of other government offices.

Insofar as the selection and placement of AMLC financial investigators, they undergo several interviews by the key officers of the AMLC Secretariat and the Human Resource Management Department of the BSP. They also undergo a series of psychological examination and background investigations before they are employed.

The unblemished reputation of AMLC investigators has been lauded by domestic and international law enforcement agencies, foreign FIUs, banking associations, government offices, justice officials, courts and the Philippine legislature.

As of 2016, there were no integrity breaches, whether actual or suspected, for the AMLC and its Secretariat. Within the same period, neither the AMLC nor its ML investigators have been investigated, much less indicted, for suspicion of committing acts which may undermine their integrity and professionalism in the performance of their functions.

In 2014, the AMLC Secretariat commissioned an Integrity and Corruption Perception (ICP) survey designed to provide qualitative and comparative information on the general level of integrity and corruption of ML prosecutors/investigators in the Philippines. This survey seeks to elicit categorical responses from various LEAs about: (i) their own experience; and (ii) their perceptions of the integrity

characteristics and behavior of others involved in financial crimes /money laundering (FC/ML) investigations. This exercise is intended to identify the targeted agencies' corruption vulnerabilities, integrity strengths and weaknesses and, in turn, confirm the frequency as well as extent of problematic practices. Though at the outset, it bears emphasis that perceptional data espoused by this ICP survey are considered subjective and are thus colored by respondents' incentives to withhold or color information through the filter of their own opinions.

The 2014 ICP questionnaire is composed of four (4) parts, each part made up of six (6) questions which essentially encapsulates the following ICP indicators for FC/ML prosecutors and investigators:

## 1. Timeliness indicators:

- 1.1. Promptness of action from the time complaint was filed; and
- 1.2. Judicious determination of probable cause

#### 2. Qualitative indicators:

- 2.1. Decision/resolution rendered based on the merits of the case;
- 2.2. Decision/resolution rendered without bias; and
- 2.3. Competency of FC/ML prosecutors and investigators to decide based on law and evidence.

#### 3. Quantitative indicator:

3.1. Sufficiency of FC/ML prosecutors and investigators to handle complaints

The above indicators (encompassing quantitative, qualitative and timeliness spectrum) were assigned equal weights as they are considered equally important in capturing ICP.

In order to gauge the respondents' integrity and corruption perception (both in the individual and institutional level), the ICP survey questionnaire employs a five-level grading system (1 being the highest and 5 the lowest), to wit:

1	2	3	4	5
Strongly Agree	Agree	Slightly Agree	Disagree	Strongly Disagree
81% to 100%	61% to 80%	41% to 60%	21% to 40%	0 to 20%

The ICP survey was used in 2014 to assess the perception of 121 respondents from six different law enforcement agencies. In 2017, the same ICP survey was conducted on representatives from 28 law enforcement agencies and government agencies, and 3 supervising agencies. Response/return rate of individuals who answered the survey vis-à-vis the number of people in the sample is at 97.8%.

Arithmetic mean (central tendency) of the responses to this ICP survey stands at 0.8 or a "Very High" rating. Scores within this range mean that ML prosecutors are perceived as highly ethical. This reflects the respondent's general impression that the subjects will not engage in some unethical/integrity-compromising behavior under certain conditions.

Arithmetic mean (central tendency) of the responses to this ICP survey stands at 0.50 or a "Moderate" rating. Scores within this range mean that FC/ML prosecutors are perceived as moderately ethical. This echoes the respondent's general impression that the subjects might engage in some unethical/integrity-compromising behavior under certain conditions.

The ICP survey results indicate that within the present sample population, financial crime/money laundering prosecutors and investigators are perceived to act with a high level of integrity under most circumstances.

# Capacity and Resources for Financial Crimes Prosecutions and Integrity and Independence of Financial Crimes Prosecutors

Civil forfeiture proceedings have been instituted against prominent government officials involved in plunder, graft and corruption cases. Prosecution of cases were not impeded or delayed by outside interference. Likewise, the courts have issued orders based on objective evaluation of the evidences gathered by AMLC financial investigators. The prosecution of the crime of money laundering is initiated by the AMLC through the assistance of the DOJ or Office of the Ombudsman (OMB), where it may be appropriate. As of 2017, the AMLC has fifteen (15) lawyers, three (3) of which are ACAMScertified, tasked to evaluate investigation reports and prepare pleadings, motions, and other documents in relation to bank inquiry, freeze order, civil forfeiture, filing of money laundering cases and other related proceedings.

The survey was also used to determine the perception of LEAs, and other government agencies on the AMLCS, the OMB and DOJ regarding their integrity and capacity. The AMLCS, OMB and DOJ obtained ratings ranging from high to very high which mean they are perceived as independent and impartial in the resolving cases.

The prosecution of the money laundering is done by the AMLC through the DOJ or the OMB as the case may be. The AMLC files civil forfeiture cases, petitions for the issuance of freeze order and applications for an order allowing bank inquiry through the Office of the Solicitor General (OSG). The AMLC has a good working relationship with the DOJ, OMB and the OSG, as embodied in the existing MOAs with the said agencies. Regular case conferences and meetings are being conducted to ensure that money laundering cases are prosecuted efficiently and effectively.

Presently, there are at least seventeen (17) lawyers from the OSG who handle AMLA related cases. This number is sufficient for the timely filing, and speedy and effective prosecution of AMLA cases. OSG lawyers are given allowances to effectively perform their functions. The AMLC is also ready to provide logistical support to OSG lawyers as the need arises.

The DOJ is the main agency of the Government which prosecutes criminal offenders after preliminary investigation. As a matter of procedure, the AMLC is the one who files a complaint-affidavit for ML before the DOJ which then issues a subpoena to the suspect/respondent for him/her to file his counter-affidavit to oppose the charge. The respondent(s) has ten (10) days to respond with copies of documents and other facts disproving the case against him/her. It is usual that the respondent can seek two extensions of time. The prosecutor conducting the preliminary investigation has 60 days to make a recommendation and refer the matter to the chief prosecutor. If after the preliminary examination probable cause exists, the DOJ will file the case in court. The DOJ then acts as the prosecutor for the AMLC.

There are twenty (20) to twenty-three (23) lawyers handling money laundering cases in the DOJ. This allows the timely and exhaustive evaluation during preliminary investigation of criminal complaints

for money laundering filed by the AMLC, and in cases where the respondents are charged in court, effective and efficient prosecution thereof.

On the other hand, the OMB is the prosecuting arm of the government for public officials violating the Anti-Graft and Corrupt Practices Act. It also prosecutes public officials committing money laundering. The procedure in the OMB is very much the same with the DOJ with the filing by the AMLC of a complaint-affidavit, and submission of counter-affidavit by the respondent.

The AMLC Secretariat regularly conducts AML/CFT training courses for DOJ and OMB prosecutors and OSG lawyers involved in the prosecution of AML/CFT cases. Resource speakers from the AMLC Secretariat discussed topics on the AMLA, as amended, and its RIRRs; R.A. No. 10168 (Terrorist Financing Prevention and Suppression Act of 2012); Asset Recovery and Forfeiture; and Financial Investigation relative to ML/TF. The operational budget of the DOJ, Office of the Ombudsman and the OSG is provided for in the Annual Budget of the government, or the General Appropriations Act of 2017. These agencies are the ones who forecast their budget needs for the year and proposes the projected budget to Congress. This budget allocation covers the salary, allowances, and other financial benefits of all their employees including those handling money laundering cases. The allocated budget also allows these agencies to purchase equipment and materials to enable their employees, including those handling ML cases, to effectively perform their duties.

Integrity and Capacity Survey (ICP) was also used to determine the perception of LEAs, and other government agencies on the AMLCS, the Ombudsman (OMB) and Department of Justice (DOJ) regarding their capacity to handle cases. The OMB and DOJ obtained satisfactory ratings ranging from **Medium to Medium High**.

## **Effectiveness of Domestic Cooperation**

AMLC Resolution No. 59, Series of 2006 authorized the AMLC Secretariat to furnish domestic LEAs and other concerned government agencies which have existing MOAs with the AMLC, information that may be relevant to the analysis or investigation of persons or companies involved possibly involved in money laundering/terrorist financing activities.

For the period 2011-2016, the AMLC Secretariat received requests for assistance from various government agencies and law enforcement agencies such as the PDEA, National Bureau of Investigation (NBI), DOJ, Philippine National Police (PNP),BSP, SEC, Office of the Ombudsman, Bureau of Internal Revenue (BIR), Philippine Center for Transnational Crime (PCTC) Interpol, Department of Foreign Affairs (DFA), Department of Finance (DOF), Insurance Commission (IC), Philippine Deposit Insurance Corporation (PDIC), Presidential Anti-Organized Crime Commission (PAOCC), Presidential Commission on Good Government (PCGG), among others. These requests for assistance involve requests for information, investigation of the predicate crimes and for the possible freezing and confiscation of its proceeds, if there are any.

For 2016 alone, the AMLCS received 201 requests for information from 31 different LEAs, and other government agencies. Most of these requests have been acted upon and given due course by the AMLC Secretariat.

Table 2-13. Requests for Assistance

Year	No. of Requests for Assistance
2011	85

2012	123
2013	105
2014	134
2015	84
2016	201

Some of the requests were archived or closed as initial investigation showed that either the crime involved is not a predicate crime to money laundering at the time of the requests or that database search yielded negative results.

The AMLCS is also a member of the National Law Enforcement Coordinating Committee (NALECC) and a number of its sub-committees, and the Joint Terrorist Financing Investigation Group (JTFIG). The NALECC is a policy-coordinating and action-monitoring mechanism for relevant government and law enforcement agencies. It further takes part in formulating law enforcement and regulatory policies and actively participates in the passage of important legislations affecting the country's peace and order, economy and environment.

The JTFIG, on the other hand, is an inter-agency task force composed of the following agencies: Philippine National Police's (PNP) Intelligence Group (IG), Directorate for Intelligence (DI), Anti-Kidnapping Group (AKG), Anti-Cybercrime Group (ACG) and Special Action Force (SAF), and also the National Bureau of Investigation (NBI), and the Philippine Center for Transnational Crime/Interpol (PCTC-Interpol). The JTFIG regularly conducts coordination meetings every Tuesday.

To date, the AMLC has 25 MOAs with different law enforcement agencies and other relevant government agencies.

## **Effectiveness of International Cooperation**

The AMLC, in its Resolution No. 59, Series of 2006, authorized the AMLC Secretariat to furnish, the Member-FIUs of the Egmont Group and other financial intelligence units which have existing Memorandum of Understanding (MOU) with the AMLC, any information that may be relevant to the analysis or investigation of persons or companies possibly involved in money laundering/terrorism financing activities. The AMLC has existing MOUs with 40 financial intelligence units.

The AMLC Secretariat received and sent the requests for information from the Egmont Secure Web (ESW) of the Egmont Group of Financial Intelligence Units:

Table 2-14. Requests for Information through the Egmont Secure Web

	2011	2012	2013	2014		2015	2016	TOTAL
Requests for Information (RFI) received	76	47	79	73	2 <sup>ND</sup> NRA	134	87	496
Requests for Information made	37	124	22	11		163*	15	372

<sup>\*</sup> The AMLCS made a request for information to all FIUs via ESW on one specific case.

Majority of the requests for information (RFIs) were on the identity of the subject or any transaction from the AMLC database. The AMLCS sees to it that these requests for records of transactions are acted within a short period of time. Some RFIs however need information from other sources of data

such as bank records, travel record and criminal records. These requests require more time as the AMLC is not the repository of these information.

Table 2-15. Information Exchanged through the Egmont Secure Web

	No. of Domisets	STATUS OF REQUESTS					
Year	No. of Requests for Assistance	Acted on within 6 Months	Acted on from 6 months to 1 year	Acted on beyond 1 year			
2011	76	66	1	9			
2012	47	36	5	6			
2013	79	55	12	12			
2014	73	39	28	6			
	2 <sup>ND</sup> NRA						
2015	68	65	2	1*			
2016	87	35	18	34*			

<sup>\*</sup> The RFIs require information from law enforcement agencies.

On the other hand, the AMLCS made 372 requests for information, from 2011-2016, to its foreign counterparts for the purpose of tracking down the assets and obtaining relevant information relating to money laundering offense, or any activity related thereto, perpetrated by subjects under investigation.

Mutual Legal Assistance Treaty (MLAT) requests are coursed through the DOJ as the Central Authority of the Philippines. The table below shows the related statistics for the period 2011 to 2016.

Table 2-16. Statistics on Mutual Legal Assistance Through the Department of Justice

Year	2011	2012	2013	2014	2015	2016	
MLA Requests received from other jurisdictions							
MLA on ML	-	7	6	6	1	8	
MLA requested by the Philippines							
MLA on ML	-	-	-	1	1	0	

The aforesaid MLAT Requests involved requests for production of bank records and other financial information, as well as asset freeze and forfeiture. Most of these requests have been acted upon and are given due course by the AMLCS.

# Accessibility of Reliable Information and Evidence

Accessibility to reliable information and evidence is assessed through the quality of the CDD framework, reliability of financial records and books and level of formalization of the economy.

Quality of Criminal Prosecution (Medium High)	Quality of Criminal Investigation	Medium High
	Capacity and Resources for Financial Crimes Prosecutions	Medium High
	Integrity and Independence of Financial Crimes Prosecutors	High
	Accessibility of Reliable Information and Evidence	Medium
	Effectiveness of Domestic Cooperation	High
	Effectiveness of International Cooperation	High

The quality of criminal prosecution assesses the ability and integrity of the prosecutorial services to appropriately initiate and conduct prosecutions of alleged money laundering offenses, including asset forfeiture. It is determined by the assessing the capacity and integrity of ML crime investigators and prosecutors as well as the effective coordination of the financial intelligence unit with is domestic and international counterparts. These AML controls are assessed in the section on Quality of Criminal Investigation.

Quality of Adjudication (Medium High)	Quality of Criminal Prosecution	Medium
	Capacity and Resources for Judicial Processes	Medium High
	Integrity and Independence of Judges	Medium High

The quality of adjudication assesses the capability and integrity of the judges/judicial officials to preside over prosecutions for money laundering offenses, including asset forfeiture in a professional and appropriate manner. Primarily, this evaluates the quality of criminal prosecution in conjunction with the assessment on the capacity and integrity of judges in presiding over prosecutions for money laundering offenses.

## Capacity and Integrity of Judges

Members of the Philippine judiciary regularly undergo trainings/seminars on new laws and jurisprudence at the Philippine Judicial Academy (PhilJA). The AMLA is a regular part of the curriculum in the said training. AMLC Secretariat personnel conduct approximately thirty (30) seminars/lectures/workshops for PhilJA on topics covering the AMLA, investigation and prosecution of money laundering cases, as well as the latest AML trends and measures.

During their AMLA training, magistrates are given updates on latest amendments to the AMLA, if any, and ML methods committed in the Philippines, including the remedies available to the government (i.e. forfeit proceeds of crime, freezing of assets and other properties suspected of being proceeds of unlawful activities). Judges and Justices are also apprised of the remedy of bank inquiry into the accounts of criminals.

The Supreme Court also promulgated A.M. No. 05-11-04-SC (Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, And Freezing of Monetary Instrument, Property, or Proceeds, Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense Under

Republic Act No. 9160, as amended), which serves as the primary rule of procedure to be observed by courts when handling petitions for issuance of freeze orders and for civil forfeiture cases and provide for provisional remedies available to the AMLC.

Under the Philippine Constitution, the judiciary enjoys fiscal autonomy. It also administers the Judiciary Discretionary Fund (JDF) which it may use to upgrade court facilities and equipment nationwide. Such fiscal autonomy and discretionary fund ensure that courts would be given the facilities they need to be conducive to the effective administration of justice. The Judiciary's budget also increases every year. Under the 1987 Constitution, Congress may not reduce the yearly appropriation for the Judiciary below the amount of the previous year.

With reference to the 1<sup>st</sup> NRA, in the Philippines, the conduct of judges and justices of collegiate courts, is governed by the New Code of Judicial Conduct (A.M. 03-05-SC) (hereafter Code) promulgated by the Philippine Supreme Court on 27 April 2004. The Code, patterned after the Bangalore Draft of the Code of Judicial Conduct, consists of six (6) Canons highlighting the standards that should be observed by judges and justices in the discharge of their official functions of administering justice and deciding cases.

Canon 1 of the Code directs judges and justices to uphold and exemplify judicial independence free from any extraneous influence, inducement, pressure, threat or interference, whether direct or indirect.

Canon 2 of the Code provides for the directive for judges and justices to maintain integrity in the proper discharge of the judicial office.

A Code of Judicial Conduct, no matter how wisely crafted, does not necessarily translate into ethical conduct on the part of magistrates. It is, however, certain that without a Code of Conduct a judge will find it difficult to navigate ethically through the mined waters of professional conduct and even in their everyday life as a judge. Prudence is certainly a necessary virtue, but the gray areas are many, and the questions they raised, difficult.

Violations of the Code may subject the offending judge or justice to criminal and administrative sanctions. For instance, a magistrate who accepts or asks money in exchange for a favorable ruling on a matter before him could be held liable for direct bribery punished under the Revised Penal Code. A magistrate who knowingly renders an unjust decision may also be held criminally liable therefor.

Administrative sanctions may include suspension or dismissal from the judiciary. Under the Philippine Constitution, only the Supreme Court can resolve administrative actions against judges and justices. There have been a number of judges and justices who have been meted administrative sanctions by the Supreme Court.

Although appointed into office by the President, members of the judiciary may only be removed from office by the Supreme Court. This somehow shields judges and justices from external pressures, specifically threats involving their removal from office, in exchange for a favorable ruling or judgment.

The AMLC is authorized to file ML Criminal Complaints before the DOJ or the Office of the Ombudsman. Upon finding probable cause that a money laundering offense has been committed, the DOJ or the Office of the Ombudsman files the Information before the Regional Trial Court (RTC) or the Sandiganbayan (i.e. anti-graft court), Below is the statistics on cases filed before the RTC and the Sandiganbayan.

Table 2-17: Number of Cases Filed before the Regional Trial Court and the Sandiganbayan

Money Laundering	2011	2012	2013	2014		2015	2016	Total
Civil Forfeiture Cases	6	8	5	8		8	9	44
filed before the RTC					- ND			
ML Criminals Cases	-	5	3	1	2 <sup>ND</sup>	4	2	15
filed before the RTC					NRA			
ML Criminal Cases	-	-	-	-		-	-	0
filed before the								
Sandiganbayan								
Total	6	13	8	9		12	11	59
	Ū		Ŭ					

In the June 2017 survey conducted by the AMLCS, the SB obtained a fairly acceptable rating on their perception on their capacity and integrity. The RTC/SC, on the other hand, obtained a fairly satisfactory perception rating, which means that they are perceived to be independent and impartial in the performance of their functions.

Considering the perception survey and the number of actions on the cases filed before them, the overall judiciary process is rated as **MEDIUM HIGH.** 

	Quality of FIU Intelligence Gathering and Processing	Medium
	Capacity and Resources for Financial Crime	Medium
	Investigations	High
	Integrity and Independence of Financial Crime Investigators	High
	Capacity and Resources for Financial Crimes	Medium
	Prosecutions	High
Quality of Asset Forfeiture	Integrity and Independence of Financial Crimes Prosecutors	High
Framework (Medium)	Capacity and Resources for Judicial Processes	Medium High
	Integrity and Independence of Judges	High
	Accessibility of Reliable Information and Evidence	Medium
	Effectiveness of Domestic Cooperation	High
	Effectiveness of International Cooperation	High
	Comprehensiveness of Asset forfeiture laws	High

The quality of asset forfeiture framework assesses the ability of the country to undertake ML/TF asset forfeiture matters that will result in effective asset forfeiture investigations, appropriate asset forfeiture orders and in the successful forfeiture of the proceeds and instrumentalities of crime. To determine the quality of AF framework, the comprehensiveness of asset forfeiture laws is assessed alongside with the capacity and ability of the FIU to conduct analysis, investigation and prosecution, and forfeiture of assets, capability and independence of the judicial process, and effectiveness of domestic and international cooperation. These primary functions of financial intelligence gathering and investigation, forfeiture of assets and prosecution of ML/TF offense, are all assessed in the previous section under the quality of criminal investigation and prosecution.

The *capacity, resources, and integrity of the judges,* as discussed in the section **Quality of Adjudication**, are likewise necessary in determining the effectiveness of the country to undertake judicial processes for cases relating to money laundering offenses and their related predicate offenses or unlawful activities. This takes into account the skills, experience and power to preside over prosecution for ML offenses. The lack of understanding and technical knowledge on money laundering and the financial system, including financial crimes, and lack of financial and human resources are some of the major impediments to effectively and fairly execute judgments on money laundering offenses.

## **Comprehensiveness of Asset Forfeiture Laws**

Sections 10 (Freezing of Monetary Instrument or Property), 11 (Authority to Inquire into Bank Deposits), and 12 (Forfeiture Provisions) of the AMLA, as amended, provide invaluable tools in the recovery of proceeds of crimes. AMLC financial investigators can only examine bank accounts or investments which are specifically mentioned in the order issued by the Court of Appeals. If in the course of the examination other accounts were discovered, these newly discovered accounts may not be inquired into or examined unless a new court order, or an AMLC Resolution, as the case may be, is secured. During bank inquiry or examination, banking institutions are duty-bound to provide AMLC financial investigators with all papers, documents, bank records, statements, pertaining to the accounts examined.

In 2016, the AMLC filed 13 petitions for the issuance of freeze order with total estimated amount of PhP2,977 billion. This is 425% higher compared to the previous year. Ten (10) of these petitions were issued on cases on illegal drugs while the remaining three (3) petitions were filed on other predicate offenses<sup>96</sup>.

Table 2-18 Petitions for the Issuance of Freeze Order filed with the Court of Appeals

Year	No. of Petitions Filed	Amount Subject of Freeze Order (in PhP Millions)
2011	14	541.48
2012	9	614.90
2013	8	614.63
2014	9	416.85
	2 <sup>ND</sup> N	RA
2015	8	567.36
2016	13	2,977.12

Not all subject of freeze orders resulted in the filing of petitions for civil forfeiture, as a result of the bank inquiry or investigation report.

-

<sup>&</sup>lt;sup>96</sup> Chapter 1. Threats Assessment, 2<sup>nd</sup> NRA

Table 2-19. Petitions for Civil Forfeiture filed before the Regional Trial Court

Year	No. of Petitions Filed	Estimated Amount Subject of Civil Forfeiture (in PhP Millions)
2011	6	584.05
2012	8	148.02
2013	5	370.63
2014	7	416.85
	2 <sup>ND</sup> NRA	
2015	8	302.77
2016	6	750.97

As of December 2016, the estimated amount forfeited is 67.80% higher compared to the PhP4.0 billion estimated amount forfeited in 2014 (previous NRA). The PhP 718.91 million subject of the petition for Civil Forfeiture were returned to the victims, particularly in relation to the Bangladesh Bank cyber heist.

Since the last NRA, there has been an increase in the number of forfeiture orders secured from the courts, and amounts of criminal proceeds forfeited and returned to victims. This only shows that asset forfeiture laws are effective as it facilitates the preservation and eventual confiscation of criminal proceeds. Table below shows the assets frozen and forfeited as of December 2016.

Table 2-20. Statistics on Asset Forfeiture Orders

	Amount in Peso-Equivalent				
Asset Forfeiture	As of 31 December 2014 <sup>97</sup>	As of 31 December 2016			
Total amount Forfeited and Remitted to the Phil Government	PhP 43,427,042.38	PhP 48,856,022.69			
Total amount Forfeited and Turned over to the Office of the Ombudsman	92,521,864.38	100,706,673.99			
Total amount Forfeited and Returned to the Victims	2,401,568.50	718,914,190.00			
Total amount Forfeited but Pending Execution (Judgment Final and Executory)	20,635,833.68	10,269,987.67			
Total amount Lifted Returned to the Victims/Investors	1,497,611,493.14	1,585,786,511.47			
Total estimated amount subject of Pending Civil Forfeiture Cases (includes PhP-equivalent values of foreign-denominated currencies <sup>98</sup> )	2,284,006,759.66	2,637,700,276.91			
Total estimated amount subject of Pending Freeze Orders (includes PhP-equivalent values of foreign-denominated currencies <sup>99</sup> )	37,528,184.07	1,591,150,921.65			
Total amount subject of Other Forfeiture Actions	26,682,589.19	26,788,726.27			
Total	PhP 4,004,815,335.00	PhP 6,720,173,310.65			

<sup>&</sup>lt;sup>97</sup>Statistics on Asset Forfeiture Orders as of 31 December 2014, based on previous NRA report.

<sup>98</sup> Based on exchange rates as of 31 December 2016

<sup>99</sup> Ibid.

National ML combating ability (Medium High)	Quality of AML Policy and Strategy	Medium High
	Effectiveness of ML crime definition	High
	Quality of Cross-border Cash Controls	Medium
	Quality of Criminal Investigation	Medium High
(meanannigh)	Quality of Criminal Prosecution	Medium High
	Quality of Adjudication	Medium High
	Quality of Asset Forfeiture Framework	Medium

The national ML combating ability determines the country's effectiveness to prosecute and penalize instances of money laundering offenses and to forfeit the proceeds and instrumentalities of crime. It is assessed through inter-related AML combating controls. Overall assessment shows that while the country has AML controls in place, the national ML combating ability is rated **MEDIUM HIGH**.

## **OVERALL NATIONAL VULNERABILITY**

Casinos, MSBs, Banking, Pawnshops and E-Money Issuers rank 1 to 5, in terms of the most vulnerable sectors and thus, need to be prioritized. Meanwhile, Dealers in Precious Metals, Lawyers and Accountants, have the lowest weighted vulnerability ratings. The overall sector vulnerability is rated **MEDIUM HIGH**.

The overall vulnerability assessment considering the sectoral vulnerability and National Combating Ability is **MEDIUM HIGH.** 

#### **ACTION PLAN**

Based on the identified weaknesses and deficiencies in the priority variables for the national vulnerability, the following are the recommended action plans:

ACTION PLAN	PRIMARY AGENCY	TIMELINE
Develop National AML/CFT Strategy	AMLC, Supervisors	Jan - Dec 2018
• Identify best practices in other jurisdictions and their	BSP, SEC and IC,	
possible application to the Philippine setting	Office of the	
Close coordination with supervising agencies, law	President, Other	
enforcement agencies, and other stakeholders, and	Supervising	
engage them to actively participate with regard to	Agencies, Law	
the AML/CFT initiatives	Enforcement	
• Coordinate with the Office of the President for the	Agencies and	
possible issuance of an Executive Order	Covered persons	
disseminating the national policy on AML/CFT	and other relevant	
• Formalization of information-exchange sharing	agencies	
agreements with law enforcement agencies (through		

<sup>100</sup> Banking, Securities, Insurance, Other Financial Institutions and Designated Non-Financial Businesses and Professions (DNFBPS) sectors vulnerabilities are assessed in Chapters 3 , 4, 5, 6, and 7.

the issuance of MOAs and creation of committees for AML/CFT initiatives)		
Regular updating of the NRA  • Periodic review and update, if necessary, of AML laws, rules and regulations  Conduct strategic analysis studies on ML or AML risk assessments taking into account developing trends that may warrant changes in the AML framework consistent to international standards		
Capacity building for all financial analysts, investigators and prosecutors  Trainings on financial investigation techniques, ML trends & typologies, and Asset Forfeiture  Improve (or design) the process of STR/CTR analysis system	AMLC, DOJ, OSG, OMB, LEAS, CPS	2017 onwards Continuing action
<ul> <li>Effective and timely coordination and/or strengthen coordination with law enforcement and other agencies, as well as with the covered persons</li> <li>Strengthen intelligence analysis system from CP reporting, to analysis, investigation and dissemination of information) through trainings, workshops</li> <li>Increase CPs' awareness in reporting through</li> </ul>		3rd Quarter 2017 to 4th Quarter of 2018
<ul> <li>trainings (Strict implementation of AML laws);         STR/CTR quality, risk-based assessment, revisit         STR/RFI prioritization and classification)</li> <li>Conduct training programs to CPs on recent trends         and best practices in the AML compliance and         reporting of other jurisdictions. This will build their         knowledge on the AML/CFT compliance.</li> <li>Access to other sources of information, such as LEAs and         govt. databases, CIF/CAIF/ID docs of clients from CPs.</li> </ul>		3rd Quarter 2017 to 4th Quarter of 2018 3rd Quarter 2018
Capacity building for all judges and justices in relation to ML/TF trends and typologies  Increase in the capacity or number of officers handling ML cases  Trainings with regard to ML investigation, trends & typologies, and asset forfeiture.  Effective and timely coordination/ strengthen coordination with law enforcement and the AMLC  This will equip the officers with information that would facilitate them in handling ML cases, which eventually may result in the Increase in the number of ML-related cases	AMLC, Regional Trial Courts, Sandiganbayan, Supreme Court - OCA	Start date: 1st Quarter 2018, continuing AML/CFT training
decided.  Strengthen border controls  • Effective Coordination with the BOC, OTS, Phil. Coast Guard	BOC, OTS, PCG AMLC,	3rd Quarter 2017 to 4th Quarter 2018

		<u> </u>
<ul> <li>Acquire or develop tools, systems and other mechanisms that the agency/ies can use to detect cross-border-related offenses</li> <li>Develop cooperative arrangements and/or committees to identify areas that need improvement and formulate policies to address the same.</li> <li>Capacity building (Increase in the capacity and resources)</li> </ul>	BSP, and other relevant agencies	(coordination with the BOC with regard to the AML/CFT initiatives)
Conduct trainings on AML/CFT, ML/TF cross- border typologies  Revisit systems by a separations.		
<ul> <li>Revisit customs laws and regulations</li> <li>Financial inclusion as strategic objective</li> <li>Continued support to the National Strategy Financial Inclusion of the BSP and other 14 government agencies (CFO, CDA, DBM, DepEd, DOF, DSWD, DTI, IC, NEDA, PDIC, PSA, EC, DAR, DOST)</li> <li>Regular educational AML/CFT campaign to financial service providers (ABROI, ABCOMP, RBAP, CTB, etc), stakeholders and partners, and the public.</li> <li>The AMLC may look into the possibility of issuing AML/CFT-related policies that will encourage financial inclusion</li> </ul>	BSP, AMLC, Government agencies mentioned, and covered persons committed to provide financial service to the underserved/ unbanked sector	Ongoing
Enhance the mechanisms currently in place to address the requirements for FI (i.e. simplified payment systems)  Microfinance loans, remittance through pawnshops, emoney service		
Propose the inclusion of tax evasion and other tax- related crimes as one of the predicate offenses to money laundering under the AMLA, as amended, pursuant to the recommendation of the FATF.	AMLC, BIR	2nd quarter 2018
Effective and timely coordination/strengthen coordination with Bureau of Internal Revenue and the AMLC. Encourage referrals of tax-related violation cases for ML investigation		1st quarter 2018
These AML controls determine the quality of CDD framework.	AMLC, BSP, SEC, IC, CIC, Industry Associations	
Creation of a nationwide or centralized information bureau that will maintain a database of client information  • For easier verification of identity of persons/corporate representatives/stockholders/ beneficial owners		Ongoing study
		Ongoing study

Monitor progress of ID systems developed by	AMLC, BSP, SEC, IC	
government agencies as alternative to a national ID	and Covered	
system	persons	
Identify best practices of covered persons under the		
BSP, SEC and IC on how to conduct identity verification		
through available sources		
<ul> <li>Sharing of information on the detection of fake</li> </ul>		
IDs and documents		
Sharing of validation procedures by CPs under the BSP,		
SEC and IC, and if necessary, the SA can issue		
circulars/guidelines of the KYC/CDD procedures		

#### III. BANKING SECTOR VULNERABILITY

#### **EXECUTIVE SUMMARY**

The total assets of the banking system as of end of 2016 amounts to PhP13.9 Trillion<sup>101</sup>. This accounted for 96%<sup>102</sup> of the Gross Domestic Product (GDP) of the country's (PhP14.5 Trillion). The 2016 total assets grew by 11.8% from 2015 level. Growth in the banking system's assets is mostly funded by savings and demand deposits. Total deposits as at end-2016 stood at PhP10.5 trillion, posting a growth of 13.8%. Deposits are primarily peso-denominated and sourced from resident individual depositors<sup>103</sup>.

Given the status of banks in the financial system, the products and services they offer to clients, banks remain to be the main avenue used by money launderers to obscure the illegal sources of their funds and other assets. Thus, the banking sector is **HIGHLY** vulnerable to ML and TF.

This vulnerability is, however, mitigated and addressed by the existence of AML/CFT legal and regulatory and institutional framework which are generally consistent with international AML/CFT standards. There are also appropriate mechanisms to regularly assess compliance by banks of these legal and regulatory AML/CFT framework and exact enforcement of the same.

The quality of general AML controls is assessed to be **MEDIUM**. Thus, resulting to the **MEDIUM** overall vulnerability of the banking sector.

#### **INTRODUCTION**

The banking sector plays a vital role in the country's financial system and economy, through financial intermediation and payments processing. At the end of 2016, the assets (PhP13.9 Trillion<sup>104</sup>) of the banking system accounted for 96%<sup>105</sup> of the Gross Domestic Product (GDP) of the country (PhP14.5 Trillion). The end-2016 total assets grew by 11.8% from 2015 level. The top five banks in the country — composed of four universal banks and one government bank — accounted for 53% of the total assets of the Philippine banking system. In total, universal and commercial banks assets comprised 88% of the banking system.

Growth in the banking system's assets is mostly funded by savings and demand deposits. Total deposits as at end-2016 stood at PhP10.5 trillion, posting a growth of 13.8%. Deposits are primarily peso-denominated and sourced from resident individual depositors<sup>106</sup>.

In terms of physical network, physical offices are increasing due to additional offices of universal/commercial banks and new foreign bank entrants. Distribution of offices are, as follows: (http://www.bsp.gov.ph/statistics/statpnnopbs.asp)

\_

 $<sup>^{101}</sup>$  Report on Economic and Financial Developments, Fourth Quarter 2016

<sup>102</sup> ibid

<sup>&</sup>lt;sup>103</sup> http://www.bsp.gov.ph/downloads/Publications/2016/StatRep\_2Sem2016b.pdf

<sup>&</sup>lt;sup>104</sup> Report on Economic and Financial Developments, Fourth Quarter 2016

<sup>105</sup> ihid

 $<sup>^{106}\</sup> http://www.bsp.gov.ph/downloads/Publications/2016/StatRep\_2Sem2016b.pdf$ 

December 2014 December 2016 December 2015 Bank **Total** Head Branches/ **Total** HO **Branches/ Total** HO **Branches** Other Other Category Office / Other (HO) Offices Offices Offices UBs/KBs 6,237 42 6,195 6,060 40 6,020 5,833 36 5,797 TBs 1,920 2,176 60 2,116 2,086 68 2,018 69 1,851 RBs/Coo 2,765 500 2,610 524 2,086 2,608 543 2,065 2,265 All Banks 11,17 602 10,576 10,75 632 10,124 10,361 648 9,713 8 6

Table 3-1. Distribution of Offices of Banks

These banks/offices are mostly located in highly urbanized and populous areas of the National Capital Region, Calamba, Laguna, Batangas and Quezon Region (CALABARZON) and Central Luzon where it is economically viable to maintain a brick and mortar branch.

Overseas, most bank branches or offices are located in the Middle East and Asia Pacific Regions, which is reflective of the strong presence of Filipino migrant workers in these regions. Bank density ratio was maintained at 7 banks per city/municipality since 2015. Demographic penetration was 16 banks per 10,000 Filipinos. <sup>107</sup>

These foreign offices, as well as remittance desk offices in the Middle East, Asia, Americas and Europe facilitated strong remittance inflows coursed through the banks, which translated into accessible financial services, deposit accounts, and investment instruments for recipients/beneficiaries.

The BSP advocates financial inclusion to contribute to inclusive growth towards poverty reduction and easier access for all Filipinos to various financial services and products offered by banks and other financial institutions. Thus, there was noted increase in the so-called "light branches" or other banking offices/micro banking offices that served as additional financial access points for the effective delivery of banking services, particularly in the countryside. Aside from physical network, the BSP allowed banks to engage in electronic banking as early as the year 2000. Banks engaged in electronic banking grew from 9 banks (2000) to 119 banks (2016). In addition, the use of electronic money (e-money) is increasing, as exhibited in the rise in number of participating financial institutions and volume of transactions. As at end 2016, net inflow of e-money transactions reached PhP1.1 trillion, 78.2 percent of which were coursed through banks. There were 29 bank electronic money issuers (EMIs), 2 non-bank EMIs, 5 other EMIs and 3 electronic money network service providers (EMNSPs). These pioneering regulatory innovations preceded the recent trend of regulatory sandboxes.

# **DATA AND INFORMATION COLLECTION**

Quantitative information on relevant banking industry statistics were gathered from available resources, such as the BSP and Anti-Money Laundering Council Secretariat (AMLCS)<sup>108</sup>, supplemented by a survey on other data not covered by existing prudential reports. The survey covered a

<sup>&</sup>lt;sup>107</sup> Status Report on the Philippine Banking system, 2<sup>nd</sup> Quarter 2016

<sup>&</sup>lt;sup>108</sup> Statistical data from the Supervisory Data Center of BSP, economic data from the BSP website, statistics on CTRs/STRs and cases filed provided by the AMLC and summary data on the results of AML examination.

representative majority of the banking industry (representing more than 70 % of the industry), as follows:

- a. Universal and Commercial Banks;
- b. Top 20 Thrift and Savings Banks; and
- c. Top 10 Rural Banks.

These banks were required to accomplish a template to collect additional quantitative information on major products/services offered (such as turnover, volume of transactions, risk profile of clients, and data on CTRs and STRs related thereon), as well as details to support the assessment of the 13 general input variables.

In June 2017, the group held a focus group discussion (FGD) to discuss the different AML general controls. This was attended by the compliance and AML officers from the industry, and representatives from the BSP and the AMLC Secretariat. The FGD allowed the parties to share their expertise and experiences on the identified areas of concern thereby providing the group better appreciation and perspective on the different variables. It was also a venue for the group to identify areas for improvement and suggest recommendations thereon. Upon completion of the FGD, initial assessments were reached for each of the 13 variables and the products risk assessment.

Overall, this NRA banking sector vulnerability assessment is a result of collaboration and cooperation between various stakeholders backed by quantitative and qualitative information gathered from reliable sources<sup>109</sup>.

#### SECTOR VULNERABILITY ASSESSMENT

The banking sector, with its role as financial intermediary and wide network coverage, is inherently vulnerable to ML/TF. Given the status of banks in the financial system, the products and services they offer to clients are among the means favored by money launderers to obscure the illegal sources of their funds. This vulnerability is, however, mitigated and addressed by the existence of legal and regulatory AML/CFT framework, which is generally consistent with international AML/CFT standards, including mechanisms to enforce their implementation and continually assess compliance thereon. Most banks have established ML/TF risk management system appropriate to their risk profile and complexity, which are being reviewed during the regular examination conducted by the BSP. Furthermore, there is a continuing and coordinated efforts among various stakeholders, comprised of the government, supervisory or regulatory agencies, banks and financial institutions, to prevent the use of the banking sector for ML/TF activities.

Nevertheless, the BSP recognizes that ML/TF landscape is dynamic. Thus, it requires focused and sustained efforts to continue improving the legal and regulatory framework and more importantly, to ensure effective implementation of the AML/CFT laws, rules and regulations. These include the need to improve on the availability and access to beneficial ownership information to facilitate conduct of due diligence on customers. Also, supervised banks and FIs need to enhance their existing AML/CFT policies and procedures and the implementation of the same, and improve their monitoring system to proactively identify unusual activities or possible suspicious transactions. Human resources dedicated for AML/CFT activities must also be increased. AML/CFT awareness, in addition to the knowledge and skills of both the officers of the regulators and the officers and staff of supervised

\_

The Group recognizes that certain limitations were encountered such as, non-availability of other data, inaccuracy in certain data provided, and time constraints in data/information collection. Nonetheless, the Group believes that these do not significantly impair the overall assessment/findings. Moving forward, these constraints shall be treated as areas for improvement to enhance data and information collection and gathering.

banks and FIs must be also be developed to succeed in our fight against ML/TF.

In this regard, the overall banking sector vulnerability is <u>MEDIUM</u> resulting from assessment of the relevant variables discussed below.

#### **ASSESSMENT OF VARIABLES**

Quality of AML Supervision	Effectiveness of Supervision/Oversight Activities	Very High
(Medium High)	Availability and Enforcement of Administrative Sanctions	Medium

# Effectiveness of Supervision/Oversight Activities

The BSP supervises banks, quasi-banks, trust entities, non-stock saving and loans associations (NSSLA), as well as other non-bank financial institutions pursuant to Section 25<sup>110</sup> of R.A. No. 7653 otherwise known as The New Central Bank Act. Further, it regulates remittance companies, foreign exchange dealers/money changers which are subsidiaries and affiliates of BSP-supervised entities pursuant to Section 80 of RA 7653 and the AMLA, as amended. Section 11 of the AMLA, as amended, also authorizes the BSP to check compliance of covered persons under its jurisdiction with AML laws, rules and regulations. The BSP exercises AML supervision through the issuance of policies and regulations, continuing off-site supervision, and the conduct of regular or special examination, including structured meetings and dialogues with supervised institutions.

The BSP conducts regular or periodic examination once a year, with an interval of twelve (12) months from the last date thereof, and/or special examinations when authorized by the Monetary Board with an affirmative vote of five (5) of its members. Effectively, all banks are subjected to a periodic examination, which includes assessment of their compliance with AML/CFT laws and regulations. For 2015 and 2016, examinations of banks/NBFIS, money service businesses and NSSLAS, and inspection of pawnshops are, as follows:

Table 3-2. Statistics on Examinations

Institution	2015	2016
Banks	544	506
Non-Banks (subsidiaries of banks)	36	43
Non-stock savings and loan associations	38	39
Money service business	11	51
Pawnshops (inspection)	491	330

The Anti-Money Laundering Specialist Group

The Anti-Money Laundering Specialist Group (AMLSG) is the technical unit in the BSP's Supervision and Examination Sector (SES) that specializes in the review and assessment of the AML/CFT framework of covered persons under the supervision of the BSP. It conducts onsite examination of banks/NBFIs/MSBs, and research and review of policy to ensure that the AML/CFT regulatory framework are updated and relevant. It also provides AML/CFT trainings to various stakeholders, and

<sup>110</sup> The Bangko Sentral shall have supervision over, and conduct period or special examinations of, banking institutions and quasi-banks, including their subsidiaries and affiliates engaged in allied activities.

maintains harmonious working relationship with the industry and other regulatory agencies to ensure policy coordination and enhancement of the AML/CFT framework of the banking industry.

Currently, there are 30 AML examiners in the AMLSG dedicated to fulfill the Group's functions and responsibilities. Consistent with risk-based supervision, the AMLSG prioritize banks/FIs to be examined based on materiality and risk (AML risk rating, products, customers, etc.)

In terms of asset size, the banks examined by the AMLSG comprise of more than 70% of the total assets of the banking system representing mostly UBs/KBs. For the other entities not examined by the AMLSG, the general examination departments<sup>111</sup> conduct the on-site supervision while the central point of contact departments<sup>112</sup> generally handles the offsite supervision and monitoring. This set up provides appropriate check and balance in the supervisory process. The AMLSG, upon authority by the Monetary Board, also conducts special examinations on highly meritorious cases. From 2011 to 2016, the BSP has conducted three (3) special examinations covering several banks/FIs triggered by national interest issues and cases.

However, the number of covered persons under BSP supervision/regulation and dynamic AML/CFT landscape warrant strengthening of the structure and resources of the AMLSG to cope with the increasing demand of an effective AML supervision. This includes the need for continuing capacity building activities. There is also a need to revisit and update the Revised Examination Manual for Anti-Money Laundering and Combating the Financing of Terrorism Activities (REMACA) and Anti-Money Laundering Risk Rating System (ARRS) to reflect changes in the AML/CFT landscape.

## Adoption of AML examination procedures

In 2013, the Monetary Board approved the REMACA to facilitate uniform conduct of AML examination. The REMACA contains specific procedures to be performed during AML examination across supervised institutions, with due consideration to proportionality to ensure that procedures are relevant to the business and complexity of the entity examined. The REMACA facilitates consistent conduct of AML examination across institutions and examination departments. There is also a need to revisit and update the REMACA to reflect changes in the AML/CFT landscape.

# The AML Risk Rating System (ARRS)

The BSP, consistent with risk-based approach to supervision, adopted in 2012 an AML Risk Rating System (ARRS)<sup>113</sup>. This is in accordance with Principle 19 of the Basel Core Principles of Effective Banking Supervision that encourages supervisors to develop and maintain a thorough understanding of the operations of individual banks, banking groups and the banking system as a whole.

The ARRS is the BSP's primary tool to understand whether the AML/CFT risk management policies and practices, internal controls of banks and other FIs are in place, well disseminated and effectively implemented. This also enables the BSP to focus efforts and resources on entities and areas exhibiting higher or elevated AML risk. The ARRS considers four (4) components, namely:

-

<sup>&</sup>lt;sup>111</sup> Examination Departments (EDs) I, II, III, and IV.

<sup>&</sup>lt;sup>112</sup> Central Point of Contact Departments (CPCDs) I, II, III, and IV.

<sup>&</sup>lt;sup>113</sup> Supervision Guidelines 2014-04.

- I Efficient Board of Directors and Senior Management oversight
- II Sound AML policies and procedures embodied in the MLPP
- III Robust internal controls and audit
- **IV** Effective Implementation

Composite rating is assigned based on a numerical scale of 1 to 4.<sup>114</sup> The highest rating (4) indicates the strongest risk management system and most effective operational practices that entail the least degree of supervisory concern. The lowest rating (1) signifies the weakest risk management system and defective implementation requiring the highest degree of supervisory concern. Enforcement action shall also be imposed depending on the overall risk rating of the covered institution.

Since the implementation of the ARRS in 2012, the quality of AML supervision and implementation by banks of their AML/CFT policies are improving given the trend of ratings assigned in the past five years. However, there are still areas of improvements that banks and other FIs need focus in order to effectively manage their respective ML/TF risks.

Board and Senior Management oversight issues have been cited during the first cycles of examination. The related enforcement actions resulted in more conscious, active oversight and participation in ensuring AML/CFT compliance in their organizations. Continuing efforts to enhance implementation of AML/CFT policies particularly on customer acceptance and identification, risk profiling, transaction monitoring and record keeping, among others, have been noted.

Noteworthy are the banking sector's efforts to comply with the AML/CFT regulations and BSP directives. Overall, the BSP recognizes the banks' continuing efforts to strengthen their respective AML/CFT risk management frameworks by investing in new AML systems, increasing manpower complement dedicated to AML/CFT compliance and monitoring, and improving their AML policies, procedures and controls.

The general consensus among banks is that AML supervision in the country is stringent and there are appropriate sanctions for non-compliance, thereby providing strong incentive for Management to enforce compliance with laws and regulations<sup>116</sup>. The BSP, through the AMLSG is committed to continuously improve its supervision and monitoring BSP covered persons. It will also review some component of the ARRS based on lessons learned for the past five years and to capture developments in the AML/CFT landscape.

Cooperation and Information Exchange with the AMLC

In February 2007, the BSP and the AMLC entered into a Memorandum of Understanding (MOU) on cooperation and information exchange. Pursuant to the said MOU, the BSP shall provide the AMLC information on specific AML violations/findings noted during regular or special examination of banks and other FIs. This will provide the AMLC critical information on bank's compliance with AML laws and regulations, and specific AML violations noted during the examination. The AMLC will then conduct its own investigation on the possible violations of banks and other FIs with the AMLA, as amended and its RIRRs, to determine propriety of the imposition of administrative sanctions and institutions of criminal actions.

<sup>&</sup>lt;sup>114</sup> 4 – sound, 3 - adequately sound, 2 - vulnerable, 1 - grossly inadequate.

<sup>&</sup>lt;sup>115</sup> Summary of AML Reports of Examination (2011-2016).

<sup>&</sup>lt;sup>116</sup> Summary of survey questionnaires given to selected banks.

In addition, such information exchange has proven helpful in gathering investigation leads in the development of ML cases instituted by the AMLC. Since banks are aware of this MOU, it creates a positive impact on the overall conduct of personnel of banks and other FIs.

The existing MOU between AMLC and the BSP is currently under review to refine and enrich the information that will be shared between the two agencies to assist in the effective performance of their respective functions.

Dialogue with the Board of Directors and Senior Management of Banks

The BSP Supervision and Examination Sector conducts meeting with the Board of Directors and Senior Management of banks to discuss significant AML/CFT issues and concerns to ensure that the Board will be able to provide appropriate strategic direction to improve the bank's AML/CFT risk management. This also result in directly obtaining the Board's commitment to address the weaknesses noted during examination.

## **Availability and Enforcement of Administrative Sanctions**

The AML/CFT penalty/sanction framework

The AMLC is empowered under Section 7 item 11 of the AMLA, as amended, "to impose administrative sanctions for the violation of laws, rules, regulations and orders and resolutions issued pursuant thereto."

The AMLC, in its Resolution No. 46 dated 24 May 2017, approved the penalty matrix for the imposition of administrative sanctions for violations of the AMLA, as amended, and its RIRRs, particularly with regard to the compliance with the AML/CFT measures. Administrative sanctions consist of monetary penalties, warning or reprimand imposed by the AMLC upon any covered institution, its officers and employees. Fines, taking into consideration the attendant circumstances, are based on the gravity of the violation (e.g. grave, major, serious, less serious and light) and size of the entity (micro, small, medium, large A and large B). Amounts of the fines are determined by the AMLC to be appropriate which shall not be more than PhP500,000.00 per violation and, in no case shall the aggregate fine exceed 5% of the asset size of the respondent.

To further improve the monitoring and imposition of administrative against erring covered persons, which includes the financial institutions under the supervision and/or regulation of the BSP, the AMLC, in May 2017, strengthened its human resources complement. The AMLC established a distinct Compliance Unit in the Compliance and Investigation Group. Similarly, the Litigation and Evaluation Unit (LEU) under the Legal Services Group in the AMLCS was created to conduct preliminary administrative investigations and the filing of Formal Charges against covered persons before the Administrative and Adjudication Unit (AAU), also under the Legal Services Group.

Proceedings of the administrative cases are non-litigious and summary in nature subject to the requirement of due process and substantial evidence. Administrative sanctions are initiated upon referral of the Report of Compliance (ROC) from the Compliance Unit or Report of Examination (ROE) from the BSP to the LEU.

Likewise, BSP Circular No. 706, Series of 2011 (otherwise known as the "Updated AML Rules and Regulations"), as amended by Circular No. 950, Series of 2017, and the BSP Memorandum to All Banks Series (M2012-017) ("AML Risk Rating System") provide that whenever a covered person is assessed to have an overall AML composite rating of "1" (grossly inadequate) based on the result of AML

examination, this may be considered as unsafe or unsound banking practice and may warrant, when considered among other factors, initiation into Prompt Corrective Action (PCA), to ensure that weaknesses warranting immediate action by the Board of Directors are addressed.

The sanctions and penalties under the BSP regulations are, as follows:

- 1. Written reprimand;
- 2. Restriction on certain licenses/product, as appropriate;
- 3. Suspension or removal from the office they are currently holding; and/or
- 4. Disqualification from holding any position in any covered institution for director/officer involved.

In addition to the non-monetary sanctions stated above, BSP may also impose monetary penalties computed in accordance with existing laws and regulations. Enforcement actions shall be imposed on the basis of the overall assessment of the covered person's AML risk management system, observing the established rules on due process.

### BSP's enforcement action

As a result of AML examinations for the past five years, total penalty of PhP1.003 Billion were imposed against 19 banks/NBFIS due to noted weaknesses in their AML/CFT risk management system and non-compliance with BSP's directives. This includes the P1.0 billion penalty imposed on a bank in relation to the alleged hacking incident of accounts of a central bank. Moreover, non-monetary enforcement actions, which include requiring the execution and submission of Board-approved letter of commitment containing specific measures to address the weaknesses noted and governance reforms, were imposed. For the past 5 years, 25 bank officers were administratively sanctioned by the banks through the issuance of either written reprimand, suspension, or termination. The BSP also issued reprimand to 15 officers for violation of their AML-related responsibilities.

It should be emphasized that the sanctions for violations of the above BSP's AML/CFT rule and regulations, shall be without prejudice to the administrative sanctions that could be imposed by the AMLC for violations of the AMLA, as amended, and its RIRRs.

For the period under review, the BSP had imposed administrative sanctions against erring banks and its personnel. On the other hand, the administrative sanctions for violations of AML/CFT under the AMLA, as amended, and its RIRRs, went into effect only in August 2017.

#### Banking institution's own administrative investigation

On the other hand, banks have their respective procedures to handle administrative investigations and sanctions against their errant officers and staff. Banks impose corresponding sanctions and/or penalties for violations of the said laws, regulation, and corporate standards, which range from written reprimand to dismissal from service, and without prejudice to further legal actions depending on the offense.

There is unanimity among stakeholders that there is a well-designed administrative sanction structure for non-compliance with AML obligations and AML-related offenses. The administrative sanction system is regarded as appropriately serious to positively influence behavior of directors, officers and employees and to ensure that covered persons maintain high AML/CFT standards in order to protect its safety and soundness as well as protecting the integrity of the national banking and financial system.

Availability a	and Eff	ectiveness of E	ntry	Controls	Close to Excellent
<b>Quality of</b> Variable)	AML	Supervision	(Inte	ermediate	High
Availability	and	Enforcement	of	Criminal	Medium High
	Quality of Variable)	Quality of AML Variable) Availability and	Quality of AML Supervision Variable)  Availability and Enforcement	Quality of AML Supervision (Intervariable)  Availability and Enforcement of	Variable)  Availability and Enforcement of Criminal

## **Availability and Effectiveness of Entry Controls**

Section 6 of Republic Act (R.A.) No. 8791<sup>117</sup>, otherwise known as The General Banking Law of 2000 (GBL), requires prior authority from the BSP) before an entity can engage in banking operations or quasi-banking functions. Those found to be operating without such authority shall be subject to sanctions under the New Central Bank Act (R.A. No. 7653). Registration of articles of incorporation and by-laws with the Securities and Exchange Commission shall not be allowed unless accompanied by a BSP issued-certification of authority.

Basic guidelines in establishing banks are set forth in Section X102<sup>118</sup> of the Manual of Regulations for Banks (MORB) of the BSP. Applications are submitted to the Office of the Supervisory Policy Department of the Supervision and Examination Sector of the BSP for evaluation of the following: (i) capitalization requirements for each type of bank<sup>119</sup>; (ii) stockholding subscription; (iii) qualifications of incorporators/subscribers, directors and officers; and (iv) business model, corporate strategy and feasibility study for the viability of the business.

Incorporators, directors and officers are subject to the Fit and Proper Rule (Section 16 of the GBL) taking into consideration the following factors: integrity or probity, competence, education, diligence and experience/training. This is to ensure that the bank will operate in a sound and prudent manner.

In July 2014, Republic Act (RA) No. 10641 (RA 10641), otherwise known as "An Act Allowing the Full entry of Foreign Banks in the Philippines", was enacted in response to the Association of Southeast Asian Nations' (ASEAN) economic integration. RA 10641 is an amendment to the existing law liberalizing the Entry and Scope of Operations of Foreign Banks in the Philippines (RA 7721). Under RA 10641, the ownership ceiling of foreign banks in the voting stock of an existing domestic bank/new banking subsidiary was increased from 60% to 100%. Another mode of entry is by establishing a branch and sub-branches with full banking authority.

The qualifying criteria, application guidelines, capitalization and documentary requirements are set forth in Section X105 of the MORB. Since the implementation of RA No. 10641 in 2014, the BSP has approved 9 foreign bank applications, with 8 already operational.<sup>120</sup>

Upon receipt of the approval to establish a bank and as a pre-condition to the issuance of Authority to Operate, the bank will be required to, among others, submit manual of operations containing policies and operating procedures of each department/unit/office covering all risk areas of the new bank.

-

<sup>&</sup>lt;sup>117</sup> An Act Providing for the Regulation of the Organization and Operations of Banks, Quasi-banks, Trust Entities and for Other Purposes

<sup>&</sup>lt;sup>118</sup> Documentary requirements and application process are detailed in Appendix 37 of the MORB

<sup>&</sup>lt;sup>119</sup> Section X111 of the MORB

<sup>120 2016</sup> BSP Annual Report

Rule 18.B of the RIRRs of the AMLA, as amended, requires banks, as covered persons to formulate Money Laundering Prevention program. Similarly, BSP's Anti-Money Laundering regulations<sup>121</sup>, requires banks, as part of their AML/CFT risk management, to adopt a comprehensive and risk-based Money Laundering and terrorist financing prevention program (MLPP), which should be consistent with AMLA, as amended.

### **Quality of AML Supervision**

The quality of AML Supervision is high due to the existence of legal basis, regulatory framework which included the AML/CFT rules and regulations, AML examination procedures and risk rating system, the dedicated AML unit charged of on-site examination and its effective implementation of these AML infrastructures. Detailed discussion of this variable is provided in the preceding section.

## **Availability and Enforcement of Criminal Sanctions**

Legal Bases

Section 14 (Penal provisions) of the AMLA, as amended, provides the criminal sanctions for violations of the law as follows:

**Table 3-3. Criminal Penalties** 

	Criminal Violation Criminal Panalty							
	Criminal Violation	Criminal Penalty						
a.	Money laundering	Imprisonment of seven (7) to fourteen (14) years and a fine of						
	[Sections 4 (a), (b), and	not less than Three Million Philippine Pesos (PHP3,000,000.00)						
	(c)]	but not more than twice the value of the monetary instrument						
		or property involved in the offense,						
b.	Attempting and	Imprisonment of seven (7) to fourteen (14) years and a fine of						
	Conspiracy to commit	not less than Three Million Philippine Pesos (PhP3,000,000.00)						
	money laundering	but not more than twice the value of the monetary instrument						
	[Section 4 (d)]	or property involved in the offense,						
c.	Ancillary [Section (e)]	The penalty of imprisonment from four (4) to seven (7) years and						
		a fine of not less than One million five hundred thousand						
		Philippine pesos (PhP1,500,000.00) but not more than Three						
		million Philippine pesos (PhP3,000,000.00)						
d.	Facilitation the	Imprisonment from four (4) to seven (7) years and a fine of not						
	commission of money	less than One million five hundred thousand Philippine pesos						
	laundering ([Section (f)]	(PhP1,500,000.00) but not more than Three million Philippine						
		pesos (PhP3,000,000.00)						
e.	Knowingly failing to	Imprisonment from six (6) months to four (4) years or a fine of						
	submit covered and	not less than One hundred thousand Philippine pesos						
	suspicious transactions	(PhP100,000.00) but not more than Five hundred thousand						
	(Second par., Section 4)	Philippine pesos (PhP500,000.00), or both.						
f.	Failure to keep records	Imprisonment from six (6) months to one (1) year or a fine of not						
	[Section 9 9b)]	less than One hundred thousand Philippine pesos						
		(PhP100,000.00) but not more than Five hundred thousand						
		Philippine pesos (PhP500,000.00).						
g.	Malicious Reporting	Imprisonment of six (6) months to four (4) years imprisonment						
	[Section 14(c)]	and a fine of not less than One hundred thousand Philippine						
	. ,,	pesos (PhP100,000.00) but not more than Five hundred						
		, , , , , , , , , , , , , , , , , , , ,						

<sup>&</sup>lt;sup>121</sup> Part Eight of the Manual of Regulations for Banks (Circular No. 706 as amended by Circular No. 950)

		thousand Philippine pesos (PhP500,000.00), at the discretion of					
		the court					
h.	Breach of Confidentiality	Imprisonment of three (3) to eight (8) years and a fine of not less					
	[Section 9(c)]	than Five hundred thousand Philippine pesos (PhP500,000.00)					
		but not more than One million Philippine pesos					
		(PhP1,000,000.00).					
i.	Knowingly participating in	Imprisonment ranging from four (4) to seven (7) years and a fine					
	money laundering	corresponding to not more than two hundred percent (200%) of					
	[Section 14(e)]	the value of the monetary instrument or property laundered					

In 2016, complaints against seven (7) senior bank officers of a universal bank involved in the alleged cyber heist on the accounts of a central bank were filed before DOJ for facilitating the commission of money laundering.

Also, in the last quarter of 2016, another money laundering complaint was filed against six senior officers of a bank for facilitating the commission of money laundering under Section 4(f) of the AMLA, as amended. These officers committed customer due diligence lapses in relation to the four (4) fictitious accounts involved in the Bangladesh Bank case. These lapses constitute omissions, which facilitated the commission of money laundering.

Pursuant to Section 14 (f) of the AMLA, as amended, the imposition of the administrative sanctions shall be without prejudice to the filing of criminal charges against the persons responsible for the violation.

Furthermore, criminal sanctions can also be imposed against juridical entities. Section 14 of the AMLA, provides that "(i)f the offender is a corporation, association, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed by their gross negligence, the commission of the crime. If the offender is a juridical person, the court may suspend or revoke its license. If the offender is an alien, he shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties herein prescribed. If the offender is a public official or employee, he shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be".

Quality of AML Policies and Procedures (Medium High)	Comprehensiveness of AML Legal Framework	Close to Excellent
	Commitment and Leadership of Managements (Intermediate Variable)	Medium High
	Effectiveness of Compliance Function (Organization)	Medium

## **Comprehensiveness of AML Legal Framework**

The Philippines, with its aim of sustaining economic development and poverty alleviation through corporate governance and public office transparency, recognizes its vital role to contribute in the global fight against money laundering and terrorist financing. Hence, the compelling need to enact responsive anti-money laundering legislation in order to establish and strengthen the AML/CFT regime in the country, which will not only boost investor's confidence but also ensure that the Philippines is not used as a site to launder proceeds of unlawful activities.

### AML/CFT Policies and guidance for banks and other FIs supervised by the BSP

In order to effectively implement the AMLA, as amended, and its RIRRS, the BSP, as the primary supervisor and regulator of banks and other BSP-supervised covered persons (CPs), issued various policies and guidelines in the form of circulars, memoranda and circular letters.

In particular, BSP Circular No. 706 dated 5 January 2011<sup>122</sup> contains the updated and consolidated AML/CFT guidelines and requirements, as well as corresponding sanctions and penalties for noncompliance therewith. It established expectations on significant AML/CFT risk areas, to wit:

- risk management system, encompassing board and senior management oversight, compliance function, money laundering and terrorist financing prevention program (MLPP), monitoring and reporting tools and internal audit;
- risk-based and tiered customer acceptance policy, due diligence standards, minimum validation procedures, face to face contact, and general guidelines for politically exposed persons (PEPs);
- c. guidelines on certain specialty risk areas such as private banking, correspondent banking, fund/wire transfer, buyers of cashier's, manager's or certified checks, shell companies, numbered accounts, foreign exchange dealers/money changers and remittance agents; (d) reporting requirements and ongoing monitoring system;
- d. record-keeping; and
- e. AML training program.

The above requirements were essentially aligned with international standards and emphasized proportionality and promotion of financial inclusion. The regulations apply to all CPs supervised or regulated by the BSP, including money service businesses (MSBs) such as foreign exchange dealers, money changers and remittance companies/agents. These MSBs are required to register with the BSP prior to operations, pursuant to existing laws and regulations. The UARR also includes provisions on the applicable penalties to erring banks to ensure AML compliance.

In addition, the BSP issued various AML/CFT circular letters and memoranda as guidance to all supervised CPs, as follows:

2014 2015 2016 **Issuance** Circular Letter 6 4 5 Memoranda 2 3 1 Circular 0 0 0

Table 3-4. Number of BSP Issuances on AML/CFT

Overall, the AML/CFT framework for the banking sector is generally compliant with the relevant Financial Action Task Force (FATF) Recommendations. To be fully compliant with the FATF Recommendations on correspondent banking, the BSP will issue rules to specify the responsibilities of intermediary institutions.

<sup>&</sup>lt;sup>122</sup> Incorporated as Part 8 of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI). BSP Circular No. 706, Series of 2011 was amended by BSP Circular No. 950 dated 15 March 2017.

Also, in the 2010 Financial System Assessment Update (FSAP), it was noted that Philippine authorities have taken significant steps to address the concerns highlighted in the previous assessment. Corrective actions were made to align regulations with relevant Basel Principles and other international standards.

Anchored on the mentioned AML/CFT laws, the cited policies and regulatory framework for banks/FIs, the BSP significantly covered material and relevant AML/CFT risk areas, including those identified by international standard setting bodies.

On 15 March 2017, the BSP, in its Circular No. 950, amended Circular No. 706. The amendments aim to align existing regulations with the 2016 RIRRs of the AMLA, as amended<sup>123</sup>, incorporate lessons learned from money laundering incidents involving banks and adopt more risk-based principles consistent with the international standards and best practice, to emphasize proportionality in application of AML procedures and foster financial inclusion, and allow use of technology in the conduct of due diligence subject to appropriate controls to manage risks.

#### **Commitment and Leadership of Managements**

Commitment to leadership as discussed in previous section is rated very high due to the existence the required institutional and regulatory framework on entry controls and AML Supervision. On the other hand, the variable availability and enforcement of criminal sanctions is rated medium high. While proportionate and dissuasive criminal sanctions are in place, enforcement is low considering the number of money laundering cases involving the banking sector.

### **Effectiveness of Compliance Function (Organization)**

#### Assessment Criteria

The banking sector possesses effective internal AML compliance functions if most banks:

- Have internal compliance programs that are commensurate to the level of risk, taking into
  account factors such as the volume and nature of the products provided, the client base
  profiles, the transaction patterns, and the cross-border nature of transactions;
- Have appointed a sufficiently resourced and independent AML compliance officer at a senior management level;
- Have effectively managed the implementation their respective money laundering and terrorist financing prevention program (MLPP); and
- Take disciplinary actions against their staff in cases of breaches of compliance policy.

#### Adequate Regulatory Framework for AML compliance

The BSP issued guidelines for an AML compliance function that supports a high level of compliance within the banking sector.<sup>124</sup>

Under Subsection X805.1/4805Q.1 of Part Eight of the MORB/MORBNFI, management of the implementation of the covered person's MLPP shall be a primary task of the compliance office. To ensure the independence of the office, the compliance office shall have a direct reporting line to the board of directors or any board-level or approved committee on all matters related to AML and terrorist financing compliance and their risk management. It shall be principally responsible for the

-

<sup>&</sup>lt;sup>123</sup> Recent amendment was RA 10365

<sup>124 §</sup> X805.1.a of Circular No.. 950

following functions, among other functions that may be delegated by the senior management and the board, to wit:

- a. Ensure compliance by all responsible officers and employees with the regulations, the AMLA, as amended, the RIRR and its own MLPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including ongoing monitoring of performance by staff and officers involved in ML/TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It shall also report compliance findings to the board or any board-level committee;
- b. Ensure that infractions, discovered either by internally initiated audits or by special or regular examination conducted by the BSP, are immediately corrected;
- Inform all responsible officers and employees of all resolutions, circulars and other issuances by the BSP and the AMLC in relation to matters aimed at preventing money laundering and terrorist financing;
- d. Alert senior management, the board of directors, or the board-level or approved committee if it believes that the institution is failing to sensibly address anti-money laundering and terrorist financing issues; and
- e. Organize the timing and content of AML training of officers and employees including regular refresher trainings.

Moreover, existing regulation mandates that in case a covered person has branches, subsidiaries and offices located within and/or outside the Philippines, the group wide compliance officer or in its absence, the compliance officer of the parent entity, shall oversee the AML/CFT compliance of the entire group with reasonable authority over the compliance officers of said branches, subsidiaries or offices.

### Assessment of AML Compliance of banks

A review of the effectiveness of the compliance functions of banks showed that there are areas of improvements, such as implementation of appropriate customer due diligence measures and risk profiling, covered transaction reporting, on-going monitoring and suspicious transaction reporting and training and AML/CFT awareness of officers and staff.

The effectiveness of the compliance function faces a number of challenges which include human resources, AML monitoring system, AML/CFT capacity building and awareness. The deficiency in AML/CFT capacity building and awareness has cascading effect in the conduct of customer due diligence, risk profiling, transaction monitoring and suspicious transaction reporting. In addition, lack of human resources and deficiency in information technology are crucial in the management of the AML/CFT risks.

It is worthy to note, however, the banks' management acknowledge such challenges faced by the compliance function and have committed to address the issues identified during examinations conducted by the BSP. Furthermore, recent money laundering cases have served to improve the awareness of compliance function in ensuring that AML/CFT policies and procedures are effectively implanted across the various branches and units of the banks.

Compliance Level of Staff (Medium)	Availability and Enforcement of Criminal Sanctions	Medium High
	Effectiveness of Compliance Function (Organization)	Medium
	AML Knowledge of Business Staff	Medium
	Integrity of Business Staff	Medium

### **Availability and Enforcement of Criminal Sanctions**

As discussed in previous section, proportionate and dissuasive criminal sanctions are in place, however, enforcement of the criminal sanction is low considering the number of money laundering cases involving the banking sector.

### **Effectiveness of Compliance Function (Organization)**

As discussed in the preceding section, the effectiveness of the compliance function is hampered to issues noted in the implementation of AML/CFT policies and procedures. It is, however, rated as medium, due to the strong commitment of banks' management of address the issues identified.

#### AML Knowledge of Business Staff

The following were considered in the assessment of this variable:

- Legal and regulatory requirement for AML training
- The training of personnel with AML responsibilities;
- Independent assessment of AML training and implementation (primarily of customer acceptance and identification process) using ARRS based on the results of examination.

### Legal and Prudential requirement for AML training

The RIRRs of the AMLA, as amended, requires all covered persons, which include banks, to adopt and implement training programs on ML/TF prevention. Pursuant thereto, Sec. X809 of BSP Circular 950 (Amendments to Part Eight of the MORB/MORNBFI) requires covered persons to formulate an annual AML training program aimed at providing all their responsible officers and personnel with efficient, adequate and continuous education program to enable them to fully and consistently comply with all their obligations under the regulations, the AMLA, as amended, and its RIRR.

The training program also includes refresher trainings. The focus of the training includes customer acceptance and identification process, record keeping, covered and suspicious transaction reporting and internal control processes. There are also trainings designed for new hires and refresher courses for personnel, relevant and appropriate to their respective AML functions.

## Assessment of the Effectiveness of the AML Training

There was a notable increase in the number of AML training hours and participants reported by banks. From 2011 to 2016, AML training hours of banks more than doubled while the number of employees who attended AML trainings increased by more than 50 percent. This data showed strong commitment of banks to improve the AML knowledge of their officers and employees.

This, notwithstanding, it was observed that some of the trainings conducted have not resulted into an effective implementation of AML policies and procedures. Otherwise stated, there is still lack of AML/CFT awareness of banks' officers and staff. Examinations conducted in 2016 and 2015 revealed that deficiency on AML of training and awareness to effectively implement lessons learned in trainings/seminars resulted in deficiencies in customer due diligence and risk profiling, on-going monitoring and suspicious transaction reporting.

Continuous AML training and Other Forms of Feedback mechanism

The BSP and AMLC conducts AML/CFT training for members of industry associations such as the Rural Bankers Association of the Philippines, Association of Bank Compliance Officers of the Philippines (ABCOMP), Bankers' Institute of the Philippines (BAIPHIL), and Chamber of Thrift Bank (CTB).

Aside from trainings, the BSP and the AMLC also issue reminders or clarifications through memoranda or Frequently Asked Questions (FAQs) on salient AML regulations, all of which are accessible in their respective websites.

### **Integrity of Business Staff**

In assessing staff integrity, the following factors were considered:

- a. Effectiveness of staff vetting programs or Know Your Employee policy;
- b. Incidence of disciplinary and administrative actions against employees, as a result of integrity issues;
- c. Criminal/Loss incidences involving employees; and
- d. Effective implementation of AML policies and procedures.

Fit and Proper Rule and Other Measures

The BSP issued regulations to implement the "Fit and Proper Rule" under Section 16 of RA No. 8791 or The General Banking Law of 2000 which provides, as follows:

"To maintain the quality of bank management and afford better protection to depositors and the public in general, the Monetary Board shall prescribe, pass upon and review the qualifications and disqualifications of individuals elected or appointed bank directors or officers and disqualify those found unfit.

After due notice to the board of directors of the bank, the Monetary Board may disqualify, suspend or remove any bank director or officer who commits or omits an act which render him unfit for the position.

In determining whether an individual is fit and proper to hold the position of a director or officer of a bank, regard shall be given to his integrity, experience, education, training, and competence."

For this purpose, the BSP maintains a watch-list of persons disqualified to be a director or officer of its supervised entities. This provides BSP with a central information file to be used as reference in reviewing and passing upon the qualifications of persons elected or appointed as directors or officers of supervised entities. Banks may request information from the said watch-list for the sole purpose of screening their nominees/applicants for directors/officers and/or confirming their elected directors and appointed officers, subject to written consent of the director/officer concerned.

Further, covered persons including banks, are required to incorporate in their MLPP an adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed to assume sensitive banking functions. Philippine banks also conduct periodic lifestyle check of employees as integrated in their KYE process to establish their honesty, integrity and ethical behavior.

Some banks have adopted a whistle blower policy to encourage its employees to report irregular activities involving bank personnel without fear of reprisal. They also have Codes of Conduct/Discipline to instill employees' sense of responsibility and commitment to the virtues of honesty, industry and integrity and establish measures and standards to institute discipline.

Internal control measures are also being adopted such as check and balance approach to assignment of duties and responsibilities, the use of Key Result Areas, Key Performance Indicators and employee performance appraisal to drive appropriate personnel behavior and instill compliance culture. Significant amount of training focusing on ethics and governance are likewise provided to employees, while appropriate disciplinary actions are taken on personnel, when warranted.

Assessment of integrity of banks' officers and staff

Based on data of crimes and losses received by the BSP from 2012-2016 as follows, only 2,186 of 34,399 (or 6.35%) incidents involved bank personnel:

	2016 (January-June)			2015 2014		2014	2013		2012	
					T	otal No. of				
	Incidents	Incidents Involving Bank Personnel	Incidents	Incidents Involving Bank Personnel	Incidents	Incidents Involving Bank Personnel	Incidents	Incidents Involving Bank Personnel	Incidents	Incidents Involving Bank Personnel
Credit Card-RELATED	2,642.00	2.00	5,330.00	9.00	4,211.00	9.00	4,294.00	4.00	4,645.00	6.00
ESTAFA	73.00	43.00	35.00	7.00	37.00	16.00	46.00	10.00	62.00	14.00
FALSIFICATION	607.00	52.00	613.00	65.00	641.00	87.00	530.00	69.00	651.00	70.00
NEGLIGENCE	126.00	83.00	223.00	173.00	244.00	180.00	247.00	191.00	207.00	157.00
ROBBERY	24.00	1.00	14.00		7.00	1.00	22.00	-	15.00	-
THEFT	1,613.00	159.00	2,648.00	157.00	1,917.00	164.00	1,189.00	165.00	323.00	149.00
OTHERS	190.00	26.00	348.00	28.00	211.00	33.00	229.00	25.00	185.00	31.00
Total	5,275.00	366.00	9,211.00	439.00	7,268.00	490.00	6,557.00	464.00	6,088.00	427.00

Also, the total number of personnel involved in the cited incidents, from 2012 to 2015 were 916, 968, 871 and 756, respectively, representing only a minimal percentage (0.48%, 2015 data) of the total workforce of the banking sector, estimated at 150,714 as at end of June 2015.

For January to June 2016 data, statistics remain at 7% of total reported incidents which involve bank personnel, broken down as follows:

Table 3-5. No. of Incidents

Offense	No. of Incidents	No. of Incidents Involving Bank Personnel
Credit Card-related	2,642	2
Estafa	73	43
Falsification	607	52
Negligence	126	83
Robbery	24	1
Theft	1,613	159
Others	190	26
Total	5,275	366

The amounts involved in the above crimes are PhP.362906 Billion and USD.000184 Billion. On the other hand, the amount involved concerning crimes perpetrated by outsiders amounted to PhP3.910460 Billion, and USD.001590 Billion and EUR.000020 Billion.

While the number of bank personnel involved in crimes as shown above and the amounts involved are low compared to the total assets of the banking sector, the effect on the reputational risks on the banks involved and the integrity of the financial system, in general, is invaluable.

It is also that while bank personnel have already attended AML trainings, there are still deficiencies in the gathering of the required minimum information and the acceptance of clients, conduct of customer of customer due diligence, risk profiling, on-going monitoring and submission of suspicious transaction monitoring. These findings impact the integrity of banks' officers and staff.

Quality of CDD	Availability and Access to Beneficial Ownership information	Medium High
Quality of CDD Framework	Availability of Reliable Identification Infrastructure	Medium High
(Medium High)	Availability of Independent Information Sources	High

### **Availability and Access to Beneficial Ownership information**

Legal entities and legal arrangements such as trusts, cooperatives, foundations, partnerships and such other types of companies are avenues for criminals in masking their true identity as beneficial owners of accounts, posing high ML and TF risk to banks and other covered persons.

Identification of the beneficial owner can be a long process given the absence of a central database system, containing information on the structure, management, control and beneficial ownership of entities, that is readily accessible in a timely fashion to facilitate customer due diligence process. Currently, the existing sources of beneficial information are the customer's declaration and the General Information Sheet (GIS) filed with the Securities and Exchange Commission. The GIS contains information on stockholders (owning 20%), directors and officers, among others, and is accessible for a minimal fee. However, to obtain the ultimate beneficial owner of a customer which is part of a conglomerate, or has layered ownership structure, the verification process can be tedious as the bank has to follow the GIS of each of the corporate owners. Information on publicly-listed companies are readily available at the Philippine Stock Exchange website. For cooperatives, the information can be gathered from the Cooperative Development Authority while for sole proprietors, the information can be obtained from the Department of Trade and Industry.

Despite the challenges in the identification of beneficial ownership, financial institutions, particularly complex banks, have adopted and implemented policies, procedures and controls in ensuring that the required information on both the legal and beneficial owners are obtained prior to account opening. Banks are required to obtain the latest GIS of corporations. For accounts opened thru a trustee, nominee, agent or intermediary, the true and full identity and existence of both the legal owner (trustee, nominee, agent or intermediary) and beneficial owner (trustor, principal, beneficial owner or person on whose behalf the account/relationship transaction is being opened/established/conducted<sup>125</sup> are required to be obtained/gathered by covered persons.

<sup>125</sup> Circular 950 page 23 series of 2017

For individual accounts (i.e., Personal Managed Trust [PMT], Investment Management Account [IMA]), it is provided in the contract that the customer shall provide all the minimum required information of the nominated beneficiary as well as the supporting documents such as birth certificate, valid and acceptable ID. Upon opening of trust, the purpose is already indicated (in the case of PMT) and no deviations of the purpose will be allowed without the approval of both parties (trustee/beneficiary and trustor). For withdrawal of funds (in case of PMT), proceeds are processed in accordance with the dispositive provisions of the contract/agreement i.e. proceeds are made payable to the school (if purpose for education) or name of the hospital (for health purposes).

## Availability of Reliable Identification Infrastructure

Banks are required to develop clear, written and graduated customer acceptance and identification policies and procedures that will prevent suspicious individuals or entities from opening an account or establishing a relationship while at the same time ensure that the financially or socially disadvantaged members of the society are not denied access to financial services. This is done, among others, by obtaining the prescribed minimum information about the customer, which shall be validated from official documents, such as government issued identification documents (IDs). For corporate and juridical entities, banks are required to verify their legal existence, organizational structure and the authority and identification of persons purporting to act on its behalf. Part of customer due diligence (CDD) is validation of the accuracy and completeness of information and IDs obtained from clients. IDs are validated through verification with government agencies, including access via mobile phones, internet or sending of "Thank You" letters, among others. These procedures aim to establish the identity and existence of the customer and assess the risk profile. Depending on the risk profile, banks are required to conduct the appropriate standard of due diligence.

Despite the absence of a national ID system, the results of examination for the past years showed improving efforts of banks to enhance their customer onboarding process, such as system and manual controls, to obtain required information and validate the same from reliable sources, particularly the government agencies which issued the identification documents. While there is no national ID system yet, efforts were made to institute a reliable identification system albeit being limited to certain sectors. In 2010, the government released the Unified Multi-Purpose ID (UMID), which covers members of the Government Service Insurance System (for those employed in the government), Social Security System (for those employed in the public sector), the Philippine Health Insurance Corporation and the Home Development Mutual Fund (for both government and private sector employees). This is a reliable ID, which contains information on the members' name, date of birth, sex and address.

Further to the UMID, several government agencies have facilities that will allow instant verification of issued identification, to wit:

**Table 3-6. Identification Verification System** 

<b>Government Agency</b>	Features	Verification Tool	
Philippine Postal Corp	- Quick Response (QR) code	QR code scanning via Mobile	
(PhIPost)	- Security Hologram	App	
	- Ultraviolet (UV) Ink		
	- Ghost Image of cardholder's photo		
Integrated Bar of the	- QR code	QR Code scanning via Mobile	
Philippines (IBP)		Арр	
Land Transportation	- Security Hologram	SMS verification against LTC	
Office (LTO)	- Ghost Image of the cardholder's photo	database – validity of number	
		and date of expiration	

Moreover, the government is set to launch the new identification card for OFWs (OFW ID). The OFW ID is intended to be used by OFWs as a universal ID for government transactions. The DOLE OFW central database is linked to other government databases (i.e., NBI clearance, SSS, COMELEC, Bureau of Immigration, LTO driver's license), and authenticity can be verified through an embedded Quick Response (QR) Code.

### **Availability of Independent Information Sources**

#### Assessment Criteria

Independent and reliable information sources are available, if sources of comprehensive and reliable historical financial information and other information about clients are available and can easily be accessed by AML-regulated institutions.

Existing regulatory framework requires risk-based conduct of customer due diligence

Existing regulation mandates banks to verify and confirm minimum information obtained from its clients as part of its customer acceptance and identification process. Higher level validation is required under existing regulation for clients that posed higher risks which include the following:

#### For individual customers:

- a. Confirming the date of birth from a duly authenticated official document;
- b. Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters, or other documents showing address or through on-site visitation;
- c. Contacting the customer by phone or email;
- d. Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means; or
- e. Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include, but are not limited to, the following:

- a. Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
- b. Inquiring from the supervising authority the status of the entity;
- c. Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
- d. Contacting the entity by phone or email.

In addition, banks are required to, among others: (a) establish a client's identity and beneficial owner, (b) screen clients against watch/sanction list and (c) monitor and analyze the client's transactional pattern/behavior without due prejudice to the reporting of a Suspicious Transaction Report (STR) to the AMLC when circumstances warrant. This requires the banks to keep a historical information and data on clients.

Over the years, banks have incorporated in their operating guidelines certain process to validate customer information and transactions. These include the following:

- a. Validate the authenticity of the information provided by the client by comparing it with the valid identification or official document provided. They are also using other independent source documents, data or information such as utility bills, employer's certification and proof of business to verify the clients' addresses and sources of income.
- b. Send by registered mail 'Thank You Letters' to the address/es of their clients to confirm the existence of the clients' address.
- c. When necessary, undertake on-site visitation to verify the identity of their client or source of funds, for example, business.
- d. Verify the validity and authenticity of client's licenses using various online facilities of relevant government agencies, such as the SEC I-view by Securities and Exchange Commission (SEC) for corporate clients, Cooperative Development Authority (CDA) website for cooperatives, Bangko Sentral ng Pilipinas (BSP) website for money service providers and Department of Trade and Industry (DTI) website for business name registration. SEC I-view also provides data on the financial capacity of the client based on the submitted financial statements including the beneficial owner of the corporate clients through their General Information Sheet.

In addition, banks are also required to conduct screening of its prospective and existing clients against watch/sanction list as well as PEP list. Some banks have invested significant capital to enhance their transaction monitoring and screening process, as well as investigation of alerts. Some banks dedicate manpower to independently review the financial profile of the customer and assess the validity or legality of transactions. Most commercial/universal banks subscribe to third party providers to enhance their verification/investigation process and adequately screen its clients. These providers provide comprehensive database regarding an individual or corporation and are accessible in a single source. It contains information such as sanctions, watch, regulatory and law enforcement lists, politically exposed person (PEP), and adverse news/media.

Banks also rely on other independent information available like historical information of clients' transactions as well as those shared by the credit bureaus and media reports. Banks maintain their respective internal watch list databases that include clients who were subject of STRs and reports on crimes and losses, clients that have been involved in fraud or presented fictitious identification documents. These databases aim to identify, at the onset any suspicious/unscrupulous individuals or corporations and is a tool for ongoing transaction and customer monitoring.

Moreover, banks are also using information shared by credit bureaus like the Bankers Association of the Philippines (BAP) Credit Bureau and the Credit Information Corporation (CIC) as a means to verify the client's financial information and history. The CIC, a government-owned and -controlled corporation that was established in 2009 is a central credit registry which collects positive and negative credit data on borrowers and provides consolidated basic credit information to individuals, businesses, financial institutions, private credit bureaus and other entities. It addresses the need for dependable information concerning the credit standing and track record of borrowers. The CIC collects credit information from various sources such as banks, financial institutions, insurance companies, financing companies, credit cooperatives, as well as utility companies and other businesses that extend loans. As of May 2017, CIC-compliant financial institutions have already given partial access to the CIC's credit information system. Currently there are 112 entities, which include local banks, insurance companies and financing companies, considered as CIC compliant. These companies have submitted all the required information (such as individual and corporation borrowers personal information, credit cards details, installment contracts as well as non-installment contracts). Both potential borrowers and lenders, including the general public, will be able to officially access the CIC's credit information system by January 2018.

The BAP Credit Bureau Inc. has several key services, which can be accessed through the Internet and processed in practically real time. This includes a loan information system (LOANDEX) used to exchange data on credit dealings. It also has a negative file information system (NFIS), which helps identify mishandled current accounts and credit cards, and adverse loan accounts (foreclosure, items in litigation, or written-off accounts). Another service is the similar names inquired previously (SNIP) system, which offers data on the number of times a similar name was inquired in NFIS for the past 60 days. The final one is the microfinance data sharing system (MIDAS), a compilation of borrowers at risk reported by microfinance institutions. All inquiries by members, including the NFIS, can be accessed through the Internet and inquiries are processed in practically real time from receipt of inquiries. Other services offered by the BAP Credit Bureau Inc. are the Real Property Database System (RPDS), an electronic compilation of fair market values of real estate held by banks and financial institutions. The Titles Caution List database (TCLD) is a web-based service that gathers and maintains information about spurious, non-existent, or otherwise questionable land titles.

	Commitment and Leadership of Managements (intermediate variable)	Medium High
Quality of	Compliance Level of Staff	Medium
Operations (Medium)	Quality of CDD Framework (intermediate variable)	Medium High
	Effectiveness of Suspicious Activity Monitoring and	Medium
	Reporting	Low

## **Commitment and Leadership of Managements**

Commitment to leadership as discussed in previous section is rated very high due to the existence of the required institutional and regulatory framework on entry controls and AML Supervision. On the other hand, the variable availability and enforcement of criminal sanctions is rated medium high as enforcement is low considering the number of money laundering cases involving the banking sector.

#### **Compliance Level of Staff**

As discussed in the preceding section, the effectiveness of the compliance function is hampered to issues noted in the implementation of AML/CFT policies and procedures. It is, however, rated as medium, due to the strong commitment of banks' management of address the issues identified.

## **Quality of CDD Framework**

The quality of CDD framework is assessed to be medium high to the availability of independent information sources such as credit bureaus and third party providers where banks can validate information and credit history of prospective clients. While access to beneficial ownership is quite cumbersome, there are measures which require corporate clients to declare their beneficial ownership. Also, despite the absence of a national identification documents, there are other alternative identification documents where the identity of clients can be verified or validated. Furthermore, there are identification documents subsequently issued by some government agencies which have security features that prevent ease of falsification and the identity of clients are verifiable either through mobile applications or request to the issuing government agency.

### **Effectiveness of Suspicious Activity Monitoring and Reporting**

Sec. 9.c of Republic Act 9160 or the Anti-Money Laundering Act of 2001, as amended, mandates that

banks and other covered persons should report to the AMLC all covered transactions and suspicious transactions within five (5) working days from occurrence thereof, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof. The reporting of covered transactions and suspicious transactions must be in accordance with the AMLC Reporting Procedures Manual dated March 2014.

AMLC Resolution No. 61, Series of 2016 further requires all banks to have their AML electronic system aligned with the requirement of the five (5)-working day reporting period. For suspicious transactions, "occurrence" refers to the date of determination of the suspicious nature of the transaction, which determination should be made not exceeding ten (10) calendar days from the date of transaction. However, if the transaction is in any way related to, or the person transacting is involved in or connected to, an unlawful activity or money laundering offense, the ten (10) —day period for determination shall be reckoned from the date the covered person knew or should have known the said suspicious transaction indicator.

Electronic copies of these CTRs and STRs are required to be preserved and safely stored for at least five (5) years from the dates the same were reported to the AMLC. Banks are also required to designate two officers who will be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA. They have the obligation to make these documents readily available without delay during BSP examinations.

The CTRs and STRs received by the AMLC from BSP-supervised financial institutions mainly come from banks (more than 90% of CTRs and STRs), as follows:

Bank	2016		201	15	2014		
Submissions	Number	Percent*	Number	Percent*	Number	Percent*	
CTRs	35,857,010	99.78	35,345,132	99.89	43,282,421	99.94	
STRs	115,694	94.16	133,420	94.76	80,286	90.98	

Table 3-7. CTRs and STRs

Out of the STRs submitted in 2015 and 2016, 42,910 and 9,940, respectively, were referred to the Compliance and Investigation Group of the AMLC for investigation.

### BSP's Regulations for Ongoing Transaction Monitoring

Universal banks (UBs) and commercial banks (KBs,) as well as BSP supervised covered persons which are considered complex, are required to adopt an electronic AML systems capable of monitoring risks associated with ML/TF, as well as generating timely reports for the use of its board of directors and senior management. The electronic transaction monitoring system should, at the minimum, detect and alert to the bank's attention, transactions and/or accounts that qualify either as CTs or STs. The system must have at least the following automated functionalities:

- a. Covered and suspicious transaction monitoring performs statistical analysis, profiling and able to detect unusual patterns of account activity;
- b. Watch list monitoring checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
- c. Investigation checks for given names throughout the history of payment stored in the system;
- d. Can generate all the CTRs of the covered institution accurately and completely with all the

<sup>\*</sup> Percentage to total submissions to AMLC of BSP-supervised financial institutions

mandatory field properly filled up;

- e. Must provide a complete audit trail;
- f. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
- g. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

Other financial institutions should ensure that their manual system has the means of flagging and monitoring the transactions mentioned above. In addition, they shall maintain a register of all STs that have been brought to the attention of senior management whether or not the same was reported to the AMLC.

Transaction Monitoring Systems and Practices – Automated and Manual Process

Based on the onsite examinations, all banks have a system of recording their transactions, either manual or electronic. However, such electronic monitoring systems needs some refinements and improvement in order to be effective in the monitoring and detection of possible suspicious transactions. Among the areas of improvements include the gathering of CDD information, required functionalities, parameters and alert generations, resolutions and disposal of alerts.

In some cases, deficiency in the gathering of raw data on CDD resulted in the ineffective monitoring of transactions. Also, it was observed in some banks that not all of the required functionalities are included in their AML monitoring systems which impacts the proper management of ML/TF risks.

The alerts parameters are either too many or too restrictive such that the system generates too many alerts which are not meaningful. Some parameters are also very limited such that possible large, complex and suspicious transaction are not captured.

While some systems generate meaningful alerts, the disposal and resolution of the same takes some time in which the essence of timely submission STR are not met. There is a mismatch of human resources dedicated to investigate and dispose these alerts vis-à-vis the number of alerts generated by the system.

# PRODUCT/SERVICE VULNERABILITY

The thirteen (13) general input variables discussed above have simultaneous impact on all banking products/services. In addition, there are five (5) major factors that were identified to have specific impact on the assessment of AML vulnerability of a particular product/service, as follows:

- a. Product volume;
- b. Average amount of transactions for products;
- c. Profile of the customer using the product;
- d. Other characteristics of products or service vulnerability (there are twelve [12] identified other factors given consideration and these are listed under item 4 below); and
- e. Existence of adequate and specific AML/CFT controls

Information on these five (5) factors was obtained from available bank reports, responses to surveys and questionnaires received from banks.

#### 1. Product Volume

This variable considers the riskiness of a particular product in relation to its volume, or the size of the transactions, or activity that flows into a particular product/service. The outstanding balance, as well as the total value of transactions for the year, is given consideration. As such, product volume is a factor in the inherent vulnerability that poses a threat to the banking sector.

### 2. Average Amount of Transactions for Products

This variable considers the average size of transactions for a particular banking product or service. When a particular product/service is customarily used to process large transactions, it makes it more attractive to money launderers since the product will enable them to launder large amounts in limited number of transactions. Assessment on this variable was based on data gathered from surveys and questionnaires accomplished by top banks, complemented by business judgment of bank officers obtained through an FGD.

### 3. Profile of Customer Using the Product

This variable considers the profile of customer as a factor in assessing the inherent ML vulnerability of a product or service offered by a bank. Knowing the type/nature of a customer who uses the product/service will give the bank an understanding of the ML risks posed by a product/service. For example, when the customer is: a foreign national/ resident; a high-net worth individual; a PEP; a resident from a tax or criminal haven jurisdictions; a high-risk individual; or known with criminal record. These types of customers will increase the possibility for the product/service to be used for ML or TF.

### 4. Other Characteristics of Product or Service Vulnerability

There are also other factors (12) present and specific to a particular product/service that increases the risk of ML or financial abuse of a particular product/service. Some of these factors are the following and corresponding riskiness of the four products is shown.

- a. Investment/Deposit Feature
- b. Cash Activity
- c. Domestic Money Transfer Feature
- d. International Money Transfer Feature
- e. Frequency of International Transfers
- f. Transactions with off-shore centers, tax havens, high risk jurisdictions
- g. Availability of anonymous or omnibus transactions
- h. Existence of ML typologies on abuse of the product
- i. Use of the product in fraud or tax evasion schemes
- j. Difficulty in tracing the records
- k. None face to face
- I. Use of agent

## 5. Existence of Adequate and Specific AML/CFT Controls for a Given Product/Service

This variable assesses whether there are adequate and appropriate AML/CFT controls to manage and mitigate any potential ML risk. When there are specific and stringent AML/CFT controls on a product/service, vulnerability to ML is reduced because of the high probability of being caught through

the submission of an STR. Thus, a money launderer would not prefer to transact with a bank that has very good AML/CFT controls in place.

### **RISKINESS OF PRODUCTS/SERVICES**

Among several banking products and services currently being offered by different banks in the Philippines, the group initially identified four banking products, perceived to be attractive for ML/TF, namely, private banking services; deposits; remittance; and trust products.

Deposit accounts provide great opportunity for ML since deposit-taking is the core business of a bank. In end-2016, total deposits of the entire banking system amounted to PhP10.5 trillion which represent 87.5% of their total liabilities of PhP12.0 trillion. Remittances were also analyzed given its contribution to the economy, steady growth and high inherent ML risk involved in facilitating fund/wire transfers. Private banking and wealth management was likewise considered given its growing size and large value or amount involved in the transaction. Lastly, trust products were analyzed given its size, continuous growth and nature of relationship involved.

An analysis<sup>126</sup> was made on the inherent ML risk of these four identified products of banks, based on certain indicators (13 as listed below), as follows:

**Table 3-8. Risk Profile of Product** 

	INDICATORS	Private Banking	Deposits	Remittance	Trust
A.	Total Value <sup>127</sup>	Low	High	Medium	High
В.	Average Transaction Size <sup>128</sup>	High	Medium	Medium Low	Medium
C.	Client Base Profile <sup>20</sup>	Very High Risk	Medium Risk	Medium Risk	Medium Risk
D.	Other Vulnerabilities:				
1.	Existence of Investment/ Deposit Feature <sup>20</sup>	Available and Prominent	Available	Available	Available and Prominent
2.	Level of Cash Activity <sup>20</sup>	Low	Medium High	Medium	Does not Exist
3.	Frequency of International Transactions <sup>20</sup>	Medium High	Medium	High	Low
4.	Anonymous or omnibus use of the product <sup>129</sup>	Not Available	Not Available	Not Available	Not Available
5.	Existence of ML typologies on abuse of the product <sup>20</sup>	Exist	Exist and Significant	Exist	Exist but Limited
6.	Use of the product in fraud or tax evasion schemes <sup>20</sup>	Exist but Limited	Exist but Limited	Exist	Exist but Limited
7.	Difficulty in tracing the transaction record of the product <sup>21</sup>	Easy to Trace	Easy to Trace	Easy to Trace	Easy to Trace
8.	Non-face to face use of the product <sup>21</sup>	Not Available	Not Available	Not Available	Not Available
9.	Availability of the product for electronic banking <sup>21</sup>	Low	Medium High	Medium	Medium

<sup>&</sup>lt;sup>126</sup> (results based on quantitative information gathered from banks, survey questionnaires and FGD).

<sup>128</sup> Assessment based on consolidated replies of banks on the data template, survey questionnaire and FGD.

<sup>&</sup>lt;sup>127</sup> www.bsp.gov.ph and consolidated replies of banks on the data template.

<sup>&</sup>lt;sup>129</sup> Assessment based on consolidated replies of banks on the data template, survey questionnaire and FGD and considering existing AML laws, rules and regulations.

E. AML/CFT Specific	Exist and	Exist and	Exist and	Exist and	l
Controls <sup>21</sup>	Comprehensive	Comprehensive	Comprehensive	Comprehensive	

Results using the assessment tool provided by World Bank, considering the above factors, are summarized below:

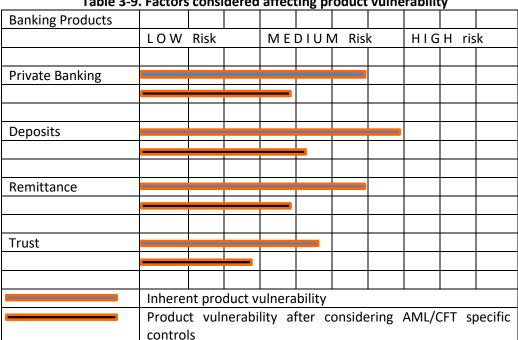


Table 3-9. Factors considered affecting product vulnerability

As shown in the table, deposits have high vulnerability for ML at 0.74, followed by remittances (0.65) and then private banking (0.64) and trust (0.50), all with medium risk. After considering AML/CFT controls in place, product vulnerabilities have considerably gone down, but deposits and remittances remain as the riskiest, at 0.48 and 0.43, respectively, although both have medium ML risk.

### A. Private Banking (Residual Risk - Medium)

Private banking products/services are offered only by few domestic commercial banks and some foreign banks operating in the Philippines to select or target clients, usually for high net-worth individuals whose investments/transactions are placed at PhP5.0 Million at the minimum but may even be higher depending upon bank's policies. Included in this category are those banks offering wealth management services, which are also offered to high net-worth individuals.

Considering the financial profile of clients, this product involves highly personalized service handled by designated relationship or account officers. With the inherent high value of transactions per client, private banking/wealth management is an attractive channel to money launderers since large volume of cross-border transactions may be done. Inherent risk is mitigated by appropriate AML controls, starting from application of enhanced due diligence for customer acceptance to strict monitoring of transactions to ensure that transactions are valid and with underlying legal or trade obligation. Banks do not allow customers to maintain anonymous accounts or engage in omnibus transactions, thus, identity and financial capacity of private/wealth banking clients are properly established at the onset. In addition, private banking/wealth management unit within the bank is subject to periodic audits by the bank's internal audit unit and covered by BSP examination.

Customer profile of private banking clients are mostly normal to high risk. These customers are generally known to the bank, and proven to be individuals or corporate entities with high income or established sources of funds. Overall, while inherent risk is high, it is adequately mitigated given adequate controls in place, thus, overall product vulnerability or residual risk is medium.

### B. Deposits (Residual Risk - Medium)

Deposit products, comprising of savings, time and demand deposits, reached PhP10.5 trillion in 2016 and represent 75.5% of the total banking system's assets of PhP13.9 trillion. Said level was 13.8% higher than end-2015 level, which is a significant growth. Bulk of deposits is in the form of savings deposits, which are mostly individual accounts in local currency. Moreover, 79% of depositors maintain deposits that are less than PhP5,000 in balance. Thus, the retail orientation of deposit liabilities reduces the product's vulnerability to ML. On the other hand, depositors with a balance of PhP2 Million and above represent 1% of the total number depositors, but their aggregate deposits represent 74% of the amount of total deposits, and these type of depositors pose high ML risk for banks. Top universal banks surveyed disclosed that bulk of their outstanding deposits are from corporate clients (50%), followed by individual clients (36%) and the rest are from micro-depositors (14%, which are low income clients). A total of 98.8% of depositors are residents.

Statistics on deposit liabilities show that ML vulnerability of deposit products is mainly attributed to few depositors who maintain significant level of deposits and activities. Moreover, in terms of the average transaction size of deposits, survey on banks disclosed that risk is medium to high. Deposit products are vulnerable to ML and financial abuse since depositors may use it as a medium to facilitate domestic and cross-border funds/wire transfer. It is also noted that technological advances are among the reasons for the increasing vulnerability of the product, enabling depositors to engage in internet/electronic banking, make withdrawals through ATMs and facilitate instant fund/wire transfers. These various features of deposit products make it more vulnerable to ML/TF risk, as compared to other products.

Given that existing and appropriate AML/CFT controls are in place, inherent ML/TF risk on deposit products is mitigated. Thus, the residual risk on deposits is medium.

## C. Remittance (Residual Risk - Medium)

The Philippines ranked third among the top recipients of migrant remittances inflow from abroad, after India and China, with total remittances amounting to USD24.3 Billion<sup>130</sup>, representing 8.5% of the Philippine GDP (USD284.8 Billion) in 2014. At the end of 2016, total remittances further increased to USD26.9 Billion<sup>131</sup>. As such, the BSP recognizes the importance of global OFW remittances in the country's economy. Thus, the BSP embarked on various initiatives to improve remittance services and environment provided to OFWs by enhancing transparency, promoting healthy competition, improving access to financial services and promoting financial learning to beneficiaries, among others.

Among the four products/services identified, remittance is the second in terms of inherent and residual risk. The inherent high risk of the product can be attributed to its use for outward, inward, foreign and domestic remittances, accessibility to all types of customers, and utilization for different purposes. As far as total value of the transaction, amount of remittances is known to be of medium risk when the purpose is for business or trade. Remittances have been known to facilitate import and export transactions, and this is coursed through international wire transfers. On the other hand, most inflows are for non-trade or personal purposes. These are usually inward remittances coming from

<sup>&</sup>lt;sup>130</sup> Source: BSP - Selected Philippine Economic Indicator - 2014.

<sup>&</sup>lt;sup>131</sup> Source: BSP - Selected Philippine Economic Indicator - 2016.

OFWs to their beneficiaries/relatives in the Philippines, which are not considered high risk considering that these are from the salaries of the OFs. For remittances coming from high-risk jurisdictions, transactions are generally subject to enhanced due diligence and more stringent review. In addition, remittance transactions are generally cash intensive and banks have the ability to process large volume and number of transactions in a very short period of time, over that of stand-alone money transfer operators.

Thus, for remittances, volume and nature of the transaction covering fund transfers are the main factors that have significant impact on product vulnerability. On the other hand, average size of transaction is medium and customer profile are also medium risk, while other risk indicators/vulnerabilities are at medium-risk, since there are several factors affecting remittances. Remittances, though, can be abused for fraud or tax evasion schemes where funds may be transferred to tax haven countries. However, inherent ML risk is mitigated due to existence of general and specific AML/CFT controls, which are appropriately in place, particularly for customer acceptance and identification and ongoing monitoring of transactions. Thus, overall ML risk for remittances is medium.

### D. Trust (Residual risk - Medium)

Trust and fiduciary business of a bank is separate from regular banking operations in view of separate licensing requirements prescribed by the BSP. In terms of product risks for various trust products, Investment Management Account "IMA" poses the highest risk because Trustee banks are appointed as "Agent" of the "Client-Principal" where the latter directs the former on where the funds will be invested in or what type of assets will be purchased by the Agent for and in behalf of the Principal in accordance with the investment guidelines signed by the Client-Principal. With regard to Total Value (Asset under Management (AUM)), the risk is high considering the total consolidated AUM level of PhP2.3 Trillion of the trust industry at end-2016.

With regard to average transaction size, the risk is medium because a significant portion of the total transaction represents trust retail products with minimum placement ranging from PhP25.0 thousand to PhP500.0 thousand for Unit Investment Trust Funds. Moreover, most trust transactions are carried-out for investment purposes.

Other vulnerabilities for trust products may include its use for domestic and international fund/wire transfers, likewise making it highly vulnerable for financial abuse or fraud activities. However, risk is mitigated due to existence of general and specific AML/CFT controls which is very high and comprehensive. As additional control, recently, most trust entities of banks have required all their trust clients to open deposit account with them for purposes of settling their transactions, to facilitate movement of funds through debit or credit to their deposit accounts. As a result, level of cash activity has gown down, or mostly none at all. This also provides another layer of review and due diligence on the customer.

Therefore, for trust products and services, inherent risk is medium. After considering AML/CFT controls, residual risk is **MEDIUM**.

#### **ACTION PLAN**

Based on the identified weaknesses and deficiencies in the priority variables of the sector, the following are the recommended action points:

ACTION PLAN	PRIMARY	SECONDARY	TIMELINE
	AGENCY	AGENCY	
AML Knowledge of Banks' Staff			
The AMLC and the BSP shall provide a comprehensive	AMLC,		Ongoing
train-the-trainors workshop/program to banks.	BSP,		
	Banks		
Banks to review and conduct training needs analysis to			
determine topics to be included in the training			
modules.			
Banks to continuously review effectiveness of trainings			
conducted and the contents and mode of delivery of			
the trainings.			
Effectiveness of Complia	nce System		
Banks shall ensure to implement previous MB	BSP,		Q4 2017
directives.	Banks		
Banks' management shall address the human resource			
challenges of compliance units.			
Banks shall ensure effective implementation of their			
respective MLPP across business units with particular			
focus on AML/CFT measures on customer due diligence			
including on-going monitoring, submission of CTRs and			
CTRs, and record keeping.			
Banks' compliance units shall proactively conduct			
compliance testing across various units.			
Banks shall regularly conduct internal audit validations.			
Banks shall ensure that violations are immediately			
rectified and bank employees who commit MLPP			
violations are subjected to proportionate and			
dissuasive sanctions.			
Effectiveness of Suspicious Activity Monitoring and Rep	oorting		
Banks shall implement BSP's directive to improve			
l · · · · · · · · · · · · · · · · · · ·			
electronic monitoring system and immediately address			
issues noted during the past examinations.			
BSP shall continue assessment on banks' compliance			
with previous directives and findings.			
Other complex banks (other than UBs and KBs) shall			
adopt their respective electronic monitoring system			
and ensure that it is compliant and effective.			
Availability and Enforcement of Administrative Sanction	ns		
BSP shall monitor actions taken on its referred AML	AMLC,		
ROEs to the AMLC for appropriate action.	BSP		
AMLC shall act expeditiously on the referrals made by			
the BSP and impose administrative sanctions when			
warranted.			

#### IV. SECURITIES SECTOR VULNERABILITY

#### **EXECUTIVE SUMMARY**

The report updated the information used to assess the vulnerability of the securities sector to ML/TF and tried to understand what has been done in the regulatory framework. A review of the regulatory requirements, laws, rules, and guidelines and the changes in the securities structure, if any was performed. The information considered in the assessment of the effectiveness of the AML/CFT framework include the comprehensiveness of the legal framework, effectiveness of supervision procedures and practices, availability and enforcement of administrative sanctions, availability and enforcement of criminal sanctions, availability and effectiveness of entry controls, integrity of staff in securities firms, AML knowledge of staff in securities firm, effectiveness of compliance functions, effectiveness of suspicious activity monitoring and reporting, level of market pressure to meet AML standards, availability and access to beneficial ownership, availability of a reliable identification infrastructure and availability of independent information sources. The findings were taken from the reports/survey submitted and the CTRs and STRs that were submitted by covered persons to AMLC.

After assessment of the relevant variables, the overall vulnerability of the Securities sector is **MEDIUM.** 

#### **INTRODUCTION**

The Securities and Exchange Commission (SEC) has continuously taken initiatives through amendments of its rules and regulations in order to improve and strengthen the capital market and be aligned with global and regional standards, best practices and International Organization of Securities Commission (IOSCO) principles.

The securities sector has always been subjected to extensive regulations by the SEC. In 2015-2016, the SEC approved the Revised Implementing Rules and Regulations of the SRC and the draft for the Implementing Rules and Regulations of the Investment Company Act and the proposed revisions for the SRC are also being prepared.

The SEC also came out with the Revised Code of Corporate Governance for Publicly Listed Companies in 2016. It stresses that a strong corporate governance framework combats corrupt practices, e.g. bribery, fraud, extortion, collusion, conflict of interest, and money laundering.

The SEC also ensures that capital market professionals are informed about AML/CFT regulations. In 2016, the SEC approved the new modularized Certification Seminar and Examination for SEC Certification Programs and Licensure Examination which include a module on Anti-Money Laundering.

To understand the AML/CFT structure and framework of the securities sector, information pertaining to AML/CFT measures, risk profiling and their monitoring system in place was gathered from the reports submitted. The profile of the securities sector is as follows:

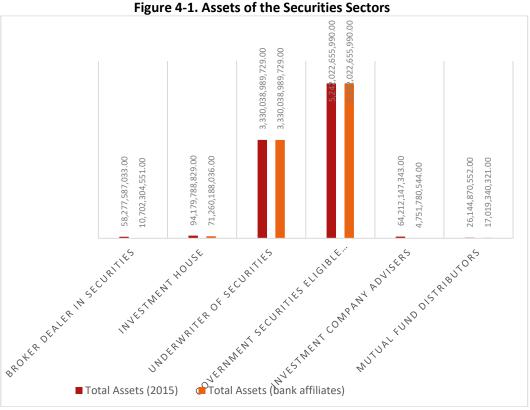
**Table 4-1. Securities Sector Profile** 

Type of License	No. of Entities (as of 2016)	Nationality	Type of Client
Broker Dealer in Securities	146	local - 131 with foreign equity - 15	retail and institutional
Investment Houses	28	local – 23	retail and institutional

		with foreign equity - 5	
Investment Company Advisers/Mutual Fund Distributors	21	local – 19 with foreign equity - 2	retail and institutional
Mutual Fund Companies	61	local	retail and institutional
Transfer Agent	22	local	retail and institutional
Underwriters of Securities	12	local- 5 with foreign equity - 7	retail and institutional
Government Securities Eligible Dealers	24	local – 15 with foreign equity - 9	retail and institutional

Most of the firms dealing in mutual funds are also bank affiliates or with foreign equity which have strict AML policies. Vulnerability to AML/CFT is mitigated by appropriate AML controls from strict customer acceptance to monitoring of transactions and regular training for their personnel. They are also subjected to regular AML audit by the SEC.

The total assets of covered persons for 2015 is PhP8,814,876,039,476, while the asset of the market intermediaries affiliated with bank is P8,675,795,259,171.00, divided into the following sectors:



### DATA AND INFORMATION COLLECTION

The data used in this assessment were collected from the following sources:

- Applicable laws, rules and circulars
- B. Reports submitted to the Securities and Exchange Commission

- Capital Market Integrity Corporation (CMIC) Audit Reports
- Revised Anti-Money Laundering Operating Manual
- Broker's Dealers Associated Person's Quarterly Compliance Report (SEC Form 30.2)
- C. Data available at the Anti-Money Laundering Council Secretariat
  The covered persons registered with the AMLC and the Covered and Suspicious Transaction
  Reports (CTRs and STRs) submitted by them to verify their claim that they submit CTRs and STRs
  to the AMLC.
- D. Survey form prepared by the Securities and Exchange Commission

The SEC prepared a survey form which were distributed to (i) twenty (20) broker-dealers representing 90% of the sector, based on total value of transactions in 2016; (ii) six (6) investment houses, representing almost 80% of the sector, based on asset size for 2015 and (iii) four (4) Investment Company Advisers to determine prevailing AML/CFT measures in place within the securities sector. Respondents to this survey are Associated Persons/Compliance Officers representing their respective institutions.

Mutual fund companies and transfer agents were not considered in the report because the transactions of mutual companies emanate from investment company advisers/mutual fund distributors while transfer agents are not covered persons. Underwriting of securities and dealers of government securities, are also excluded from the Report considering that such functions are usually provided by firms which are affiliated with banks, thus, covered by the banking sector.

Also, several group discussions/meetings were conducted to discuss the AML General Controls. The group discussions/meetings were attended by the representatives from the SEC and the AMLC. The discussions allowed the representatives from the SEC to communicate with the AMLC representatives the results of the survey and the prevailing practices in the industry as communicated to them by the stakeholders, which in turn were considered to make an appropriate rating of the general variables. The meeting also served as a venue to discuss the gaps on the variables and to suggest recommendations to address said gaps.

In general, the assessment in the vulnerability of the security sector is a result of the collaboration and cooperation of the stakeholders supported by quantitative and qualitative information.

### **SECTOR VULNERABILITY ASSESSMENT**

The vulnerability map, after assessing each input variable, showed an overall **MEDIUM** securities sector vulnerability, because of **MEDIUM** quality of general controls.

The SEC recognizes that the system of ML/TF is constantly changing and there is a need to continually improve the regulatory requirements to improve implementation of the AML/CFT laws, rules and regulations. The vulnerability of the securities sector to ML/TF risks are mitigated and addressed by the continued efforts of the industry to adhere to AML international standards in order to protect their reputation.

However, as the securities sector is still vulnerable to ML/TF risks, market intermediaries should still be equipped with a good risk based customer acceptance policies and procedures to prevent suspicious entities and individuals from opening an account. There is also the need to enhance their AML/CFT monitoring system to track unusual activities and suspicious transactions. On the part of the

SEC, there is a need to conduct regular audits on market intermediaries focusing on their compliance with to AML/CFT requirements.

Quality of AML Supervision	Effectiveness of Supervision Procedures and Practices	Medium High
(Medium)	Availability and Enforcement of Administrative Sanctions	Medium

The Quality of AML Supervision is rated based on whether the institutions under the Securities sector are covered by comprehensive supervision regime supported by appropriate powers, staff and other resources

#### **Effectiveness of Supervision Procedures and Practices**

The SEC supervises and regulates the following covered persons:

- securities dealers, brokers, salesmen, investment houses, and other similar persons managing securities or rendering services, such as investment agents, advisors, or consultants;
- ii. mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities; and
- iii. other entities, administering or otherwise dealing in commodities, or financial derivatives based thereon, valuable objects, cash substitutes, and other similar monetary instruments or properties.

Supervision over the above-mentioned covered persons is made by the implementation and enforcement of the Securities and Regulation Code (SRC) or Republic Act (RA) No. 8799, The Investment Houses Law or Presidential Decree No. 129, Investment Company Act or R.A. No. 2629, and the Corporation Code of the Philippines or Batas Pambansa Blg. 68.

The current organizational structure of the SEC has an ad-hoc AML/CFT desk as an attached function to its Enforcement and Investor Protection Department (EIPD) addressing queries on AML/CFT matters. To formalize the function of the AML/CFT desk and to address the AML/CFT challenges and gaps, the SEC approved last 2016 the creation of twenty-eight (28) positions and the creation of an AML unit. The SEC also submitted to the Department of Budget and Management (DBM) the approved the plantilla positions in the said unit for budget purposes.

Meanwhile, the EIPD through its Market Surveillance Division and the Capital Markets Integrity Corporation (CMIC) have authority to monitor and regulate equities trading. The EIPD is also authorized to conduct surveillance of the trading of securities in exchanges and ensure compliance of market participants and intermediaries with Sections 24, 26 and 27 of the SRC and its IRR and in pursuance thereof, coordinates with SROs (PSE, PDEX & CMIC), market participants (TPs, IH, TAs PDTC, etc.) and other law-enforcement agencies (NSI, PNP-CIDG, AMLC, etc.). This may allow easier monitoring of such transactions.

In addition, the SEC performs oversight regulation through the on-site supervision conducted by the CMIC, a self-regulatory organization (SRO) whose mandate is to monitor and supervise the broker-dealers who are members of the Philippines Stock Exchange (PSE). Although the CMIC examines all its members at least once a year, the examination is focused on the violation of the Securities and

Distributor/

Investment Company Advisers

Investment

Houses

2015

2016

2014

2015

2016

**STRs** 

14

8

0

0

0

Regulation Code, including customer identification and record keeping requirements as well as the existence of an AML/CFT Manual. However, in 2016 per SEC instruction, the CMIC included in its audit the validation of compliance with the AMLA requirements. Thereafter, the CMIC files with the SEC monthly reports of its periodic examinations started and completed during the month, within ten (10) days after the end of each month, together with a summary of findings for audits completed.

The Commission may, on its own initiative, conduct periodic or parallel examinations of members to validate the SRO's findings and conduct on-spot audit inspections of the relevant SRO department to check if it is fulfilling its duties and responsibilities as an SRO.

In the case of securities affiliated with banks, it is the Bangko Sentral ng Pilipinas (BSP) which audits the same to ensure compliance with the AMLA, its RIRR and BSP Circular No. 706. As of December 2016, there are eleven (11) broker-dealers affiliated with banks; nine (9) mutual fund investor/investment company advisers and twenty-one (21) Investment Houses/Underwriter of Securities.

Lastly, the SEC issued directives in the form of letters addressed to all covered persons under its supervision and regulation to reiterate the requirements of AMLA. For the year 2015-2016, the Commission directed them to register with the Anti-Money Laundering Council (AMLC) and to submit CTRs and STRs. As a consequence, the number of CTRs submitted to the AMLC increased, as shown in the data of the AMLC:

Table 4-2. SEC Covered Persons Registered and Reporting to AMLC

12

10

4

5

4

50,302

49,558

2,380

3,889

5,256

TYPE OF INSTITUTION	YEAR	NO. OF ENTITIES REGISTERED WITH SEC	NO. OF ENTITIES THAT REGISTERED WITH AMLC	NO. OF CTRs SUBMITTED TO AMLC	NO. OF SUBMITO AN
	2014	148	85	406,245	30
Brokers/Dealers	2015	1/10	9.4	525 018	10

58

61

27

28

28\*

ITTED MLC Brokers/Dealers 2015 148 525,918 2016 10 146 85 591,671 Mutual Fund 2014 54 11 46,262 3

Based on the AMLC data about 60% of brokers, 16% of MF/ICA and 14% of Investment Houses have registered with AMLC as of 2016. Despite the directive of the SEC to register with the AMLC, covered persons still failed to register. The reason for the same is that it is not a requirement for incorporation nor for the issuance of a secondary license. Also, in 2016 there are twenty-eight (28) Investment Houses registered with the SEC and twenty-one (21) of these are affiliated with banks to ensure compliance with AMLA. Thus, the fact that Investment Houses did not submit STRS does not mean that they are not compliant with the AMLA but since the BSP is checking compliance to at least 75% of the total Investment houses.

<sup>\*21</sup> of the Investment houses are affiliates of banks and thus subject to the supervision of the BSP

### **Availability and Enforcement of Administrative Sanctions**

The power of the SEC to impose administrative sanctions for violation of the AMLA on the requirement of customer identification and verification, record keeping and the delay or non-submission of AML Manual emanates from the 2015 SRC Implementing Rules and Regulations and Memorandum Circular No. 19, respectively. The sanctions comprise of suspension, or revocation of license, disqualification from being an officer, member of the Board of Directors or monetary penalties.

In addition, the CMIC, as mentioned earlier, conducts audit to ensure that broker-dealers comply with the Securities Regulation Code and its implementing rules and regulation, the AMLA and its implementing rules and regulations. In case of non-compliance, it imposes sanctions ranging from monetary fines to suspension. In the years 2015 – 2016, CMIC referred the following cases to the SEC for AMLA violations:

**Table 4-3. Sanctions Imposed on SEC Covered Persons** 

YEAR THE AUDIT CONDUCTED	TYPE OF INSTITUTION	NO. OF INSTITUTIONS INVOLVED	VIOLATION	SANCTION
2016	Broker- Dealers	2	customer acceptance policies/face-to-face verification	written reprimand/monetary penalty
2015	Broker- Dealers	3	keeping current/updating of information; information for corporate clients; know its clients well, updating of info	monetary penalty/written reprimand

In the case of securities affiliated with banks, the BSP is authorized to impose administrative sanctions in cases of violation of the AMLA, its RIRR and BSP Circular No. 706. Consequently, in case of non-compliance, it may impose administrative penalties in the form of reprimand, suspension, removal or disqualification from office of the director/officer and monetary penalties.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of	Quality of AML Supervision	Medium
Management in  Securities Firms	Availability and Enforcement of Criminal Sanctions	Medium High
(Medium High)	Level of Market Pressure to Meet AML Standards	High

The Commitment and Leadership of Management in Securities Firms assesses the management of the securities institutions or firms' (of the assessed securities institution type) commitment and leadership in relation to AML, and how the managements are influenced by regulations on the entry or registration controls, the quality of AML supervision and enforcement of criminal sanctions, and market pressure.

### **Availability and Effectiveness of Entry Controls**

The Securities Regulation Code, the Investment Houses Law and the Investment Company Act provide the primary source mandating the SEC's authority to regulate the securities sector. The SEC formulates policies and recommendations on issues concerning the securities market. It regulates, investigates or supervises the activities of persons to ensure compliance and impose sanctions for the violation of laws and the rules, regulations and orders issued.

The implementation of the 2015 SRC IRR provided the following entry controls to ensure high level of compliance with AML requirements. Entities applying for registration in the securities sector are required to submit Written Supervision and Control Procedures which shall take into consideration the requirements of the AMLA, as amended, while persons applying for registration including the directors and officers of the firms are required to submit their bio-data as well as certified true copy of educational, professional/technical or other academic qualifications.

The current policies and programs are strongly aligned with the AML/CFT regime's mission objectives. In fact, as per existing doctrines and policies, programs for the implementation of the regulated sectors licensing and registration processes are set in place. In support thereof, for strict implementation are policies requiring covered persons to submit their respective Money Laundering Programs and Processes (MLPPs). On the other hand, associated persons and salesmen or traders in the securities sector are now required to take separate AML/CFT examinations.

Relative thereto, the augmentation of existing capabilities in terms of manpower complement and dedicated unit to address gaps posed by challenges to effective implementation, are currently underway. Presently, efforts towards a realization of the need for a dedicated Unit is in the pipeline, with the pending DBM request for approval of an additional personnel to man the SEC's AML/CFT desk.

Indeed, the current environment has provided a foundation ripe for enhanced building blocks needed to strengthen the securities sector's regulation. As gleaned from the data, an existing system where close interaction between the public and private sectors is being enhanced. As far as the SEC is concerned, there is a dire need to adapt to the increased mandate of the law as seen from the current amendments to the legislation. Supplementing current complement with an increase in budget, additional manpower, relevant trainings, including possible reorganization of existing structures (e.g. creation of a dedicated Unit within EIPD of the SEC to oversee thrusts on integrating AML/CFT initiatives) is in order. This Unit shall be tasked to focus on research and analysis, and to recommend strategic plans and policies, and acquisition of relevant materials/equipment and facilities to accommodate expansion.

Significantly, after a review of existing key performance indicators, the SEC needs to formulate a definitive role in further enhancing its Entry Controls in support of higher strategy. This would mean the need to review current systems initiatives which impact on medium to long-term strategies towards achieving an ideal internationally compliant status for the securities sector AML/CFT regulation.

As observed, there is also the need to address interoperability by identifying and converging essential tasks (lifted from its mandate of providing specific and implied tasks) of the agency's relevant AML/CFT function. In so doing, a securities regime, which would be at par with international standards, as well as endowed with a local imprint, could be established.

From addressing the tactical and operational gaps and challenges, the securities sectors regime could be aligned with higher strategy of national objectives designed to support national interests (e.g. secure environment for investments and economic prosperity of the nation as a whole).

### **Quality of AML Supervision**

The quality of AML Supervision is also a factor in enforcing the commitment of the Securities institutions. The SEC has the authority to enforce laws, rules and regulations on AML/CFT matters.

### **Availability and Enforcement of Criminal Sanctions**

The AMLA, as amended, imposes sufficiently harsh penalties consisting of imprisonment and/or fines upon persons found to have committed money laundering offenses, including, transacting the proceeds of predicate crimes, facilitation and attempt to commit money laundering. Notably, criminal penalties may be imposed for failure to file CTRs and STRs.

Imprisonment for money laundering and other violations of the AMLA, as amended, ranges from seven (7) to fourteen (14) years.

The AMLC enforces AML obligations through the filing of criminal complaints with the DOJ. For money laundering activities, the predicate crimes employed to derive proceeds for money laundering are identified, which, in the case of the securities sector, are violations of the SRC. The filing of the complaint commences the preliminary investigation, an administrative procedure in which the respondent is given the opportunity to refute the complaint's allegations. If the investigating fiscal finds the existence of probable cause for money laundering, he issues a resolution recommending the filing of a criminal *information* before the proper court. Otherwise, he dismisses the complaint. The filing of the information in court marks the beginning of judicial proceedings. Money laundering is a bailable offense.

Unless the accused pleads guilty to the offense charged or to a lesser or other offense, criminal proceedings undergo trial. The prosecution must meet the required burden of proof for criminal cases: beyond a reasonable doubt.

The statistics on SRC-related violations are as follows:

#### For the year 2015:

Predicate offense (Violation of Securities Regulation code)	Number of cases detected or investigated	Number of complaints filed with the DOJ	Number of convictions (cases)	Number of persons convicted	Number of cases with information filed before the courts	Number of cases referred to AMLC
Sec. 8 R.A. No. 8799	95	2	1	1		1
Sec. 10, R.A. No. 8799	1					
Sec. 12, R.A. No. 8799	61					
Sec. 17.1, R.A. No, 8799	1					
Sec. 24 (b) (i) and (iii) R.A. No. 8799					1	
Sec. 26, R.A. No, 8799	12					
Sec. 27, R.A. No. 8799	3					
Sec. 28, R.A. No. 8799	12					
Sec. 68, R.A. No. 8799	18	1				
Total	203	3	1	1	1	1

#### For the year 2016:

Predicate offense	Number of	Number of	Number of	Number of	Number of	Number of
(Violation of Securities	cases	Complaints	convictions	persons	cases with	cases
Regulation code)	detected or	filed with the	(cases)	convicted	information	referred to
	investigated	DOJ			filed before	AMLC
					the courts	
Sec. 8 R.A. No. 8799	75	2			4	14
Sec. 26, R.A. No. 8799	54	3			4	
Sec. 27, R.A. No. 8799	1					
Sec. 28, R.A. No, 8799	16	8			5	
Sec. 68, R.A. No. 8799	1					
Total	147	13	0	0	13	14

# **Level Market Pressure to Meet AML Standards**

The securities sector together with other financial institutions is aware of the need to adhere to strict AML/CFT laws and regulations both from local and international parties. Local and foreign regulators, enforcement agencies, business partners, and international counterparty financial institutions are some of the sources of market pressure to meet AML standards.

Market intermediaries associated with foreign entities are required to comply with international AML/CFT regulations and are required to use AML/CFT controls of the conglomerate. Some of them are also subjected to audit/visit by the AML Compliance Unit of their foreign counterpart at least once a year.

The recent development of the global and international financial practices is an indication that the market intermediaries should continuously strengthen their AML/CFT standards and be aligned with global best practices.

The SEC together with the AMLC is working towards the effective implementation and enforcement of AML/CFT initiatives in the securities sector. The challenge for the SEC and the AMLC is to continue its coordination with securities industry to ensure there is common understanding of the AML/CFT requirements and the rules and regulations are disseminated to all regulated entities.

Quality of Internal	Comprehensiveness of AML Legal Framework	Medium High
AML policies and procedures	Commitment to Leadership of Management in Securities Firms	Medium High
(Medium)	Effectiveness of Compliance Function	Medium

**Commitment to leadership of management** takes into account the institutions' commitment and leadership in AML and their respective managements are influenced or affected by the regulations on entry controls such as registration and licensing, and the quality of AML supervision. This was discussed in the previous section.

#### Comprehensiveness of AML Legal Framework

The SEC, being the authority responsible for AML/CFT preventive measures and monitoring compliance of the covered persons it regulates, issued various Circulars to effectively implement and enforce the anti-money laundering regime and combating terrorist financing:

- 2016 Revised Code of Corporate Governance for Publicly Listed Companies;
- 2. 2016 Modularized Certification Seminar and Examination for SEC Certification Programs and Licensure Examination, including a module on Anti-Money Laundering;
- 3. 2015 Revised Implementing Rules and Regulation of the Securities Regulation Code;
- SEC Memorandum Circular No. 19, Series of 2016
   Re: Revised Code of Corporate Governance for Publicly Listed Companies;
- 5. SEC Memorandum Circular No. 19, series of 2014
  - Re. Submission of the Anti-Money Laundering Manual & Anti-Money Laundering Compliance Form (for Financing and Lending Companies);
  - SEC Memorandum Circular No. 10, series of 2013
  - Re. Updated General Information Sheet (inclusion of page 1-A pursuant to Anti-Money Laundering Act, as amended);
- 6. SEC Memorandum Circular No. 2, series of 2010
  - Re. Revised Guidelines in the Preparation of Anti-Money Laundering Manual for SEC covered institutions;
- 7. SEC Memorandum Circular No. 8, series of 2010
  - Re. Extension of the deadline to submit Revised Anti-Money Laundering Manual for SEC covered institutions pursuant to SEC Memo Circular No. 2, s. 2010;
- 8. SEC Memorandum Circular No. 12, series of 2004
  - Re. Guidelines in the Preparation of the Revised Anti-Money Laundering Operating Manual for Covered Institutions;
- 9. SEC Memorandum Circular No. 11, s. 2004
  - Re. To all SEC Covered (Regulated) Institutions: Submission of the Anti-Money Laundering Council of reports;
- 10. SEC Memorandum Circular No. 9, series of 2002
  - Customer identification an AMLC Forms for Covered Transactions Reports and Suspicious Transactions Reports for Covered Institutions; and
- 11. SEC Memorandum Circular No. 1, series of 2002
  - Re. Anti-Money Laundering Operating Manual for Covered Institutions.

In SEC Memorandum Circular No. 2, Series of 2010, the SEC issued the guidelines and requirements for the covered persons with respect to their respective AML/CFT program: (i) customer identification and verification, including beneficial ownership; (ii) risk-based customer acceptance policy, (iii) record keeping requirements; (iv) reporting requirements and on-going monitoring of covered and suspicious transactions; and (v) AML training programs.

Aside from the regulations issued by the SEC on 2015 and 2016, it created on December 2016 a Technical Working Group tasked to revise Memorandum Circular No. 2, Series of 2010 in order to update the same in compliance with the 2016 Revised Implementing Rules and Regulations of the AMLA, as amended, issued by the AMLC.

Aside from the above-mentioned Circulars and RIRR, the SEC on a regular basis disseminates to its regulated persons Resolutions regarding entities and persons, local or international, which are in the watch list of the UN and Anti-Terrorism Council, including Resolutions involving interpretation of the law or the RIRR.

### **Effectiveness of Compliance Function**

The assessment of the current state of the Philippine's AML-CFT regime's Securities Sector's *Effectiveness of Compliance Functions*, validates the existence of strong cooperation and consultation by and between the regulator and the regulated institutions. The programs and policies instituted by the SEC in recent years would show high awareness by the regulated institutions of their need to establish comprehensive, risk based and well-resourced independent AML/CFT compliance functions.

To this effect, 100% of the securities sector's covered institutions were found to have designated compliance officers tasked to implement their respective AML programs. Figures would also reveal that compliance officers in this sector maintain a manual of compliance procedures, which ensures staff compliance with AML/CFT regulations. In the current setting, the covered institutions have in place in their respective systems reporting of CTRs and STRs to ensure compliance.

Notably, likewise set in place are mechanisms underscoring the strong relationship with the regulators - with most of the compliance officers themselves acting as liaison officers between their respective companies and the AMLC. In line with this, feedback validates that compliance officers/ Associated Persons immediately disseminate updates on AML/CFT regulations to officers and staff after engagement with said regulator. Moreover, the same feedback reveals that more than half of the sector's compliance officers would take it upon themselves to prepare and submit required reports to the AMLC.

In furtherance thereof, it has been established that CMIC examinations of PSE broker-dealers is being done, ensuring to a certain extent, compliance with AML/CFT regulations.

Finally, collaboration with other regulatory agencies contribute to a stronger framework, with the BSP examinations on market intermediaries affiliated with the banking sector (e.g. banks) further enhancing compliance with AML/CFT regulations.

However, on the operational level, there is a need to enhance the capabilities of the concerned Agencies initiatives through enhancement of the existing laws and legal policies<sup>132</sup> alike; continuing integration of all stakeholders (public and private) deemed necessary to effectively achieve mandate; enhancing current and perceived manpower's knowledge, skills and values, including recruitment of competent manpower to complement the existing manpower (both regulator and regulated); key leadership at all levels of the concerned organizations (public and private); undertaking dynamic trainings designed to enhance AML/CFT knowledge and skills, including those meant to develop and enhance the interoperability of concerned agencies; providing and enhancing existing resources required for AML/CFT initiatives; and provide a safe and secure installation, in a networked environment, to AML/CFT regime's database, including acquisition of equipment to maintain integrity of resources and to allow a sustained collaboration alignment among concerned agencies.

Page **141** of **300** 

Staff Compliance on Securities Firms (Medium)	Quality of AML Supervision	Medium
	Availability and Enforcement of Criminal Sanctions	Medium High
	Effectiveness of Compliance Function	Medium
	Integrity of Staff in Securities Firms	Medium High
	AML Knowledge of Staff in Securities Firms	Medium

The *quality of AML supervision* is assessed based on the effectiveness of the supervisory authority in implementing supervision procedures and practices, and in enforcing administrative sanctions. The *availability and enforcement of criminal sanctions* considers the legal framework, enforcement actions taken against securities firms and individual members of the management and their staff.

Compliance to AML can be assessed through three inter-related factors. One is the *effectiveness of compliance function* which assesses whether the securities firms or institutions have a comprehensive, risk-based and well-resourced with independent AML compliance function. The effectiveness of compliance function contributes to the quality of internal AML policies and procedures, as discussed in the above AML combating control.

### **Integrity of Staff in Securities Firms**

Another factor is the integrity of staff of the securities firms. This assesses whether the staff acts with integrity and does not act in willfully blind manner or collude with criminals.

Republic Act No. 8799 or the Securities Regulation Code states that the State shall establish a socially conscious, free market that regulates itself, encourage the widest participation of ownership in enterprises, enhance the democratization of wealth, promote the development of the capital market, protect investors, ensure full and fair disclosure about securities, minimize if not totally eliminate insider trading and other fraudulent or manipulative devices and practices which create distortions in the free market. These general mandates necessitate that market participants operate with the highest ethical standards and integrity and comply with all laws and rules intended to achieve these goals.

However, there are still instances where employees of the market intermediaries perpetuate criminal acts under the SRC. The most recent case is the alleged scam committed by a former official of the Philippine Stock Exchange (PSE) who was accused of orchestrating the biggest scam in PSE history amounting to Three Hundred Million Pesos (PhP300,000,000.00) and who was subsequently indicted by the DOJ. The DOJ recommended no bail for the syndicated estafa charges and approved the filing of a separate case for the said employee over bouncing checks.

Cases like this made industry participants, regulators, and legislators recognize the necessity for an enhanced focus on ethics and compliance, and the need to take remedial actions and introduce proactive initiatives.

On the other hand, it is satisfactory that integrity issues of market participants were acknowledged and addressed as there were rules specifically requiring codes of conduct and effective compliance programs in securities firms. In general, the CMIC imposes upon all its members fair, ethical and

efficient practices in the securities industry. In addition, it obligated its members to adhere to the following guidelines in dealing with their clients, their firms and the CMIC, thus:

- i. Traders and salesmen should adhere at all times to the principles of honesty, integrity, fairness and good business practice in the conduct of their business affairs;
- ii. Transactions that may involve conflicts of interest should be avoided, but when they cannot possibly be avoided, a trader or salesman should ensure that the client's interest is not subordinated to his own and his client is treated fairly before the transaction is executed. Fair treatment includes, but is not limited to, full disclosure to the client of all material facts related to a transaction involving conflict of interest;
- iii. Traders and salesmen should act and carry themselves in a manner that would promote and maintain the integrity of their firm, in particular, and the market, in general;
- iv. Traders and salesmen should observe all applicable regulatory laws, rules and regulations, comply with all regulatory requirements and abide by the internal rules of their firm at all times;
- v. Trader or salesman shall not accept or solicit an advantage from any person in connection with his company's business if such act can influence his objectivity in performing his duties, induce him to act against the interest of his company and clients, or lead to allegations of impropriety;
- vi. Traders and salesmen may come across non-public or confidential information on listed companies or their clients or employer. Without prejudice to the disclosure and other requirements of the Securities Laws or other relevant laws, traders and salesmen have a fiduciary duty in respect of such information and, unless authorized by the relevant parties, shall not disclose, share or otherwise use the information, especially for their personal gain or benefit;
- vii. Traders and salesmen shall not initiate or otherwise participate in market rumors, which may lead to allegations of price manipulation or insider trading;
- viii. Traders and salesmen shall not engage in excessive gambling of any kind with persons having business dealings with their company. In social games of chance with clients or business associates, they must exercise judgment and withdraw from any high stake; and
- ix. Trading Participants and their directors, officers, employees and duly authorized agents shall exercise utmost professionalism in dealing with CMIC.

Similarly, as provided for in Section 39.1.1.3.2. of the 2015 Implementing Rules and Regulations of the Securities Regulation Code, the CMIC, as the SRO, shall adopt comprehensive rules governing its organization and governance, qualifications and rights of shareholders, listing of securities, trading of securities, settlement of contracts, qualification of members and other participants, ethical conduct of members and other participants, supervision and control of members, financial and operational responsibility of members, and discipline of members and other participants.

Furthermore, in 22 November 2016, the 2016 Code of Corporate Governance for Publicly-Listed Companies was issued. The Code requires the Board of the publicly listed companies to adopt a Code of Business Conduct and Ethics, which would provide standards for professional and ethical behavior, as well as articulate acceptable and unacceptable conduct and practices in internal and external dealings. Furthermore, the Board shall ensure the proper and efficient implementation and monitoring of compliance with the Code of Business Conduct and Ethics and internal policies.

The above are only a few examples of laws, rules and regulations mandating effective supervisory and compliance programs at securities firms. These reinforce the obligation of the staff in securities firms to act with integrity. Additionally, these framework draws the attention to staff not to act in a willfully blind manner or conspire with offenders or act dishonestly. These also ensure that staff does not

become unwittingly involved with offenders who seek to use their products including specialized knowledge and skills.

However, these specific requirements and procedures are not enough. Firms should have a culture of compliance inculcated from the top to bottom of the hierarchy to advocate a compliant and high-integrity atmosphere at a firm and thus, the following regulations are in place:

- Applicants for registration as salesmen and associated persons must have no disciplinary history that would subject them to refusal of registration under Section 29 of the SRC or warrant the suspension or revocation of their registration; and
- ii. Applicants for registration as an Associated Person, must not have been censured or reprimanded by a professional (e.g. IBP, PRC, etc.), or regulatory body (e.g. SEC, BSP, IC, etc.) for negligence, incompetence or mismanagement, or dismissed or requested to resign from any position or office for negligence, incompetence or mismanagement, or be subject to any other disqualification under Section 29 of the Securities Regulation Code.

#### **AML Knowledge in Securities Firms**

Lastly, AML knowledge plays a role on the effectiveness of compliance function. Officers and staff of securities firms should have understood their AML duties and obligations.

The SEC through Memorandum Circular No. 2, Series of 2010 directed covered persons under its supervision and regulation to ensure that its staff are well-trained in the aspect of AML/CFT matters. The training must give the staff proper grounding or background on money laundering, the procedure in conducting appropriate customer identification and verification, the requirement for the retention of records, the proper identification of covered and suspicious transactions and the need and manner of reporting such transactions to the appropriate designated person within the covered institution and offenses and penalties arising from the AMLA violation. Furthermore, a higher level of instruction covering all aspects of anti-money laundering procedures should be provided to supervisors and managers.

In addition, covered institutions are obligated to conduct refresher trainings at least once a year to remind their staff and officers of their responsibilities and to make them aware of any changes in the laws and rules relating to money laundering, as well as the internal procedures of the covered institutions.

Based on the survey conducted by the SEC, the associated persons and compliance officers of the concerned covered persons disseminate updates on relevant AML rules and regulations to their officers and employees during meetings and trainings, and through issuances of memoranda. Similarly, they require their employees to undergo annual online AML/CFT trainings with focus on customer acceptance and identification process, record-keeping, covered and suspicious transaction reporting, and internal control processes. Trainings also include employees' obligations and responsibilities as well as updates on any changes in AML laws, rules and internal policies, and procedures. The said trainings are complemented by examinations to check the level of understanding of AML/CFT rules and regulations.

Every application for registration of a Corporate Broker/Dealer is accompanied by yearly schedule/timetable on the implementation of the training program for the staff, which specifies, among others, the description of the training program, date of implementation and name of participants.

In fact, to ensure compliance with the requirement on training, brokers-dealers conducted 81 and 95 AML training for the years 2015 and 2016, respectively, compared to the 83 trainings conducted last 2014.

Furthermore, securities firms employ staff who possess the skills, knowledge and expertise to carry out their functions effectively. They review employees' competence and take appropriate action to ensure they remain competent for their role.

On the other end of the spectrum, the SEC regularly conducts seminars for salesmen and associated persons of Brokers/Dealers, an integral part of which is a discussion on AMLA. For the years 2015 to 2016, the SEC conducted seven (7) seminars. Also, annual refresher courses and training programs are mandatory requirements for the renewal of license of market intermediaries.

Aside from trainings, the SEC also issues reminders or clarifications through memoranda or frequently asked questions on salient AML regulations which are accessible in the website and it provides market intermediaries updated materials on AML/CFT regulations.

Quality of CDD	Availability and Access to Beneficial Ownership	Medium High
Quality of CDD framework (Medium)	Availability of Reliable Identification Infrastructure	Medium High
(	Availability of Independent Information Sources	Medium

The quality of CDD framework assesses whether a country has the legal, institutional, and technical framework to identify and verify the identities of natural and legal persons, as well as the capacity to store the identification records. The framework shall also facilitate the use of information by authorized parties for AML purposes.

# **Availability and Access to Beneficial Ownership**

Admittedly, there is no single database or facility containing information on beneficial interests in corporations, trusts and similar entities available in the country. Despite this challenge, authorities and covered persons can obtain information on beneficial ownership from the SEC for corporations and partnerships, the Cooperative Development Authority (CDA) for cooperatives, and Department of Trade and Industry (DTI) for sole proprietorship.

Section 18 of the SRC in relation to its 2015 IRR, requires that any person who acquires beneficial ownership of more than five (5%) of a class of share must submit a sworn statement to the SEC stating such fact and other details pertaining to the acquisition, such as the identity, residence and citizenship of the beneficial owner, nature of such beneficial ownership, the purpose of his acquisition, and details pertaining to the contract of acquisition. Complementing said provisions, Rule 30.2.1.2.4.2 of the 2015 SRC IRR on the Ethical Standard Rule of Information About Clients, requires broker dealers to acquire mandatory client information to establish beneficial ownership, among others. Furthermore, the SEC has the power to inquire the ultimate beneficial ownership.

Information on the structure, management, control and beneficial ownership are primarily obtained by covered persons from clients. Representations of clients are required to be supported by relevant documents, such as Certificate of Registration, Articles of Incorporation or Certificate of Partnership,

By-laws, General Information Sheet (GIS), and identification documents of shareholders and officers of the client. Moreover, covered persons are required to put in place satisfactory measures to identify natural persons with controlling interest and natural persons who comprise the management of a legal person or arrangement.

Financial transparency and customer identification and verification processes are enhanced when AML-regulated institutions are able to verify the identity of customers using reliable, independent source documents, data or information. This will prevent the use of fictitious documents.

# **Availability of Reliable Identification Infrastructure**

Prevailing regulations on customer identification require covered persons to perform the following:

- 1. Develop a clear written customer acceptance policy and procedures in offering its products and services;
- Record competent evidence of the client's true and full identity or representative capacity, domicile, legal capacity, occupation or business purpose, and other identifying information;
- 3. Apply a full range of customer due diligence measure based on the risk posed by clients;
- 4. Undertake initial and regular verification of material client information and conduct continuing due diligence to ensure that client transactions are consistent with the client's ownership, business profile and source of funds; and
- 5. Monitor unusually large transactions and unusual patterns of transactions.

To comply with the requirement of verifying and validating the identity of their clients, covered persons require the presentation of a valid, government-issued identification document for individuals, Certificate of Incorporation/Registration, Articles of Incorporation or Certificate of Partnership, By-laws, latest GIS, and identification documents of shareholders, officers and official representatives for legal entities or juridical persons.

Although there is no single national ID system in the country, authorities recognized a list of acceptable identification documents. The government institutions issuing the foregoing IDs perform verification on the identity and personal information of the member before issuing the ID. Hence, the member's information (i.e. name, sex, age, birthday, address, nationality, etc.) contained in these IDs can be reasonably relied upon by covered persons.

Broker-dealers representing 90% of the value of equity transactions for the industry in 2016 claim to comply with the foregoing customer identification requirements. Actual compliance is checked by the CMIC annually.

The availability of independent and reliable sources of information determines the transaction patterns of clients. This facilitates customer due diligence (CDD) process, which includes identifying and or verifying clients' transactional patterns and commercial history. Information may be obtained from credit bureaus, previous banking relationships, and utility bills.

### **Availability of Independent Information Sources**

CDD requires the verification and validation of client information. Primarily, covered persons verify client information by checking the veracity of the client representations with official identification documents such as a government-issued ID for individuals, Certificate of Incorporation Registration, Articles of Incorporation or Certificate of Partnership, By-laws, latest GIS, and identification

documents of shareholders, officers and official representatives for legal entities. When there is doubt as to the accuracy of the information provided by the client, covered persons cannot reasonably form a belief as to his/her true identity, the following measures are commonly employed to validate client information and identity: 1) requiring the client to submit additional documents such as barangay certification, utilities statements, recent bank statements, income tax return, and Statement of Assets Liabilities and Net Worth (SALN) for PEPs; 2) contacting the client by telephone; 3) contacting the employer of individual clients; 4) and sending a letter to the client's address.

Covered persons associated with foreign institutions, including broker-dealers whose transactions constitute ninety percent (90%) of the total volume of equities trading transactions in 2016, two investment houses and two investment company advisers have access to a database or facility that screens prospective clients.

For broker-dealers, an additional measure to validate a prospective client's identity is the requirement of opening a bank account under his name prior to the start of business relations, which means that the bank conducted a customer identification and verification on the client. In addition, broker-dealers conduct their own customer identification procedures and not merely rely on the client on-boarding-procedures of the bank.

### **PREVAILING PRACTICES**

### A. Customer Identification and Verification (Know -Your-Customer Rule)

Based on the survey conducted by the SEC it was determined that, covered persons strictly implement their know your customer (KYC) policy by interviewing their clients personally whenever possible and requiring the presentation of at least one (1) valid, government-issued identification document. However, in cases where It allowed the opening of accounts through the internet or any other mode, said covered institutions have measures in place, such as obtaining certification by appropriate authorities of the documents provided, requisition of additional documents and requiring the first payment to be carried out through an account in the clients name with a bank who undertakes similar customer due diligence and requiring the submission of documents authenticated by the Philippine Embassy or Consulate for non-resident clients.

Also, covered persons practice risk profiling of clients. In fact, market intermediaries with foreign affiliates have an established Client Identification Program (CIP) where all clients are vetted in accordance with the CIP which is based on internal global standards for client identification and local regulatory requirements. CIP uses the risk- based approach which categorizes each client based on the money laundering, terrorist financing and financial crime risk they represent. The level of due diligence will depend on the risk profile of the client being on-boarded.

For high risk clients or Politically Exposed Persons (PEPs), it is the practice of the covered persons to refer the clients to the Compliance Officer for further investigation. Thereafter, the decision on the on-boarding of the prospective clients devolves upon the President or senior management of a committee created for the purpose.

Lastly, all covered persons surveyed regularly update their Customer Account Identification Form (CAIF) at least once a year or whenever necessary.

### B. Reporting of Covered and Suspicious Transactions

Based on the survey conducted, covered persons adopted an automated AML system in order to capture covered and suspicious transactions and eventually report the same to the AMLC. However, a great number of market intermediaries are not registered with the AMLC. Consequently, it would mean that a significant number of market intermediaries are not reporting STRs and CTRs. Based on the data available at the AMLC, there is a big gap between the entities registered with the AMLC and the entities reporting CTRs and STRs:

NO. OF **NO. OF ENTITIES ENTITIES** NO. OF ENTITIES **INDUSTRY TYPE YEAR REGISTERED** REGISTERED **REPORTING AMLC** WITH SEC 85 2014 148 85 2015 148 84 84 Brokers – Dealers 2016 146 85 85 11 Mutual Fund 2014 54 11 Distributor/Investment 2015 58 12 12 Company Adviser 2016 10 10 61 2014 27 4 4 **Investment Houses** 2015 28 5 5 2016 28 4 4

**Table 4-4. SEC- Covered Persons** 

### C. Record Keeping

Based on the survey conducted by the SEC, covered persons maintain and safe keep all the records of their clients for at least five (5) years from the date of the transaction.

	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium
Quality of Operations in Securities Firms	Quality of CDD Framework	Medium
(Medium)	Commitment and leadership in Management in Securities Firms	Medium High
	Staff Compliance in Securities	Medium

The quality of operations in securities firms assesses the quality of the operations of securities firms in preventing money laundering. Staff compliance, commitment and leadership of management, and quality of CDD framework are among the factors that contribute to the quality of AML operations in securities firms. Another factor that contributes to the quality of operations is the effectiveness of suspicious activity monitoring.

### **Effectiveness of Suspicious Activity Monitoring and Reporting**

The securities sector should have effective and appropriate systems for record keeping, monitoring and STR reporting to support their AML policies and procedures.

Memorandum Circular No. 2, Series of 2010 requires the following obligation to the market intermediaries in relation to suspicious monitoring and reporting:

- 1. To institute a system for the mandatory reporting of covered transactions and suspicious transactions;
- 2. To keep confidential from their customers the information or the fact that a report has been made or is in the process of being reported to the AMLC;
- 3. To report covered and suspicious transactions only to the AMLC;
- 4. To report to the AMLC the fact that their client has engaged in any of the unlawful activities under the AMLA; and
- 5. To maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the AMLC.

Likewise, the same Circular includes a safe harbor provision protecting from any administrative, criminal or civil proceedings any person for having made a suspicious or covered transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law. This provision aimed to encourage reporting of covered and suspicious transactions.

Based on the survey conducted by the SEC, the market intermediaries have a system in place to report covered and suspicious transactions to the AMLC. This is evident by an increase in the No. of CTRs submitted by market intermediaries in the years 2015 and 2016:

Table 4-5. Covered and Suspicious Transaction Reporting of SEC- Covered Persons

TYPE OF INSTITUTION	YEAR	NO. OF CTRs SUBMITTED TO AMLC	NO. OF STRS SUBMITTED TO AMLC
	2014	406,245	30
Brokers/Dealers	2015	525,918	10
	2016	591,671	10
Mutual Fund Distributor/	2014	46,262	3
Mutual Fund Distributor/	2015	50,302	14
Investment Company Advisers	2016	49,558	8
Investment Houses	2014	2,380	0
	2015	3,889	0
	2016	5,256	0

Furthermore, although there is a decrease in the number of STRs reported, most number of STRs filed in 2015 were related to an investment scam involving several unlicensed entities which allegedly offered or sold to the public, unregistered securities in the form investment contracts involving gold which occurred during the third and early fourth quarter of the year, unlike in 2014 wherein the most number of received STRs were related to graft and corruption.

Quality of AML Controls	Quality of Operations in Securities Firms	Medium
(Medium)	Quality of Internal AML Policies and Procedures	Medium

The quality of AML controls is assessed based on the overall quality of two components, (1) the comprehensiveness and effectiveness of AML policies and (2) operations within the securities firms. Both components assessed the commitment of leadership of management and effectiveness of compliance function.

#### **PRODUCTS VULNERABILITY**

	Securities Trading	Medium
Products Vulnerability	Mutual Funds	Medium
	Securities Underwriting	Medium Low

The following are major factors that were identified and used to assess the specific impact on the AML vulnerability of the sector's product/service. The information was obtained from surveys/reports submitted by market intermediaries.

#### 1. Volume and value of transactions

The riskiness of a particular product in relation to the volume and the value it generates or the size and the amount of transactions that flows into the product was considered in this variable. The total volume and value of transaction for the year for a particular product is an inherent factor to the vulnerability of the securities sector. When large transactions are placed in a particular product, launderers are attracted to use and launder illicit proceeds or funds from unlawful activities.

## 2. Profile of the customer using the product

The profile of the customer using the product is an inherent factor in assessing the ML vulnerability of a product. To know the type/nature of the customer who uses the product will provide the securities sector an understanding of the ML risks that it is exposed to.

### 3. Existence of Adequate and Specific AML/CFT controls

To manage and mitigate any potential ML risk, the AML/CFT controls of a particular product is assessed whether it is adequate and in place. When there are specific and strict AML/CFT controls on a product/service, vulnerability to ML is lessened because money launderer would not prefer to use a product that has stringent AML/CFT controls in place.

### **RISKINESS OF PRODUCTS/SERVICES IDENTIFIED**

**Equities Trading** is becoming a popular investment avenue in the Philippines. Broker-dealers play an important role in the financial markets, as they provide the infrastructure that facilitates stock trading. In 2015 and 2016 the total value of transactions that passed through or were executed by broker-dealers amounted to 1,799B and 1,776B, respectively. Investors are also embracing online platforms to trade stocks. For 2015, the number of online stock market accounts grew by 35.6% to 239,668 up from the previous year's count of 174,592. For 2016, according to the PSE Annual Report on stock market accounts, online trading accounts grew by 27.8% to 302,516. Online trades accounted for 53.7% of total market transactions in 2016.

Comparative statistics as to the performance of the trading in the Philippine Stock Exchange are, as follows:

	2015	2016
PSEi	6,952.08 – down 3.9% YTD	6,840.64 – down 1.6% YTD
Total Value Turnover	P2.151 trillion	P1.929 trillion
Average daily value	P8.96 billion – Up 1.8% YOY	P7.81 billion – down 12.9%
turnover		YOY
Market Capitalization	P13.47 trillion – down 5.5% YTD	P14.44 trillion – Up 7.2% YOY
Foreign Transaction	P59.76 billion net selling	P2.16 billion net buying
No. of listed companies	311	318
Initial Public Offerings (IPOs)	4 –Crown Asia Chemicals Corp.	4 – Golden Haven Memorial
	(CROWN); SBS Philippines (SBS)	Park, Inc. (HVN); Cemex
	Metro Retail Stores Group, Inc.	Holdings Philippines, Inc.
	(MSRGI); and Italpinas	(CHP);Pilipinas Shell
	Development Corp. (IDS)	Petroleum Corp. (SHLPH); and
		Shakey's Pizza Asia Ventures,
		Inc. (PIZZA)

Thus, the vulnerability of equities trading to money laundering is **MEDIUM**.

Equities trading can be an attractive channel for money laundering. Broker dealer firms are vulnerable to such risks if AML/CFT measures are not in place. ML risks are somehow mitigated by the regular audit conducted by the CMIC that ensures that these covered persons comply with regulatory requirements.

# **Investment House/Underwriting of Securities**

As regulatory and economic age environments improved, investment houses began to take on more role in capital market development. When opportunities for the industry was flooded with privatization, project finance and underwriting deals, investment houses contributed largely in the areas of issue management and underwriting deals ushering the age of initial public offerings.

The underwriting of securities by investment houses is a function usually provided by firms which are affiliated with banks. Investment houses with bank affiliation are covered by the bank's internal audit unit and the periodic examination of BSP. With this, the vulnerability of investment houses to money laundering is **MEDIUM LOW.** Inherent risks are mitigated by strict customer acceptance and close monitoring of customer transactions. Further, in the recent years, the bulk of transactions of investment houses have been limited to financial advisory only.

# **Mutual Fund/Investment Company Advisers**

The popularity of mutual funds in the Philippines is fast catching up. One of the main attractions of mutual funds is that it affords its investors the services of full-time professional managers whose job is to analyze the various investment products available in the market and select those that would give the best possible returns to the fund and its shareholders.

Most of the firms dealing in mutual funds are either affiliates of foreign entities which have stringent AML policies used within the conglomerate or bank affiliates subject to bank regulation and audit. Vulnerability to AML/CFT is mitigated by appropriate AML controls from strict customer acceptance to monitoring of transactions and regular training for their personnel. They are also subjected to regular AML audit by the SEC. The vulnerability of mutual fund is **MEDIUM.** 

# Factors considered affecting product vulnerability

Indicators Equities Trading		Investment House	Mutual Fund	
Volume and value of	High	Medium	Medium	
transactions	півіі	Medium	Medium	
Profile of customer	Medium	Low	Low	
using the product	Medium	LOW	Low	
Existence of adequate	Medium	Medium	Medium	
AML/CFT controls	ivieulum	iviedium	iviedium	

# **ACTION PLAN**

Considering the general variables and the identified gaps and deficiencies, the following are the recommended action plans.

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Propose amendments to SEC Memorandum Circular No. 2, Series of 2010 to reflect the changes in the AMLA, as amended and its 2016 RIRR, such as:  i. The requirement for covered persons supervised and regulated by the SEC to register with the AMLC within ten (10) working days from receipt of its certificate of registration with the SEC;  ii. Guidelines on customer identification for onboarding of clients without face-to-face and customer identification reliance on third party or intermediary;  iii. Requirement for covered persons to profile their customers into low, medium or high risk and tiered customer due diligence for each classification;  iv. Adoption of a mechanism by covered persons on freezing of securities and complying with inquiry orders.	SEC	AMLC	Ongoing
Coordinate with the AMLC on the following matters:  i. implementation of sanctions for violations of the AMLA and its RIRR;  ii. drafting of a Uniform Rules on Administrative Sanctions  iii. providing trainings for SEC, CMIC other SROs, and covered persons  iv. checking of covered persons if registered with the SEC and AMLC	SEC	AMLC	2 <sup>nd</sup> Semester, 2017
Creation of a new unit/division within the EIPD focused on the following:	SEC	AMLC, CMIC, PDEX	Ongoing 2017 – 2018

i.	check compliance with AML/CFT rules and		
	regulations;		
ii.	develop working arrangements with CMIC,		
	AMLC and other SROs;		
iii.	monitor if market intermediaries submit CTRs		
	and STRs and if monitoring systems are in		
	place		
iv.	create a TWG for the drafting of Uniform Audit		
	Program Guide and Code of Ethics; AND		
٧.	provide regular trainings for both SEC staff and		
	market intermediaries;		

#### V. INSURANCE SECTOR VULNERABILITY

#### **INTRODUCTION**

The Insurance Sector is composed of all the Covered Persons (CPs) under the jurisdiction of the Insurance Commission (IC). It is comprised of different industries, namely: Insurance Industry, Pre-Need Industry and the Health Maintenance Organizations Industry. As of October 2017, a total of one hundred ninety-eight (198) companies are licensed to conduct insurance business in the country. The profile of the Insurance Sector is as follows:

#### **INSURANCE INDUSTRY (196)** PRE-НМО **TOTAL NON-LIFE** MUTUAL INSURANCE COMPOSITE PROFESSIONAL **SERVICING NEED** NO. OF **BENEFIT BROKERS** REINSURANCE INSURANCE OR CPs **GENERAL** ASSOCIATION **COMPANY** 27 62 4 16 28 242 60 35 1 9

**2017 Insurance Sector Profile** 

Life insurance companies are licensed to write life policies providing protection against financial loss that would result from the premature death of an insured. The named beneficiary therein receives the proceeds and is thereby safeguarded from the financial impact of the death of the insured. Non-life insurers, on the other hand, are licensed to write non-life policies such as fire, casualty, and marine insurance. Composite insurers write both life and non-life insurance policies. Mutual Benefit Associations (MBAs) are licensed to write accident and life insurance for its members. Insurance Brokers sells, solicits, or negotiates insurance for compensation. Professional Reinsurance are companies that provide financial protection to insurance companies. Reinsurers handle risk that are too large for insurance companies to handle on their own.

### A "Servicing Insurance Company" 133 may either be:

- 1. A domestic insurance company which is (a) in a state of "run off"; (b) "running-off" towards closure; (c) expressly allowed by the Insurance Commission to "run-off"; or (d) a distressed company expressly prohibited by the Insurance Commission to sell policies, whose business transactions are confined to:
  - (i) accepting periodic premium payments from its policyholders, or
  - (ii) granting policy loans and paying cash surrender values of outstanding policies to its policyholders, or
  - (iii) reviving lapsed policies of its policyholders, and
  - (iv) such other related services. Activities
- A foreign life insurance company that withdraws from the Philippines whose business transactions are confined to accepting periodic premium payments from, or granting policy loans and paying cash surrender values of outstanding policies to, or reviving lapsed policies of, Philippine policyholders, and such other related services.

-

<sup>133</sup> Circular Letter No: 2014-14

**Pre** - **Need** companies are corporations registered with the Insurance Commission authorized/licensed to sell or offer pre-need plans<sup>134</sup>. **Health Maintenance Organizations** are juridical entities legally organized to provide or arrange for the provision of a pre-agreed or designated health care services to its enrolled members for a fixed pre-paid fee for a specified period of time<sup>135</sup>.

The insurance sector is smaller than the banking sector in terms of asset. Total assets of bank sector amounted to P12,085.7 billion<sup>136</sup> compared to the total assets of the Insurance Sector P1,291.6 billion<sup>137</sup> for the comparative year 2015.

During the previous NRA, it was concluded that the areas of prioritization in order to deter ML risks in the insurance sector are the Quality of AML/CFT Supervision and Staff Knowledge. As such, the action plan included the improvement of dissemination of AML/CFT laws and regulations implemented the IC each company's AML compliance officers and alternate compliance officers, and the resort to the use of electronic mail for such dissemination. Another action plan was the inclusion of AML/CFT typology trainings in the annual training plan and design special training programs for examiners and coordination with the AMLC Secretariat for their program offerings.

It was recognized that there is significant room for improvement when it comes to the registration with the AMLC, monitoring of covered persons and/or their respective officers and employees with other AML/CFT requirements and the need to issue and implement stringent penalties and sanctions for violation of AML/CFT Rules and Regulations.

Since the last NRA Report was issued, the Insurance Commission exerted efforts to improve its regulatory functions and come up with measures, such as issuance and implementation of new regulations, through circular letters which aimed to address the identified weaknesses and deficiencies in the priority variable of the Insurance Sector and to further ensure the prevention of money laundering incidents in the Insurance Sector.

More importantly, the monitoring of insurance companies, pre-need companies and MBA's have become more effective and implementation of regulations more secured. Among such efforts include the creation of the AML Division and issuance of IC AML circulars.

This report shall reflect and focus on the developments in the insurance sector since the implementation of various action plans that were formulated during the last NRA Report.

In the First NRA Report covering the period 2011-2014, the vulnerability of the Insurance Sector to ML Risks was rated **Medium-Low**. In the present NRA, the rating of the vulnerability of the Insurance Sector to ML Risks is **MEDIUM**.

### a. Covered Persons Under the Insurance Commission Supervision

All insurance institutions/entities in the Philippines, such as insurance companies whether life, non-life insurance companies or composite (both engaged in life and non-life insurance business), mutual benefit associations, pre-need companies, insurance agents (natural persons), insurance brokers, professional reinsurers, reinsurance brokers, holding companies, trust for charitable uses, Health Maintenance Organizations (HMOs) and all other persons and entities supervised and/or regulated by

<sup>&</sup>lt;sup>134</sup> R.A. 9829 or the Pre-Need Code of the Philippines

<sup>&</sup>lt;sup>135</sup> DOH Administrative Order No. 34 (s. 1994)

<sup>&</sup>lt;sup>136</sup> http://www.bsp.gov.ph/downloads/Publications/2015/StatRep\_2Sem2015b.pdf

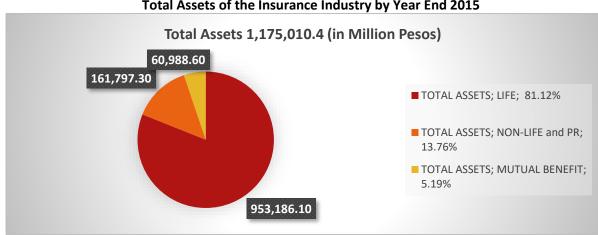
<sup>&</sup>lt;sup>137</sup> Asset of Life Insurance companies + assets of Non-Life Insurance companies + assets of MBAs + assets of Pre-Need companies= Total Assets of the Insurance Sector

the Insurance Commission (IC) are considered covered persons subject to AML/CFT preventive measures under the Anti-Money Laundering Act (AMLA), as Amended.

### b. Insurance Industry Profile

The Insurance Industry's performance continues to thrive. At the end of 2015, the insurance Industry has a combined asset of PhP1.175 trillion<sup>138</sup>, which is 9.91% higher than the PhP1.059 trillion in 2014.

Based on the 2015 figures, life insurance companies operating in the Philippines have assets in the total amount of PhP 953,186.1 million, which constitutes 81.12% of the Insurance Sector. Life insurers sell a number of products such as whole life insurance, term insurance and investment-linked products. On the other hand, the non-life insurance and professional reinsurance companies had a total asset of PhP 161,797.3 million, which constitutes 13.77% of the Insurance Sector as of the end of 2015. MBAs also contributed PhP 60,988.6 million in assets constituting 5.19% of the total Insurance Sector.



Total Assets of the Insurance Industry by Year End 2015

Various indicators are used to measure the performance of the insurance industry. This performance is measured in terms of premium volume, insurance consumption, and market penetration rate.

In 2015, the life companies generated PhP 188,818.2 million in premium income, an 18.96% increase compared to PhP 158,727.2 million premium production in 2014. This was primarily brought about by the 28.93% increase in the premiums produced by variable life products, from PhP 107,564.2 million in 2014 to PhP 138,687.9 million in 2015, and 12.09% increment in the traditional group life products, from PhP10,296.4 million in 2014 to PhP11,541.4 million in 2015.

For Non-Life Insurance companies, total net premiums written, likewise, rose by 14.06%, from PhP32,058.8 million in 2014 to PhP36,565.7 million this year. This was due to the 21.46%, 16.78% and 12.19% increases in casualty, fire and motor car businesses, respectively, which constituted 86.8% of the total net premiums written.

As for Mutual Benefit Associations, premium rose from PhP6,437.9 million to PhP6,877.3 million for a 6.83% increase.

<sup>&</sup>lt;sup>138</sup> Combined assets of Life Insurance, Non-Life Insurance and Professional Reinsurance, and Mutual Benefit Associations.

The total premium volume or production of the insurance industry reached PhP232,261.2 million, which translates to a 17.77% increase compared from PhP197,223.9 million in 2014.

For year 2015, insurance and reinsurance brokers contributed ₱53.27 billion direct premiums to the insurance industry, 9.75% higher than the ₱48.54 billion contribution the previous year. The insurance brokers accounted for 95.41% of the total premiums while the reinsurance brokers shared the remaining 4.59%.

The increase in the premium production can be attributed to the 36.57% 28.78%, 24.60% and 12.21% boost in health, life, engineering and fire business, respectively, which constituted 75.92% of the total premiums produced.

As in the prior years, fire insurance business had the biggest share contributing 28.37% of the total premiums, followed by health with 24.60%, life with 16.39%, motor vehicle with 8.94% and other lines of business accounting for the remaining 21.70%.

Brokers' Business Operations, 2015 (PhP millions)				
Line of Business	Insurance Brokers		Reinsurance Brokers	
Lille Of Busilless	Premiums	Commission	Premiums	Commission
Life	8,729.54	1,832.76	0	0
Fire	14,047.70	1,097.12	1,061.85	63.80
Ocean Marine	777.69	131.47	80.04	1.64
Inland Marine	326.44	64.71	8.39	0.54
Marine Hull	1,055.66	78.48	187.63	18.53
Aviation	1,324.35	46.72	23.58	2.26
Fidelity and Surety	1,129.75	267.78	5.23	0.51
Motor Vehicle	4,736.46	1,116.54	24.64	1.72
Health	13,104.22	1,254.71	0	0
Accident	650.42	155.72	253.04	15.72
Engineering	2,966.74	237.15	526.45	48.02
Miscellaneous	1,972.54	399.04	274.72	33.28
Total	50,821.51	6,682.20	2,445.57	186.02

As a result of the increased premium production, the commissions earned by the brokers likewise improved by 24.40% from ₱5.52 billion last year to ₱6.87 billion this year.

The growth of the insurance industry is also noted based on the substantial increase of the Insurance Penetration Rate (IPR) and Market Penetration Rate (MPR). Penetration rate indicates the level of development of insurance sector in a country, it is measured as the ration of premium underwritten in a particular year to the GDP<sup>139</sup>. Market penetration is a measure of the amount of sales or adoption of a product or service compared to the total theoretical market for that product or service. Additionally, it can also include the activities that are used to increase the share of a particular product or service. <sup>140</sup> In 2015, the IPR, which defines the contribution of the entire insurance sector to the GDP of the country, grew to 1.75% compared to the 1.56% in 2014 or a 12.18% increase. On the other

<sup>&</sup>lt;sup>139</sup> http://economictimes.indiatimes.com/definition/penetration-rate

<sup>&</sup>lt;sup>140</sup> http://www.investopedia.com/terms/m/market-penetration.asp

hand, the MPR or the percentage of insured lives compared to the total population has increased to 41.27% in 2015 from 37.39% in 2014 or a 10.38% increase.

With its robust performance, the insurance sector plays a significant role in the financial market. Whence, constantly reviewing the rules and regulations of the Insurance Commission to further develop and strengthen the enforcement of law to prevent money laundering (ML) and financing of terrorism (FT) is imperative.

# c. Pre-Need Industry Profile

Pre-need companies are corporation registered with the IC that are authorized/licensed to sell or offer to sell pre-need plans. It also refers to schools, memorial chapels, banks, nonbank financial institutions and other entities which have also been authorized/licensed to sell or offer to sell pre-need plans insofar as their pre-need activities or business are concerned.

The total reported assets of seventeen (17) pre-need companies rose to PhP 115.61 billion in 2015, up by 8.05% from PhP107.00 billion in 2014. Moreover, investments in Trust Fund which accounted for 85.22% of the total assets grew by 3.75% year-on year from PhP 94.96 billion to PhP 98.52 billion.

Total liabilities of the industry went up to PhP 99.25 billion, up by 12.13% from the prior year's PhP 88.51 billion. This was attributed to the 10.59% growth in Pre-Need Reserves which comprised 93.74% of the total liabilities.

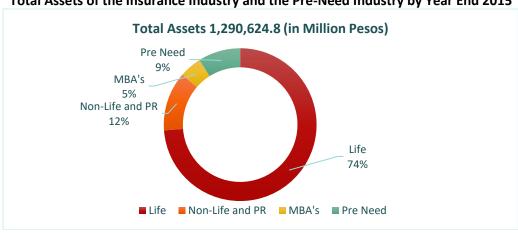
The industry's net worth dropped by 11.52% from PhP18.49 billion to PhP16.36 billion. The drop was due to the 38.85% decrease in Retained Earnings on Trust Fund, from PhP19.82 billion to PhP12.12 billion.

On the other hand, the total investments of the pre-need industry were valued at PhP103.87 billion, an 8.05% increase from the prior year's PhP96.11 billion. The increase was attributed to the 75.29%, 20.39% and 11.99% improvement in real estate, bonds and stocks, respectively, which comprised 82.90% of the investments.

Although premium production expanded by 22.42%, from PhP13.29 billion in 2011 to PhP16.27 billion in 2015, the net income contracted by 27.00%, from PhP2.00 billion to PhP1.46 billion. This was brought about by the 152.81% increase in taxes.

The pre-need companies sold a total of 694,159 plans, some 2.97% higher than that of the prior year, mainly due to the 3.26% increase in memorial life business.

While the condition and performance of the pre-need industry require an overall improvement, effective and responsive regulation and supervision are exercised to protect the industry from risks against money laundering and financing of terrorism.



### Total Assets of the Insurance Industry and the Pre-Need Industry by Year End 2015

### d. Health Maintenance Organizations

Executive Order (E.O.) No.192, Series of 2015, transferred jurisdiction over HMOs from the Department of Health (DOH) to the IC in order to regulate and supervise the establishment, operations and financial activities of HMOs. E.O. No. 192 took effect on December 2015.

As of 29 June 2017, there are twenty-five (25) HMOs with Certificate of Authority issued by the Insurance Commission for license year 2017-2018 although there are 28 HMOs recognized by the Commission, the difference being the Certificate of Authority issued by its former regulator, the Department of Health.

However, HMOs are not included in this National Risk Assessment.

### DATA AND INFORMATION COLLECTION

Data were gathered through the conduct of a survey. Survey forms were distributed by the Insurance Commission to its supervised entities. Also, industry associations were notified of the same to help the Commission to distribute the survey forms to their respective member-companies. From the total number of companies that were surveyed, the following are the percentages of respondents from each of the sector:

Table 5-1. Response Rate on Survey

	2017 survey
Life Insurance Companies	93.55%
Non-Life Insurance companies	82.54%
Pre-Need companies	87.5%
Mutual Benefit Assoc. Inc. (MBAI)	80%
Brokers	65.63%

The General Input Variables section of the assessment tool are mainly based on the existing AML law, implementing rules and regulations, relevant IC circular letter, survey, IC Annual Report and IC Key Statistical Data. Similarly, the IC Annual Report 2015 and Key Statistical Data for 2013 to 2015 were mainly used in the assessment of the Input Variables for Selected Specific Products, particularly on the volume and average transaction size of each product. Rather than analyzing the products per industry, the group looked at all of the products entirely as belonging to one insurance sector.

The survey conducted covered only the periods 2013 to 2016. As regards the annual report of covered persons/entities, the data is limited up to year 2015 because the submission of the 2016 Annual Report was due on the last day of May 2017. Verification of such report is pending as of the making of this assessment. The Insurance Sector Working Group conducted quantitative assessment based on the data available from the IC and the survey.

The World Bank has provided an updated risk assessment tool that was used in this NRA. The updated module is an improved version of the previous module used in the 2011-2014 NRA. In the present module, variable on Commitment to Corporate Governance was replaced by Availability and Effectiveness of Entry Controls in the list of General AML Control Variables. The new variable assesses the availability and effectiveness of entry controls including licensing, registration or other forms of authorizations to operate.

### Quality of AML General Controls of the Insurance Sector and the Pre-Need Sector

For this section, the ratings given were assessed and determined by the members of the National Risk Assessment Insurance Sector Sub Working Group basing their evaluation mainly on the answers provided by the covered entities in the surveys, ratings given in the first NRA and using the National Risk Assessment Tool Guidance Manual as their guide. However, due to limited time and manpower, the answers provided by the covered entities in the surveys were not subjected to further probing.

Each of the industry's rating (insurance, pre-need and MBA) was given corresponding weights according to the premiums collected per industry cluster (life insurance, non-life insurance, MBAs and pre-need). The premiums collected from each industry cluster were used as a gauge to determine the weight of contribution of each industry vis-à-vis the entire insurance sector. This approach allows fair exposure of each industry cluster from the insurance and pre-need industry in determining the insurance sector's overall vulnerability.

The industry weight of each industry cluster based on the premium production for 2015 are as follows:

Industry Cluster	Premiums (in Millions)	Industry weight
Life	188,818.2	75.97%
Non-Life	36,565.7	14.71%
Pre-need	16,269.2	6.55%
MBA's	6,877.3	2.77%
Total	248,530.4	100%

**Table 5-2. Premium Production for 2015** 

The Life Industry cluster contributes to nearly 76% of the total premium production of the Insurance Sector. This is three fourths (3/4) of the total premium produced, a major portion of the entire sector. The Non-Life Industry Cluster is second with 14.71% contributing a significant share in the premium production. Pre-need's and MBA's Industry cluster come third (3<sup>rd</sup>) and fourth (4<sup>th</sup>) with 6.55% and 2.77%, respectively.

### **Legal Framework**

The AMLC and IC are tasked by law to monitor the compliance of Insurance Companies to the requirements set forth by the Anti-Money Laundering Act (AMLA), as amended and other Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations issued. The IC is also the

competent authority responsible for prudential or market supervisions as regard to activities of any persons (legal or personal) or entities engaged in the insurance business or offering insurance products.

The IC issues guidelines, through circular letters, to ensure compliance of insurance companies and other covered entities to the AML/CFT requirements provided by the AMLA, as amended. The rules aim to deter ML and TF consistent with the Financial Action Task Force (FATF) recommendations. These AML/CFT rules and regulations are likewise in compliance with the Insurance Core Principle (ICP) No. 22 issued by the International Association of Insurance Supervisors (IAIS), which requires the insurers and intermediaries to take effective AML/CFT measures.

These issuances aim to achieve the following specific objectives:

- 1. To ensure compliance with the AMLA, as amended and the Terrorist Financing and Suppression Act of 2012;
- 2. To protect the reputation of insurance companies and other regulated entities;
- 3. To maintain the integrity of the insurance companies from being used as vehicles for money laundering and terrorist financing activities;
- 4. To assess the effectiveness and adequacy of the entities AML/CFT programs; and
- 5. To ensure that they perform their duties of vigilance in accordance with the guidelines set by the IAIS on matters related to AML/CFT.

In addition, the Insurance Code, as amended, provides powers to the Insurance Commissioner to impose penalties for violations of rules and regulations, such as on AML enforcement. Further, the insurance regulator, as a member of the International Association of Insurance Supervisors (IAIS), adheres to the Insurance Core Principle (ICP) on AML/CTF.

Pursuant to the AMLA, as amended, its implementing rules and regulation, AMLC resolutions, and relevant IC AML/ CFT Circular Letters, covered persons under the supervision of the IC are required to comply with the following:

- 1. Formulation and updating of Anti-Money Laundering Operating Manual containing effective policies, procedures, and internal control to combat money laundering and financing of terrorism;
- 2. Know Your Customer (KYC) or Customer Due Diligence (CDD) requirements;
- 3. Record-Keeping requirements for at least 5 years;
- 4. Covered transaction report and suspicious transaction report submission;
- 5. Designation of AML Compliance Officer and Alternate Compliance Officer;
- 6. Other reportorial requirements;
- 7. Internal Control and Procedure aimed at preventing and impending money laundering including audit function or procedure to test the system to ensure compliance with the program;
- 8. Providing training for responsible officers and personnel or staff;
- 9. Registration with the AMLC

# SECTOR VULNERABILITY ASSESSMENT

The overall vulnerability of the insurance sector to ML/TF risk is **MEDIUM**. The vulnerability of the insurance sector is dependent on the strength of the AML general controls and product specific variables.

Based on the assessment of the sector, the input variable **AML Knowledge of Staff in Insurance Companies** should be given priority by the sector. The pre-need survey respondents admitted that AML trainings were given mainly to their compliance officer. Nevertheless, these trainings were echoed to their employees.

Another priority variable is **Effectiveness of Supervision Procedures and Practices.** In the latter part of year 2015, the Insurance Commission created the Anti-Money Laundering Division, which is a dedicated unit for AML supervision of its covered persons. By start of 2017, the AMLD began its risk-based and supervisory on-site examination of covered persons. To date, there is still no consolidated AML rules and regulations dedicated specifically to determine compliance to the AML requirements.

Quality of AML Supervision	Effectiveness of Supervision/ Procedures and Practices	Medium High
(Medium)	Availability and Enforcement of Administrative Sanctions	Medium

The quality of AML Supervision of the Supervisory Authority is an interplay of supervision/oversight activities and administrative sanctions.

# **Effectiveness of Supervision/Procedures and Practices**

The Insurance Commission, as the supervisory authority ensures that regulated entities are compliant with AML/CFT regulations by performing its supervisory functions with diligence. The industry stakeholders also believe that the regulator exercises prudence and judiciousness in the performance of their supervisory functions. In 2016, the IC was conferred the ISO 9001:2008 Certification to the Insurance Commission after a thorough assessment of IC's Quality Management System.

As provided in Section 253 of the Insurance Code, as amended, the Commissioner shall, at least once a year and whenever he considers the public interest so demands, cause an examination to be made into the affairs, financial condition and methods of business of every insurance company. Covered persons are subject to a mandatory annual examination in which, AML examination is incorporated on a risk-based approach. AML examination is focused primarily on high risk value life insurance products with high investment level. Further, under Rule XIX of the 2016 Revised Rules and Regulations (RIRR) of Republic Act No. 9160, as Amended, the IC is authorized to assist the AMLC in checking the compliance of IC covered persons on the requirement of the AMLA, its RIRR and AMLC issuances.

In 2015, the AML Division of the IC was established, which is primarily tasked to ensure compliance by IC covered persons with the requirements under the AMLA, as amended, its RIRR, all AMLC issuances and related IC Circular Letters. By the start of 2017, the Anti-Money Laundering Division (AMLD) has started its comprehensive and risk-based AML/CFT examination procedure. The result of the examination will be the basis in updating the IC's supervisory on-site examination of covered persons to determine whether such covered persons are compliant with pertinent AML/CTF rules and regulations. The challenge, however is that the AML Division has only 6 plantilla positions, of which, only 4 positions are filled-up.

The AMLC and the IC also has an existing Memorandum of Agreement (MOA) for the effective coordination and information exchange to effectively prevent, control, detect and investigate unlawful activities under Section 3(I) of the AMLA, as amended, or any violation of laws that the IC is

tasked to implement, which would give rise to the commission of any unlawful activity under Section 3(I) of the AMLA, and money laundering activities arising therefrom.

### **Availability and Enforcement of Administrative Sanctions**

Concomitant with its power to supervise insurance companies, is the power to impose administrative sanctions. Both the IC and the AMLC have authority to impose administrative sanctions on IC-supervised covered persons.

Sec. 437 of the Insurance Code, as amended, provides the Insurance Commissioner with administrative power to fix and assess fees, charges and penalties as the Commissioner may find reasonable in the exercise of regulation. In addition, Sec. 438 of the law provides that the Insurance Commissioner, at his discretion, may impose sanctions for any willful failure or refusal to comply with, or violation of any provision of the Insurance Code, or any order, instruction, regulation, or ruling of the Insurance Commissioner; commission of irregularities; or conducting business in an unsafe or unsound manner as may be determined by the Insurance Commissioner.

In 2015, the IC AML Division issued circular letters providing penalty for non-compliance with the requirement on designation of AML Compliance and Alternate Compliance Officers. Several covered entities were sanctioned by the Commission due to non-compliance therein. Below are the number of companies sanctioned by IC for period 2015-2017 for failure to timely furnish/submit the names and contact details of AML compliance and alternate compliance officers:

Table 5-3. Number of Companies that were Sanctioned

Year	Number of Sanctioned Company
2015	6
2016	9
2017	14

The figures above which indicate an upward trend on the number of sanctioned companies under the supervision of the IC would show that the regulator is becoming more focused on enforcement of AML/CFT rules and regulations through the dedicated division it created in 2015 to specifically monitor compliance with AML/CFT rules and regulations

The AMLC, in its Resolution No. 24 dated 24 May 2017, approved the Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as Amended, which provides for rules of procedure that will govern the adjudication of administrative cases and sanctions for violations of the AML, as amended, its RIRR and all AMLC issuances.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of Insurance	Quality of AML Supervision (Intermediate Variable)	Medium
Company's Management ( Medium High)	Availability and Enforcement of Criminal Sanctions	Medium High
	Level of Market Pressure to Meet AML Standards	High

Commitment of leadership to address ML risks is influenced by entry controls, AML supervision and criminal sanctions.

### **Availability and Effectiveness of Entry Controls**

The Insurance Commission, the regulator, supervisory authority and the licensing body for insurance companies, pre-need companies, mutual benefit associations, insurance brokers and insurance agents has entry controls that are clearly identified within the laws and regulations. Among the factors considered by the IC in licensing insurance companies are the direction and administration, as well as the integrity and responsibility of the organizers and administrations, the financial organization and the amount of capital, which reasonably assure the safety of the interests of the policyholders and the public.

For pre-need companies, yearly renewal of license is also imposed. It may be renewed provided that, (i) it has no solvency and trust fund deficiencies; (ii) it has no paid-up capital impairment; and (iii) is continuing to comply with the provisions of the pre-need code, and the circulars, instructions, rules and regulations of the commission. <sup>141</sup>

For insurance brokers,<sup>142</sup> the application of a broker which is a partnership or corporation must be accompanied by the application and requirements of a soliciting official. In order to be issued a license, the brokerage company must have a qualified and approved soliciting official.

The IC also conducts Agent's Computerized Examinations for individuals who wish to acquire license to be able to engage in the selling of insurance policy contracts of insurance companies to the public. Applicant may apply for examination for non-life, life, variable, and health and accident, and Compulsory Third Party Liability (CTPL) only. The applicants who pass the tedious examinations, AML question included, are called insurance agents and are required to undergo AML related seminars and trainings.

### **Availability and Enforcement of Criminal Sanctions**

In case of non-compliance with AML laws and regulations, the AMLA, as amended, provide appropriate criminal penalties in case. The penalties are sufficient to deter or mitigate breach of AML regulations. Person in the insurance industry regard the criminal sanctions regime as sufficiently dissuasive to positively influence individual behavior problem.

### **Level of Market Pressure to Meet AML Standards**

The life and non-life products are generally available in the Philippine jurisdiction. Reinsurance transactions, marine hull and marine cargo insurance mainly involve cross border transactions since these are big risks that cannot be covered by Philippine insurance companies. The pre-need and MBA sectors, which are significantly smaller than the life and non-life sectors, maintained that their clientele are only from the domestic market. Hence, the pressure to comply with AML standard comes mainly from the regulators and mother company of domestic IC regulated entity, and not from the market. The Philippine insurance industry, however, is actively participating in the ASEAN integration and cross border transactions with other ASEAN Member states will likely be probable in the future.

<sup>&</sup>lt;sup>141</sup> Under Section 10 of Implementing Rules and Regulations of Republic Act No. 9829, otherwise known as "Pre-Need Code of the Philippines"

<sup>&</sup>lt;sup>142</sup> An insurance broker refers to any person who for any compensation, commission or other thing of value acts or aids in any manner in soliciting, negotiating or procuring the making of any insurance, on behalf of an insured other than himself. A reinsurance broker is one who, for compensation, acts or aids in any manner in negotiating contracts of reinsurance, or placing risks of effecting reinsurance, for any reinsurance company in the Philippines.

Quality of Internal AML Policies and Procedures (Medium High)	Comprehensiveness of AML Legal Framework	High
	Commitment and Leadership of Managements (Intermediate Variable)	Medium High
	Effectiveness of Compliance Function (Organization)	Medium

# **Comprehensiveness of AML Legal Framework**

The Insurance Commission, pursuant to its powers under the Insurance Code, as amended, has also issued its own several AML/CFT circular letters to further strengthen and combat money laundering and terrorist financing risk. For period 2013-2017, the IC issued the following AML related Circular Letters which address ML and TF risks:

**Table 5-4. IC Issuances on AML-Related Matters** 

Circular Letter No.	Date	Description/Subject Matter
1. 2017-22	07 April 2017	Filing of 2016 Annual Statement- MBAs- This Circular requires MBAs to submit completely accomplished <b>ANTI-MONEY LAUNDERING COMPLIANCE FORM.</b>
2. 2017-21	07 April 2017	Filing of 2016 Annual Statement- Life Insurance Companies- This Circular requires life insurance companies to submit completely accomplished <b>ANTI-MONEY LAUNDERING COMPLIANCE FORM.</b>
3. 2017-10	14 February 2017	Supplement to CL No. 2015-05 dated 05 February 2015, as Amended by CL No. 2015-13 dated 25 March 2015 on the <b>Submission of the Names and Contact Details of AMLA Compliance Officer and Alternate Compliance Officer</b> , Providing for a Cap on the Penalties that may be Imposed
4. 2016-56	19 September 2016	Submission of the Names and Contact Details of Anti-Money Laundering Compliance Officer and Alternate Compliance Officer by Health Maintenance Organizations
5. 2016-42	29 July 2016	Guidelines on Approval of Requests for Lectures, Resource Persons, and Facilitators from the Insurance Commission – This Circular provides guidelines on how to request the IC for AML/CFT lecturers.
6. 2016-41	29 July 2016	Minimum Capitalization and Financial Capacity Requirements for HMOs  - This circular includes IC AML rule on cash infusion.
7. 2015-13	25 March 2015	Amendments to Circular Letter No.2015-05 dated 05 February 2015 on the Submission of the Names and Contact Details of AMLA Compliance Officer and Alternate Compliance Officer
8. 2015-05	5 February 2015	Submission of the Names and Contact Details of AMLA Compliance Officer and Alternate Compliance Officer
9. 2014-51	12 December 2014	Monitoring of "Pigeon Holes" at the premises of the Insurance Commission –This circular was issued to address the issue on dissemination of newly issued CLs and correspondences.
10. 2014-38	11 September 2014	Application of Enhanced Due Diligence Relative to Jurisdictions Identified in the Financial Action Task Force (FATF) Public Statement dated 27 June 2014 and Taking into Account the Information Relative to the Jurisdiction Mentioned in FATF's Compliance Document also dated 27 June 2014
11. 2014-33	14 July 2014	Anti-Money Laundering Council (AMLC) National Risks Assessment (NRA) Project Data/Information Collection Requirement

12. 2013-33	04 November	Adoption and Implementation of the 2013 Market Conduct Guidelines
	2013	– This Circular include agent's AML responsibilities such as reporting and
		attendance to AML training provided by companies

The Insurance Commission also issues circulars disseminating rules, regulations and policies issued by the AMLC to IC-supervised covered persons. Among AMLC issuances disseminated by the IC are the 2016 Revised Implementing Rules and Regulations, <sup>143</sup> AMLC resolutions, <sup>144</sup> and reports from financial intelligence units of other jurisdictions. <sup>145</sup> With the creation of the AMLD, it is expected that the IC will issue more AML/CFT policies. Among the responsibility of the AMLD is the updating and/or formulating of IC AML/CFT rules and regulation and IC risk-based examination procedure. Although there are specific AML/CFT rules and regulation applicable to IC covered persons, there is a need to consolidate and/or update the same.

These laws, regulations and IC Circulars are usually disseminated by the regulator to the industry associations and to the companies through their respective AML Compliance and Alternate Compliance Officers' email addresses. In addition, the issuances are likewise posted on the regulator's website as well as on the Office of the National Administrative Register (ONAR) of the University of the Philippines College of Law. Also, pursuant to Circular Letter No. 2014-51 dated 12 December 2014, the newly issued IC AML CLs are disseminated through the companies' respective pigeon holes in the IC premises.

To ensure implementation of AML/CFT laws, regulations and issuances, management of companies should be committed in addressing ML/TF risks and companies should possess effective internal AML compliance functions. Commitment of management has been assessed as Medium High with the strict entry controls imposed for the private sector.

### **Effectiveness of Compliance Function (Organization)**

With respect to internal compliance function, majority of the insurance companies have internal control programs that are commensurate to the level of risk, taking into account factors such as the volume and nature of products provided, the client base profile, and the cross-border nature of transaction. Also, majority of the insurance companies have appointed a well-resourced and independent AML compliance officer at a senior management level pursuant to CL No. 2015-05, as amended.

	Availability and Enforcement of Criminal Sanctions	Medium High
Compliance of Insurance Company's	Effectiveness of Compliance Function (Organization)	Medium
Staff (Medium)	AML Knowledge of Staff in Insurance Companies	Medium
	Integrity of Staff in Insurance Companies	Medium High

<sup>&</sup>lt;sup>143</sup> IC Circular No. 2017-07, 31 January 2017

<sup>144</sup> IC Circular No. 2016-49, 1 September 2016 (on AMLC Reso. No. 69, 17 August 2017); IC Circular No. 2016-43, 8 August 2016 (on AMLC Resolution No. 61, 20 July 2016); IC Circular No. 2016-36, 7 July 2016 (on AMLC Reso No. 48, 15 June 2016); IC Circular No. 2016-13, 10 March 2016 (on AMLC Reso No. 5, series of 2016); IC Circular No. 2015-17, 31 March 2015 (on AMLC Reso. TF-03, 10 December 2014).

\_

<sup>&</sup>lt;sup>145</sup> IC Circular No. 2015-18;

Compliance of staff can be influenced by availability and enforcement of criminal sanctions, effectiveness of an internal control programs which is able to check compliance of staff, and the knowledge and integrity of the staff.

### **Availability and Enforcement of Criminal Sanctions**

Criminal sanctions for AML/CFT violations are available and dissuasive, although no insurance company staff has been convicted of money laundering. Internal compliance function is assessed as Medium with majority of the companies having an internal control program.

# AML Knowledge of Staff in Insurance Companies

AML Knowledge of Staff in Insurance Companies has been identified as a priority variable, with employees of the pre-need industry focusing only on training of compliance officers only. The rest of the industry is generally knowledgeable in AML regulations. This signifies that they are most likely compliant in providing AML training programs to their officers and personnel. Insurance companies have provided sufficient AML trainings to its officers and personnel. Hence, they are aware of AML compliance and reporting procedures, and obligations and the legal consequences of AML compliance breaches.

AML related trainings/seminars are being conducted by AMLC and the IC. Interested covered person who wish to undergo such seminars or trainings must reach out to AMLC and IC for the scheduling of their seminar or training. For period of 2017 – 2016, the IC conducted six (6) Governance and AMLA Workshops.

#### Integrity of Staff in Insurance Companies

The industry players have also established their own Code of Conduct to ensure the integrity of their employees and agents. Most covered entities reported that a background check is performed prior to hiring or prior to membership to an association. Screenings are also conducted for the hiring of insurance agents. Insurance agents have to renew their licenses every three (3) years, thereby allowing IC and the insurance companies to monitor the performance and quality of the agents.

The NRA survey revealed that there were incidences of theft or fraud. Answers provided by covered persons to the survey revealed that three (3) out of twenty (25) life insurance respondents, reported a breach of integrity from their employees with only minimal infractions. For non-life companies, six (6) out of the total fifty-one (51) respondents reported a breach with only minimal infractions. For Pre-Need Companies, only one (1) out of thirteen (13) respondents reported a breach with only minimal infractions. For Mutual Benefits Association, only two (2) out of twenty-eight respondents (28) reported a breach with minimal infractions. For Insurance Brokers, four (4) out of forty respondents (40) reported a breach with minimal infractions.

Majority of the response from the covered entities indicate that these entities and person themselves have meted administrative sanctions on erring employees. Administrative sanctions that may be imposed are reprimand, written warning, suspension or termination. It is imperative that companies, as well as the regulator, adopt mechanisms that will encourage reporting of suspicious transactions and at the same time, protect the reporting person/entity.

Quality of CDD Framework (Medium High)	Availability and Access to Beneficial Ownership information	High
	Availability of Reliable Identification Infrastructure	Medium High
	Availability of Independent Information Sources	Medium

The quality of a sector's CDD framework will depend on whether beneficial ownership information is available and accessible, customers can be identified based on a reliable ID system and covered persons are able to verify transaction history of their customers.

### Availability and Access to Beneficial Ownership information

The IC Circular Letter No. 32-2006 provided systems and programs, which includes identification of the "Beneficial Owners" in contracts and policies issued by covered persons. A systematic and appropriate recording of PEPs and beneficial owners/ultimate collectors is also implemented in the Insurance Sector. As a matter of fact, some big foreign players in the sector have complied with these recording requirements even before local laws were passed because they had to comply with foreign laws such as Bill C-25 (Canadian Law) and, The Foreign Account Tax Compliance Act (FATCA).

As compared to other sectors, beneficial ownership information is easier to establish in the insurance sector. the nature of insurance product itself requires the insurers to identify who the beneficial owners are for every policy. It also follows the unique concept of insurable interest where the owner must prove that he has an insurable interest over the insured before said application to purchase may be approved. In like manner, the benefits for the policy holders or owners of insurance products are separate from the benefits given to the beneficiaries. Hence, if the named beneficiary or ultimate owner cannot be identified, then the benefits will not be released to him/her.

# <u>Availability of Reliable Identification Infrastructure</u>

With respect to identifying customers and beneficiaries, the absence of a reliable national ID system is a blockage for a more efficient and more effective verification process. Nonetheless, companies maintain a system to verify the identity/profile of their clients and members. In addition, the payment of benefits and/or claims is consummated through the issuance of checks, wherein the beneficiary/claimant is declared as the payee. Since the transaction involves checks to be encashed, it will again undergo a tedious verification process by the bank which can identify and curb possible money launderers or finance terrorist.

Commonly used IDs by prospective clients to be presented to insurance companies are government IDs issued by the Philippine Regulation Commission (PRC) for professionals, Integrated Bar of the Philippines (IBP) for lawyers, Social Security System (SSS) for private employees, Government Service Insurance System (GSIS) for government employees, Land Transportation Office (LTO) as driver's licenses, and the Department of Foreign Affairs (DFA) as passports. Covered persons also utilize SEC I-view to verify the identification documents provided by their client to the companies as indicated in the previous NRA report.

### **Availability of Independent Information Sources**

Although there are only a few available independent sources of comprehensive, reliable historical information on clients, this variable is rated medium since there are database which can help determine or verify their identity, transactional patterns and commercial history such as those

maintained by credit bureaus. For example, some companies in the pre-need industry use the services of the Credit Management Association of the Philippines (CMAP), at a cost, to verify prospect agents. Some companies take advantage of internet search engines, such as Google and Yahoo, to get online information about their client. For MBAs, the verification process is done through their membership forms, government issued IDs, specimen card, payroll slip and personnel certification. For MI-MBAs, their partner MFI conducts a thorough background check on their potential clients by validating the information written in the application forms. Despite these efforts however, the industry feels that a reliable, foolproof, and effective national identification system will enable not only the insurance industry but the other sectors and the government as well, to curb money laundering and terrorist financing.

Quality of Operations (Medium)	Commitment and Leadership of Managements	Medium High
	Compliance of Insurance Company's Staff	Medium
	Quality of CDD Framework	Medium
	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium

Quality of operations of an insurance company would depend on the commitment of management, compliance of staff, quality of CDD framework and, suspicious activity monitoring and reporting.

Insurance companies generally registered medium to medium high level of management commitment, compliance of staff and quality of CDD framework. These factors should also be tied in with the ability of the company to effectively monitor and submit suspicious transaction reports. The said controls are assessed in the preceding section.

# Effectiveness of Suspicious Activity Monitoring and Reporting

The answers submitted by the covered entities to the NRA survey show that all covered persons have AML monitoring system in place to capture Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs). The system used by the covered entities may either be an in-house system, which is compliant with the Anti-Money Laundering Council's Version III Reporting procedures, or a software system that is bought from a reputable third-party provider of Anti-Money Laundering Software.

The AMLC has also noted that more and more covered persons of IC have registered with them to comply with the existing circular. AMLC is in the process of updating its database of IC covered persons to better keep track with them. Below is the table of Covered Transaction (CTR) and Suspicious Transaction (STR) submitted by the sector to the AMLC.

**Table 5-5. Covered Transaction Reports** 

Covered Persons	2011	2012	2013	2014	2015	2016	Grand Total
INSURANCE COMPANIES &	24,020	67,994	68,631	68,396	60,634	57,984	347,609
PROFESSIONAL REINSURERS							
PRE - NEED COMPANIES	162	337	572	1,255	503	776	3,605
MBAS & TRUSTS	19	39	215	176	136	147	732
INSURANCE BROKERS	17,028	16,551	21,319	14,495	7,662	-	77,055

GRAND TOTAL	1 41 229	84 871	90 737	84 322	68 935	58 907	429,001
GIVIND TOTAL	71,223	0-7,07 1	30,737	07,322	00,555	30,307	723,001

**Table 5-6. Suspicious Transaction Reports** 

Covered Persons	2011	2012	2013	2014	2015	2016	Grand
							Total
INSURANCE COMPANIES &	51	162	261	358	467	697	1,996
PROFESSIONAL REINSURERS							
PRE - NEED COMPANIES	-	-	-	2	-	-	2
INSURANCE BROKERS	-	-	2	4	-	-	6
GRAND TOTAL	51	162	263	364	467	697	2,004

The table of STR clearly indicates that from year 2011 to 2016, the reporting of suspicious transaction has an upward trend. Thus, insurance companies are complying with the AML regulations set forth by the regulators.

#### **PRODUCT VULNERABILITY**

In assessing the input variables, namely, volume and average transaction size, the insurance sector group considered the statistical data available with the IC's Statistics Division for the period covered. The group identified the general classification of the products for each insurance industry and obtained the premiums contributed for each class of product.

- For the life industry, premium income for the product was considered in the assessment.
- For the non-life industry, net premium for the product was considered in the assessment.
- For the pre-need industry, the products consist only of Life/Memorial and premium of the product was considered in the assessment.
- For the MBA industry which offers mainly life insurance products, the data on premiums contributed by the whole MBA industry were considered in the assessment.
- For the micro-insurance products, the data on premiums contributed by entities selling micro-insurance product were considered in the assessment.

For the average transaction size, the premium collected (dividend) was assessed against a second variable (divisor). For life and non-life products, the divisor is the number of policies for each class or line of product; for pre-need, it is the number of plans for each product line. For MBAs, the number of members for the whole MBA industry was considered with the assumption that all members avail of the life insurance.

Based on the assessment conducted, **VUL Life Insurance** poses the highest risk among insurance products assessed with its <u>MEDIUM</u> residual risk rating. Its inherent vulnerability is due to the total value/size and the availability of investment type policy. There are also reported existence of ML typologies on the existence of the product. The risk however is mitigated by the availability of product specific AML controls.

### **Variable Unit-Linked Insurance**

Introduced in the Philippine insurance market at the turn of the century, VUL products have been generating significant amount of premiums, proving to be a strong support in sales production to

traditional insurance products. As shown in the table below, there is a steady increase in the demand for VUL Life products. Variable Life products have been steadily increasing as the insurance product of choice, due to its versatile use and the improving sophistication and financial literacy of the insurance market.

Year	2011	2012	2013	2014	2015
Number of Variable Policies Sold	404,077	562,954	837,821	1,122,086	1,500,111
% of Variable Products Sold out	11.53%	14.93%	21.82%	27.34%	33.89%
of the Total New Businesses					
Premium Income of Variable	38,907.3	71,962.9	121,957.3	107,564.2	138,687.9
Products					
( <del>P</del> Million)					
% of Premium Income of	45.05%	59.82%	71.25%	67.76%	73.45%
Variable Products out of the					
Total Premium of Life Products					

Table 5-7. Variable Unit-Linked-Life Products

In a VUL policy, a client acquires both the protection of a traditional life insurance and the growth of potential of investment funds in one financial package. In VULs, a minimum death benefit is guaranteed, hence, the actual take-out can be higher; the cash values are not guaranteed, and "top-up premiums" and "partial withdrawals" are allowed. The policyholder has the chance to choose which investment fund will the premium be invested to. This gives the client relative freedom and power over his/her money. However, the investment risk is borne entirely by the client. If the fund of choice performs well, so will the invested part of the premium (also called account value), and vice versa. Moreover, most VUL policies allow policyholders to pay "top-up" premiums by buying additional units of investment fund and potentially increase the benefits of their plans. Withdrawals from the investment fund are also allowed. However, partial withdrawals reduce the potential benefits of the policy.

A significant feature of VUL policies is the provision of a mandatory 15-day cooling off or free-look period during which the policyholder can change his mind and get back the premium, i.e., the current account value plus charges applied, of the VUL policy being returned. Also, a number of VUL plans provide a loyalty bonus for policyholders who maintain their policies for a required number of years. The amount of bonus, ascertained by the insurance company and subject to conditions, are usually used to create additional units in the account value.

On the other hand, in traditional insurance policy, the death benefits and cash values are guaranteed, premiums are fixed, and the policyholder does not have the option where the insurance company shall invest his premium. In ordinary life insurance, only the death of the insured will entitle the beneficiaries to avail the product's full benefits. Because of this, clients are considered low profile. Investment/Deposit feature is not available in this ordinary life insurance product however, a considerable high surrender value over the years may be considered an attractive deposit feature for money launderers. The feature of some insurance products, requiring death or injury upon the insured to avail of its full benefits, makes it difficult for money launderer to acquire sufficient financial benefits from these products.

Insurance and Pre-Need companies registered in the Philippines can only sell their products here, thus, there is low probability of "off shore centers". 146 It should also be noted that insurance products are

<sup>&</sup>lt;sup>146</sup> Countries which offer little to no government interference in the activities of legitimate business owner and financial institutions

subject to the stringent underwriting to validate the financial capability of the applicant to satisfy its financial obligation once the application is approved. If the financial underwriting finds that the funds will come from anonymous accounts or unverified off shore accounts, then, more often than not, the application will be denied.

Insurers keep a systematized document of their client's information to up-sell their clients. Insurers also make use of the medical information of their clients; this means that they deal with hospitals or doctors who have more established and effective records or management processes.

Insurers use field underwriting which requires them to deal with the client face-to-face to fully understand the risk involved in covering a particular client. Very low risk products are exceptions. The use of agent is high because the agency force is still the main distribution system for insurance products. Agents facilitates the selling of insurance products as they explain to buyers the product and its feature face-to-face.

The insurance sector is significantly mature to recognize and determine money laundering risk within the industry. This is the very reason why the regulators and insurance companies alike have established specific controls to ensure that no transaction involving funds from launderers or terrorist get pass by them. If old clients are re-classified to become launderers or terrorist, their system will detect this and reporting to their regulator follows.

#### **ACTION PLAN**

Using the updated module provided by the World Bank, the Insurance Sector Working Group was able to identify the weaknesses and deficiencies in the priority variables of the Insurance Sector. Below are the recommended action points to address these identified gaps:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Coordination with AMLC Secretariat for offered AML/CFT related seminars/	IC AMLCS		ongoing
lectures			
Formulation, consolidation and updating	IC	AMLCS, PLIA,	On or
of IC AML/CFT rules and regulation with		PIRA, RIMANSI,	before
sanctions for non-compliance		Pre-Need	March 2018
		Federation,	
		AHMOPI,	
		PAHMO	
Language and the state of the ANAL (CET		(All Industry	
Increase capacity building for AML/CFT	10	Associations)	0
	IC		Ongoing
Submission of Compliance Checking	IC		ongoing
Report (CCR) on violations of AML/CFT	AMLCS		
To require covered persons with			
Certificate of Authority issued by IC to			
register with the AMLC			

#### VI. OTHER FINANCIAL INSTITUTIONS

### **EXECUTIVE SUMMARY**

The sub-sectors within the Other Financial Institutions (OFIs) are rated as follows:

Vulnerability Rating	NSSLAs	Stand-Alone MSBs	PS with Corollary Businesses	Lending and Financing Companies	Non-Bank E-Money Issuers
FINAL VULNERABILITY	Medium	Medium High	Medium High	Medium	Medium

Of the OFIs assessed, stand-alone MSBs [stand-alone money changers (MCs) and foreign exchange (FX) dealers, and stand-alone remittance agents (RAs)] have the highest money laundering and terrorist financing (ML/TF) risk. This is due to the common use of cash, higher exposure to overseas customers, use of informal overseas networks that may not be regulated, and very low turn-out of registration with AMLC for purposes of CTRs/STRs submissions. Given that it is only recently that MSBs have taken serious attention to AML/CFT activities in their businesses, this translates to poor implementation of policies and procedures which in turn increases the industry's vulnerability to such levels.

Emerging ML/TF risks have also made Non-Stock Savings and Loan Associations more vulnerable, particularly those in the military and police sectors. Non-Stock Savings and Loan Associations in these sectors have been used to disguise proceeds of unlawful activity, such as graft and corruption, plunder, bribery, malversation of public funds, and the like. Accordingly, the industry is rated as having **MEDIUM** vulnerability.

Vulnerability of Pawnshops with corollary businesses is rated as **MEDIUM-HIGH.** As covered persons under the Bangko Sentral ng Pilipinas (BSP), they are subject to periodic on-site and off-site examinations, particularly on matters pertaining to anti-money laundering and countering the financing of terrorism (AML/CFT) issues. However, with the sector's potential for further growth, visà-vis the inherent high risk in the money changing business as well as operational complexity in the remittance activity, there is a projected challenge in the monitoring of reportable transactions.

With respect to lending and financing companies,<sup>147</sup> the factors that pulled their vulnerability rating to **MEDIUM** is the lack of anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory and supervisory framework of the Securities and Exchange Commission (SEC), the agency mandated to regulate and supervise them. Added to this is the absence of adequate manpower of SEC that could conduct on-site examinations.

Finally, with respect to Non-Bank E-Money Issuers, its overall vulnerability is **MEDIUM**.

### **INTRODUCTION**

The OFIs is composed of six (6) sub-sectors, the (1) Non-Stock Savings and Loans Associations, (2) Stand-Alone Money Service Businesses, (3) Money Service Businesses in general (Pawnshops with

<sup>&</sup>lt;sup>147</sup> Excludes those affiliates and subsidiaries of banks and other BSP regulated entities.

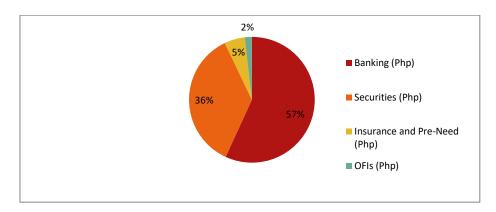
corollary businesses), (4) Lending Companies, <sup>148</sup> (5) Financing Companies, <sup>149</sup> and (6) Non-Bank E-Money Issuers.

In terms of assets size, the financing industry is the biggest in the sector. It is followed by the non-stock savings and loan associations, pawnshops with corollary businesses, lending companies, and non-bank e-money issuers. The ranking is based on the following:

Period	Financing Companies (PhP in Millions)	Non-Stocks Savings and Loan Associations (PhP in Millions)	Pawnshops with Corollary Businesses (PhP in Millions)	Lending Companies (PhP in Millions)	E-Money Issuers <sup>150</sup> (PhP in Millions)	Stand- Alone MSBs
2014	262,134.50	204,360.71	40,836.69	8,871.96	17,609.00	
2015	224,808.63	166,099.75	43,226.83	6,970.39	4,478.06	No
2016	No available data	180,697.66	No available data	No available data	2,668.00	available data <sup>151</sup>

Compared with banking, securities, and insurance sectors, the OFIs, in terms of assets size, represents a small fraction of the country's financial system.<sup>152</sup>

Banking (PhP)	Securities (PhP)	Insurance and Pre-Need (PhP)	OFIs (PhP)
13,900,000,000,000	8,814,876,039,476	1,290,061,000,000	445,583,657,974 <sup>153</sup>



### **SECTOR VULNERABILITY ASSESSMENT**

Vulnerability assessment of Other Financial Institutions is undertaken on a per sub-sector basis, taking into account their individual AML controls and product risk assessment.

<sup>&</sup>lt;sup>148</sup> Include only those regulated and supervised by the SEC.

<sup>149</sup> Ihid

<sup>&</sup>lt;sup>150</sup> Refers to two (2) major players in the industry, Pay Maya and Globe G-Exchange.

<sup>&</sup>lt;sup>151</sup> Examination conducted on the top 20 MSBs yielded no significant data on asset size and volume of transactions as they are not required to submit financial statements.

<sup>&</sup>lt;sup>152</sup> Based on the 2015 data on assets size.

<sup>&</sup>lt;sup>153</sup> Excluding stand-alone MSBs. But in terms of branch network, there are about 30,000 MSB offices compared to 10,000 banking offices.

### A. THE NON-STOCK SAVINGS AND LOANS ASSOCIATIONS (NSSLAS)

NSSLA includes any non-stock, non-profit corporation engaged in the business of accumulating the savings of its members and using such accumulations for loans to members to service the needs of households by providing long-term financing for home building and development and for personal finance. It does not transact business with the public.

Membership is confined only to a well-defined group of persons, which consists:

- (1) employees, officers, and trustees of a company, including member retirees;
- (2) government employees belonging to the same office, branch, or department, including member-retirees; and
- immediate members of the families up to the second degree of consanguinity or affinity of those falling under Items 1 and 2 above.

#### ML/TF Risk

Among the groups catered by NSSLAs, military and police NSSLAs are found to be more vulnerable to ML/TF risks. Military and police NSSLAs are headed by high-ranking military/police officials who are considered politically exposed persons (PEPs) under the ML/TF regime. NSSLAs in these sectors have been used to disguise proceeds of unlawful activity, such as graft and corruption, plunder, bribery, malversation of public funds, and the like.

Of the 81 NSSLAs in the Philippines, only 13 or 16% belong to the military/police sectors. However, these already comprise 74% or PhP133.3 Billion<sup>154</sup> of the total NSSLAs asset size.

#### **Vulnerabilities**

- Fraud in the acceptance of new members, acceptance beyond the membership criteria, and weak implementation of member identification process (KYC policy)
- Eighty-four percent (84%) of the NSSLAs' Total Resources are managed by retired military officials. High rate of non-reporting of Suspicious Transactions (132 unreported suspicious transactions) due to deference to transactions made by high-ranking military officials. These NSSLAs could be guilty of willful blindness in not reporting suspicious transactions.
- The ongoing process of monitoring members' transactions is weak, and enhanced due diligence is not strictly implemented, specifically by those in the military and police sectors.
- Despite the asset size and considerable number of members in NSSLAs, specifically in the
  military and police sectors, the existing regulations, do not require NSSLAs to have an
  electronic monitoring and reporting system capable of monitoring ML/TF risks and
  generating timely reports. The requirement of AML Electronic Monitoring system is
  mandatory only for universal and commercial banks.

The vulnerability of NSSLAs to ML based on the last assessment was **MEDIUM**.

Quality of AML	Effectiveness of Supervision/Oversight Activities	High
Supervision (Medium High)	Availability and Enforcement of Administrative Sanctions	Medium High

<sup>&</sup>lt;sup>154</sup> Based on the total industry assets as of 2016.

-

Quality of AML Supervision is rated based on whether NSSLAs are covered by a comprehensive supervision regime supported by appropriate powers, staff and other resources.

NSSLAs are covered by strict monitoring and supervision by the BSP. They are subject to both risk-based periodic, and special examinations by the BSP on matters relating to the AML/CFT requirements of the law and related BSP issuances, specifically BSP Circular No. 706, Series of 2011. In addition to regular examination, offsite monitoring is adequately in placed. NSSLAs are subject to the basic requirement on AML particularly, customer identification and due diligence, record keeping, reporting of CTRs/STRs and regular training for its personnel.

The **effectiveness of the supervision** regime is also linked with administrative sanctions. The more the sanctions are effective, proportionate, and dissuasive, the more likely it is that management and staff members will comply with AML laws and obligations.

Both the AMLC and the BSP can impose **administrative sanctions** to NSSLAs, its board, management and staff. The BSP can provide for non-monetary sanctions comprising of reprimand, suspension or removal or disqualification from office of the director/officer involved. In addition, monetary penalties can be imposed computed in accordance with existing regulations. In some cases, an escalated enforcement action called Prompt Corrective Action can be applied to an NSSLA. This requires immediate action of the concerned NSSLA and close supervisory attention of the BSP.

In one of BSP special examination involving high profile graft and corruption case, all members of the Board of Trustees, Compliance Officer, and Internal Auditor have been issued warning by the BSP. Said NSSLA was also imposed a monetary penalty. At the same time, an administrative case has been filed against its two former Branch Managers.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of	Quality of AML Supervision (Intermediate	Medium
Managements	Variable)	High
(Medium High)	Availability and Enforcement of Criminal	Medium
	Sanctions	High

The management's commitment and leadership in addressing ML risks can be influenced by entry controls, AMLC supervision and criminal sanctions.

Effective entry controls help to reduce money -laundering vulnerability, and ensure a higher level of compliance with AML requirements. Pursuant to Republic Act No. 8367, NSSLAs are required to register with the Securities and Exchange Commission (SEC) and obtain an authority from the BSP prior to transacting any business.

The quality of AML Supervision is also a factor in enforcing the commitment of NSSLAs. The BSP has the power to enforce laws, including orders, instructions, rules and regulations promulgated by the Monetary Board. Additionally, the BSP has the power to require an NSSLA, its trustees, officers and agents to conduct and manage its affairs in a lawful and orderly manner. Qualifications of each member of the board of trustees and officers of NSSLAs are regularly evaluated by the BSP to determine if they are fit and proper to assume their functions. This includes evaluation of educational attainment, training certification, experience, etc. of each trustee and officer.

Criminal sanctions are available under Section 14(a)(b)(c)(d)(c) and (f) of the AMLA, as amended. Penalties provided are effective, proportionate and dissuasive and is imposable on natural and covered persons. NSSLAs have been subject of investigation for being used as a conduit to money laundering, although none of its officers and staff have been convicted of money laundering.

In one of the high-profile graft and corruption cases, an NSSLA was used to finance bribe money to high-ranking government officials. The wife of a member-retired military officer opened special savings deposits (SSDs) under her name and several others. Each SSD earns 13% per annum. She had to use the names of other persons since a special deposit account (SDA) has a limit of PhP25 Million (USD581,000). From that SSD, the wife can borrow funds from NSSLAs using the SDA as a back-to-back guarantee, bearing an interest of 8%. In effect, the client can freely use money from NSSLAs and still earn from it. This unsound and highly irregular practice is a scheme that was also used to bribe government officials.

Recent special examination by the BSP also disclosed that high-ranking military and police officers used individuals who are not qualified members of their families to launder the proceeds of their graft and corrupt practices. The money borrowed from the NSSLAs would then be used to pay kickbacks or to bribe high-ranking government officials.

Quality of AML Policies and Procedures (Medium High)	Comprehensiveness of AML Legal Framework	Very High
	Commitment and Leadership of	Medium
	Managements (Intermediate Variable)	High
	Effectiveness of Compliance Function	NA a dissua
	(Organization)	Medium

The *quality of AML policies and procedures* of NSSLAs are assessed at **Medium High** considering the comprehensiveness of its AML legal framework and the general commitment of its management to address ML/TF risks.

NSSLAs are created pursuant to Republic Act No. 8367, which provides for its regulation, organization, and operation. It is considered covered persons under the AMLA, as amended, and is regulated and supervised by the BSP. As such, they are required to comply with the obligations under the Republic Act No. 9160, also known as the Anti-Money Laundering Act of 2001 (AMLA), as amended, and are subject to regular AML/CFT examinations by the BSP.

While management of the implementation of the NSSLA's policies and procedures is the primary task of the compliance office, the ultimate responsibility to implement rests with its board of trustees. Each NSSLA has its own compliance officer assisted by number of personnel depending on the size, nature of operation and risk profile of the institution. However, common BSP examination findings show: (i) failure to establish effective compliance testing program commensurate to the AML-related risk taking activities; and (ii) absence of or inadequate AML compliance testing by the Compliance Office. This then warranted a Medium rating for effectiveness of compliance function.

Compliance Level of Staff (Medium)	Availability and Enforcement of Criminal Sanctions	Medium High
	Effectiveness of Compliance Function (Organization)	Medium
	AML Knowledge of Business Staff	Medium High
	Integrity of Business Staff	

**Compliance Level of NSSLA staff** is assessed with regard to the AML legal framework and their institutional obligations.

Management and staff of NSSLAs are expected to know the law and their obligations under the law. NSSLAs usually send the board of trustees, management and other key officers to attend the AML trainings provided by the AMLC and BSP. On the other hand, other NSSLA personnel particularly those in the frontline perform their functions with basic knowledge on AML rules and regulations.

**Table 6-1. AML Trainings** 

		AMLC Database		
Type of Institution	Year	No. of AML Trainings on Reporting Procedure	No. of Participants	
Non-Stock Savings and Loans Associations	2014	22	75	
	2015	18	193	
	2016	26	281	

NSSLAs are also required to adopt and implement a comprehensive ML/TF Prevention Framework throughout the institution. This has to be cascaded to all its employees. It was noted during BSP examinations that the policies and procedures need minor refinements to consider the appropriate risk profile, nature of operation and size of the institution and dissemination to its personnel.

With respect to integrity, NSSLA industry generally regards their board of trustees, management and staff members as having integrity to protect the interest of the institution from known AML related risks. However, some NSSLAs have been used in the past to disguise proceeds of unlawful activity, such as graft and corruption, plunder, bribery, and malversation of public funds. The involved NSSLA's and their staff were investigated by the AMLC and may be subject to criminal sanctions once found guilty.

In addition, a standard report known as the Report on Crimes and/or Losses (RCL) which is required to be submitted to the BSP showed that internal crimes/losses, though not AML related, are often due to employee fraud. To address this, NSSLAs enforce code of ethics which contains disciplinary action for breach of internal rules and other regulations.

Quality of CDD Framework (Medium Low)	Availability and Access to Beneficial Ownership Information	Not Applicable
	Availability of Reliable Identification Infrastructure	Medium High
	Availability of Independent Information	Close to
	Sources	Nothing

The variable, **Availability and Access to Beneficial Ownership Information** is not applicable to NSSLAs as all members and/or clients are individuals only.

With respect to the identification of its clients, NSSLAs can rely on the identification document issued by an official authority, even in the absence of a national identification system in accordance with the regulations. In addition, NSSLAs membership is confined only to a well-defined group of persons. This then makes it easier for NSSLAs to verify the identity of their clients. Regular members of NSSLAs are personnel of one private company, or government employees belonging to the same office, branch, or department.

Customer due diligence processes are easier to perform, and are generally of a higher quality, if NSSLAs are able to determine transaction patterns of clients. There is no existing independent information source to which an NSSLA can rely on to determine transactional patterns and commercial history. This is due to the nature of confined membership of the industry.

	Commitment and Leadership of Managements	Medium High
Quality of Operations	Compliance Level of Staff	Medium
(Medium)	Quality of CDD Framework	Medium Low
	Effectiveness of Suspicious Activity Monitoring and Reporting	Low

As discussed above, commitment of leadership in addressing ML risk is rated as Medium High due to the entry controls enforced by SEC and the BSP, the supervisory authority of the BSP, and the dissuasive criminal sanctions available and which can be enforced against erring NSSLAs and their officers and staff. Compliance level of staff is at a medium due to reported involvement of NSSLAs in ML activities. Furthermore, there are also incidents of employee fraud. Quality of CDD is at a Medium Low due to the lack of independent information sources to check transaction patterns of clients.

The quality of operations within NSSLAs in preventing abuse for money laundering is also affected by the Effectiveness of Suspicious Activity Monitoring and Reporting. This variable assesses whether the covered person has an effective and appropriate system for record keeping, monitoring, and STR reporting to support their AML policies and procedures.

In the case of NSSLAs, they implement a manual record keeping system. Know-Your-Customer related documents and transaction records are being maintained on a per branch basis. This set-up makes it difficult, especially for big institutions, to monitor the commensurability of transaction activities against members' profile. CTRs and STRs submitted by the NSSLA's for the period 2014-2016 are summarized in the table below:

Table 6-2. CTRs and STRs submitted by NSSLAs

Type of Institution	Year	No. of entities registered with AMLC	No. of entities reporting CTRs/STRs	No. of STRs Submitted to AMLC	No. of CTRs Submitted to AMLC
Non-Stock Savings	2014	49	28	4	33318
and Loans	2015	51	29	111	45122
Associations	2016	57	32	86	54277

Most NSSLAs have no comprehensive databases of politically exposed persons and sanctioned individuals to facilitate timely screening of members with potential high AML risk exposure. The system is also insufficient to monitor members with multiple transactions in different branches.

# B. MONEY SERVICE BUSINESSES (MSBS)

MSBs include large sophisticated chains with nationwide and international operational facilities that focus on providing financial services, such as the issuance of electronic cash cards (e-money issuers), lending (pawnshops), money transmission (remittance agents), and foreign exchange transactions (money changers) to various customers.

MSB chains (e.g., pawnshops and remittance agents) usually maintain several organizational levels to conduct their business. Each level is authorized to approve certain transactions. The number of authorization levels may vary depending on the amount of customer transactions and the number of branches.

This part of the assessment covers stand-alone MSBs or those not affiliated with banks, pawnshops, and other BSP-supervised entities, i.e. stand-alone: (1) MCs/FX dealers, and (2) RAs; and MSBs in general, namely: pawnshops with corollary business of remittance or money changing/FX dealing or both.

# **B.1** Stand-Alone MCs/FX Dealers

Stand-alone MCs/FX dealers refer to entities that are not affiliated with BSP-supervised entities, and regularly engage in the business of buying and/or selling foreign currencies. For this purpose, the term MCs can be interchangeably referred to as FX dealers.

In practice, MCs/FX dealers provide several services that are also provided by banks and other regulated financial institutions. A BSP-supervised covered person that has a MC/FX dealer as a customer requires the submission of a copy of the latter's certificate of registration issued by the BSP as part of the customer identification documents. Aside from having a MC/FX dealer license, MCs/FX dealers can also simultaneously register as RAs.

In the Philippines, the biggest stand-alone MCs/FX dealers are corporations. But those formed as sole proprietorships have weekly average transaction volume ranging from over a hundred of millions to billions of pesos.

### **Vulnerabilities**

ML risks for this sector are inherently high as money changers handle large amounts of physical cash and transact mainly with walk-in and one-off customers. The large number of customers, including PEPs, and the short time taken to complete individual transactions pose significant challenges in identifying suspicious transactions. This is especially so when transactions can be broken down into several smaller transactions to avoid the reporting thresholds.

Stand-alone MCs/FX dealers are becoming the favorite channel for laundering proceeds of illegal drugs, graft and corruption (e.g., PDAF scam), frauds/estafa (e.g. Aman Pyramiding scam), and other predicate offenses. There is significant non-reporting of covered and suspicious transactions due to non-registration with the AMLC. It was also noted that owners of stand-alone MCs/FX dealers often use their personal bank accounts (instead of using accounts under the name of the registered MCs/FX

dealers) in conducting their money changing business. MCs/FX dealers, which are not BSP-registered RAs, also facilitate the remittance/transfer of funds on behalf of their clients to obscure the sources and destination of funds.

Overall, the ML/TF vulnerability for stand-alone MCs/FX dealers based on the last assessment is medium high. Given that it is only recently that MSBs have taken serious attention to AML/CFT activities in their businesses, this translates to poor implementation of policies and procedures which in turn increases the industry's vulnerability to such levels.

#### **B.2** Stand-Alone RAs

Stand-alone RAs refer to persons or entities that are not affiliated with BSP-supervised entities, and offer the services of remitting, or transferring money, on behalf of any person, to another person and/or entity. They include money or cash couriers, money transmission agents, remittance companies, and the like.

# Basic Business Model of an RA

The basic money transmitter business model involves three parties: the sender/originator, remittance agent, and recipient/beneficiary. RAs may engage in money transmission for individual and juridical entity customers. A commercial RA may engage in wholesale transactions with no network of agents. The sender provides the funds to the RA with instructions to deliver the same to the recipient. The RA conducts the transaction by taking the funds from the sender and delivering the same to the recipient. The operation for transfer of funds may either be domestic or international.

Large RAs usually have a head office, transaction clearing center/s, service/s, regional offices, and branches. They may also enter into partnerships with agents that include established businesses, like banks, convenience stores, gasoline stations, pawnshops, supermarket chain remittances, and even small variety stores. The money transmission home office pays its agents using a fee matrix that provides predetermined charges (fees) for remittances. Agents receive commissions on the fees charged for transferring money, and some receive a portion of any foreign exchange profit that may be received by the money transmitter.

When a transaction to send or receive money is initiated by a sender, the RA's employee or agent will contact the RA's service center. This is generally done over the phone, through short messaging system or with the use of an online computer system installed in the branch or agent location. The information from the sender transaction form is entered into the service center computer system. The transaction documents obtained from the originator/sender or beneficiary/recipient should be kept by the RA for five (5) years or longer when it is the subject of an ML/TF case.

Another business model involves five parties, namely: sender, branch or agent, money transmitter, receiving agent, and recipient. Additional parties mentioned above are branches or agents, and receiving agent. Through branches and agents, RAs can expand customer access points. Attracting existing businesses, such as convenience stores, to act as agents allows the RA to provide customer access and convenience while at the same time leveraging valuable and limited financial resources.

The RA must have a means to deliver the funds to the recipient. Therefore, to be able to complete the transmission activity, the RA will normally enter into agreements with receiving agents. Receiving agents are other financial service providers (including banks) that are in closer proximity to the recipient. Again, the relationship between the RA and the receiving agent is contractual and the cost of the arrangement to the RA is fee-based.

Regardless of the business model adopted, each RA has its own forms to document the sending and receiving of money. Generally, the basic information recorded on these forms includes but is not limited to: a) source of funds; b) date of the transaction; c) amount of the transaction; d) name of the person sending money (sender); e) name of the person receiving the money (recipient); and f) reference (transaction) number assigned by the service center.

#### **Vulnerabilities**

RAs typically cater to individuals, expatriate professionals, and small and medium enterprises. The channels used for the remittance of funds to beneficiaries overseas include local and foreign banks, pawnshops, other registered remittance agents and informal networks, such as overseas agents. Beneficiaries generally receive their funds via door-to-door cash delivery, direct credit to their bank accounts, or self-collection of funds at designated outlets. Customers usually settle their transactions in cash. They may also use checks or make deposits directly to the registered RAs bank accounts.

The cash-intensive nature of remittance transactions, the low cost of remittance, and the swiftness of processing a large number of transactions attract potential money launderers. Cross-border fund flows also pose a greater risk of illicit funds being introduced into the financial system. For instance, there have been cases where proceeds derived from scams and online frauds/cybercrimes were transferred to and from the Philippines through RAs.

The informal overseas networks that some RAs use to remit funds may not be adequately regulated in the overseas jurisdictions for AML/CFT purposes. In addition, overseas RAs that transact with local registered RAs and banks often do not disclose the identity of their overseas customers or sources of funds. Consequently, this may increase the industry's exposure to risks. In particular, smaller RAs may not have adequate resources and systems to put in place additional risk mitigation measures. Common control weaknesses noted in RAs include failure to conduct comprehensive CDD and establish the source of funds, as well as inadequate monitoring system to identify unusual and/or suspicious transactions.

Like the stand-alone MCs/FX dealers, ML/TF vulnerability for stand-alone RAs is **MEDIUM HIGH** due to the common use of cash, higher exposure to overseas customers, use of informal overseas networks that may not be regulated, and very low turn-out of registration with AMLC for purposes of CTRs/STRs submissions.

### C. PAWNSHOPS (WITH COROLLARY BUSINESSES)

A "pawnshop" refers to a person or entity engaged in the business of lending money on a personal property delivered as a security for loans. It is synonymous and used interchangeably with "pawnbroker" or "pawn brokerage." It is also understood as pawning, which is the practice of lending money and accepting and/or keeping gold and other personal properties of value as collaterals. In the Philippines, it is the usual mode of having fast cash especially in cases of unforeseen and immediate need of the unbanked and under-banked sector.

Pawnshops with remittance and money changing businesses, on the other hand, refer to those, which, on top of the pawning activity, likewise offer remittance services and money changing or foreign exchange dealership as corollary businesses. They maximize and take advantage of the network and portfolio established and already available for the pawnshop business.

The industry of pawnshops with remittance and money changing businesses is one that provides significant contributions to the economy. Not only does it extend immediate relief for those who are

in need of cash and provide a one-stop facility for clients in need of its corollary services, but its assets provide a significant boost to the economy through additional financial inclusion services, employment opportunities and tax revenues. For the years 2012, 2013, and 2014 alone, the total recorded assets of the top 20 pawnshops with remittance and money changing businesses amount to PhP24.775 Billion, and PhP25.851, and PhP32.824 Billion, respectively.

The growth in the industry carries an increased ML/TF risks owing to the industry's tendency for expansion and greater complexity of operation, especially in the areas of money changing and remittance businesses.

### **Vulnerabilities**

Owing to the sector's potential for further growth, vis-à-vis the inherent high risk in the money changing business as well as operational complexity in the remittance activity, there is a projected challenge in the monitoring of reportable transactions. In addition, the sector continues to encounter the following ML/TF risks associated transactions:

## **Pawnshop**

- PEPs pawning high-value pieces of jewelry;
- Pawning personal effects like jewelry and watches, related to or representing proceeds of theft and robbery;
- Small-time pawnshops pawning customers' pawned items to other pawnshops to sustain their operations;
- Vault items stolen by branch personnel for resale and/or pawning;
- Violation of the Anti-Fencing Law in cases where the customer is unable to present proof of ownership; and
- Fictitious pawn transactions processed by branch personnel without actual collateral.

# **Remittance Agent**

- Fraudulent transactions arising from online purchases and romance scams; and
- Fraudulent claims using counterfeit identification documents.

### **Money Changer**

- Use of counterfeit bills; and
- Multiple transactions of one client using different falsified IDs bearing different names.

# Assessment of Variables for Stand-Alone MSBs and Pawnshops with Corollary Businesses

Quality of AML Supervision	Effectiveness of Supervision/Oversight Activities	Medium High
(Medium)	Availability and Enforcement of Administrative Sanctions	Medium High

Supervision of MSBs is primarily assigned to the Integrated Supervision Department I (ISD I). ISD I has long handled the inspection of pawnshops and money changers. In 2015, it started to include in its

program the on-site examination of remittance agents in coordination with the Anti-Money Laundering Specialist Group (AMLSG) in view of the increasing risks attached to these entities. Currently, ISD I uses the same framework used to examine bigger financial institutions. It applies the standardized Anti-Money Laundering Risk Rating System (ARRS) of the BSP as required by existing supervision guidelines resulting in the establishment of a better AML Ratings Database for reference in making informed policy decisions.

While the use of the ARRS is a step in the right direction for the supervision of the entities, the capacity of the ISD I as a unit need to be improved due to the sheer disparity in terms of the number of examiners versus the number of entities handled by the department. As of 16 December 2016, there are more than 18,000 registered MSBs with the BSP that require supervision. While the figures are expected to drop after the full implementation of the re-registration of MSBs under Circular Nos. 938 and 942, the projected 50% re-registrants will still prove to be a challenge in terms of supervision.

In relation to the capacity of the examiners, there is a need to provide more opportunities in terms of trainings and advancement considering the increasing risks those MSBs poses. In addition, ISD I is designated to handle entities engaged in emerging technologies. With the emergence of Financial Technology and its correlated businesses, there is a need to equip the examiners with necessary skills and technical capacity to handle examinations geared towards non-traditional products.

Both the AMLC and the BSP can impose administrative sanctions on MSBs, its board, management and staff. The AMLC, pursuant to Section 14.f of the AMLA, as amended, it can impose administrative sanctions, consisting of monetary penalties, warning or reprimand, upon covered persons, its officers, and employees who violate provisions of the AMLA, as amended.

Likewise, the BSP can provide for non-monetary sanctions comprising of reprimand, suspension or removal or disqualification from office of the director/officer involved. In addition, it is granted the power to cancel the certificate of registration issued to entities that have violated their undertaking of continuously complying with prevailing AML rules and regulations. This power was recently exercised by the BSP when it cancelled the certificate of registration granted to an MSB determined to be involved in the Bangladesh Bank Heist. The said exercise of such administrative powers led to the increase in awareness of the industry on the repercussions of failing to raise the level of AML/CFT compliance to an acceptable level.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of Managements	Quality of AML Supervision (Intermediate Variable)	Medium
(Medium High)	Availability and Enforcement of Criminal Sanctions	Medium High

MSBs are subject to strict entry controls which have been reinforced with the creation of Circulars No. 938 and 942. With the new re-registration initiative through the Circulars, a major reset has been made to all supervised MSBs for the benefit of both the entities and the regulators. For the entities, the Circulars provided them ease of registration since the network approach is now being implemented. Certain entities, which were previously required separate registration, can now be under the umbrella of the network they are using, thereby eliminating the need for separate registration by being just listed under the oversight of the network provider. On the regulator side, it provided an opportunity to purge the list of inactive entities and/or entities that do not have updated details with the BSP database.

Among the salient features of the Circulars are provisions on: 1) the fit and proper rules for the owners, directors, and/or officers of the MSBs; 2) requirement for all owners, directors, and officers to undergo AML training prior to the issuance of a certificate of registration; and 3) capitalization requirements based on business type and projected levels of activity. The combination of the foregoing factors, and the existence of a dedicated unit handling the registration process, has proven to be effective as far as the re-registration process is concerned.

Commitment of management in addressing ML risks is also a function of AML supervision. BSP, as the supervisory authority, has imposed sanctions, and has in fact, cancelled the certificate of registration of an MSB involved in the Bangladesh Bank Heist. Imposition of sanctions then reinforces commitment of management.

Criminal sanctions are available under Section 14(a)(b)(c)(d)(c) and (f) of the AMLA, as amended. Penalties provided are effective, proportionate and dissuasive and is imposable on natural and covered persons. Criminal cases have been filed against officers of MSBs involved in money laundering activities.

Overlity of ANAL Policies	Comprehensiveness of AML Legal Framework	Very High
Quality of AML Policies and Procedures (Medium)	Commitment and Leadership of	Medium
	Managements (Intermediate Variable)	High
	Effectiveness of Compliance Function	Medium
	(Organization)	Low

The Philippines, as one of the top global remittance destination<sup>155</sup> has long recognized the importance of the MSBs in contributing to the overall growth of the Philippine Economy. Along with this growing reliance on remittance comes with the need for relevant laws and regulations to temper potential exposure to AML/CFT risks given the inherently high risk of doing cross border transactions. MSBs are subject to the same AML laws and regulations as applicable to other covered persons under the supervision of the BSP. They are covered by the recently issued BSP Circular No. 950<sup>156</sup>.

The importance of AML/CFT activities related to MSBs has been reiterated by the issuance of BSP Circulars No. 938<sup>157</sup> and 942<sup>158</sup>wherein continuing compliance with prevailing AML/CFT rules and regulations is essential for the continued existence of the business entities. The Circulars require the execution of a deed of undertaking, on the part of the MSBs, that any violation of the AMLA, as amended, and the correlated BSP rules and regulations, will subject the erring MSB to sanctions as may be applicable.

While the issue of authority of the BSP over MSBs subsists, this loophole has been temporarily addressed by the issuance of the 2016 Revised Implementing Rules and Regulations (RIRR)<sup>159</sup> of the AMLA, as amended, stating that for purposes of the RIRR, foreign exchange dealers, money changers, and remittance and transfer companies are covered persons under the regulation of the BSP. The issue on the indirect authority of the BSP over such entities should be addressed once the BSP charter is amended.

<sup>157</sup> Approved 23 December 2016

Page 185 of 300

<sup>&</sup>lt;sup>155</sup> Migration and Remittance Factbook 2016 – Advance Edition, World Bank Group

<sup>156</sup> Approved 15 March 2017

<sup>&</sup>lt;sup>158</sup> Approved 20 January 2017

<sup>&</sup>lt;sup>159</sup> Approved 21 September 2016

In setting up an internal compliance unit, consideration should be given to the size and structure of most MSBs. In most cases, particularly for sole proprietorships, owners themselves act as compliance officers since hiring dedicated and independent compliance officer does not appear a good business sense as it would mean increased business cost. For bigger entities, established as corporations, they have dedicated compliance officers.

Internal compliance function of MSBs is assessed at Medium Low as examination results showed that compliance units are not sufficiently-resourced to be effective. In addition, there is a general absence of culture of compliance among the entities since compliance officers are still subservient to the orders of the business owners. It is noted that though bigger entities are established as corporations, they are close corporations whose ownership is limited to family members. Combination of the aforementioned factors renders the compliance functions as generally existent, but not operating effectively.

	Availability and Enforcement of Criminal Sanctions	Medium High
Compliance Level of Staff	Effectiveness of Compliance Function (Organization)	Medium Low
(Medium)	AML Knowledge of Business Staff	Medium High
	Integrity of Business Staff	Medium High

Compliance level of staff is influenced by criminal sanctions, internal compliance function, AML knowledge and staff integrity.

Criminal sanctions is seen to be available, with some MSB owners/officers charged with money laundering. Internal compliance is seen to be medium low in effectiveness as examination results showed that compliance units are not sufficiently-resourced.

With respect to AML knowledge, general examination show that most entities have issues with the quality of AML knowledge of its staff. Part of the examination of MSBs' continuing education and training program include review of type, frequency and hours of training, number of participants, training materials, and validation exam. While most employees know the basic concepts such as KYC and customer profiling, these employees have difficulty translating such knowledge into practice as shown by noted implementation lapses.

**Table 6-3. AML Trainings** 

			Provid	ed by BSP	Provided	l by AMLC
Type of Institution		Year	No. of AML Trainings	No. of Participants	No. of AML Reporting Procedure Trainings	No. of Participants
		2014	27	795	9	23
	Remittance Agents	2015	27	717	10	18
MSBs		2016	28	812	13	182
		2014	30	665	2	4
	Pawnshops	2015	24	507	1	1

		2016	23	565	5	49
	EV Dealers / Manay	2014	27	113	3	4
	FX Dealers / Money Changers	2015	27	133	4	7
	Changers	2016	28	252	20	66
	FX Dealers / Money	2014			5	6
	Changers /				9	27
	Remittance Agents	2016			29	192
Dayunchan	Per Remittance and FX/MC	2014	30	883	1	2
Pawnshop with		2015	24	807	1	2
WILII		2016	23	1072	6	34
Non Stock Sovings and Loans		2014			22	75
	Non-Stock Savings and Loans Associations				18	193
A	330010110113	2016			26	281

Although most entities require their employees to attend the basic introductory AML course provided by the BSP, this should still be complemented by refresher course with topics different from the introductory course. However, given the very limited avenues for such employees to get quality AML training and refresher courses, it translates to employees having limited understanding of their AML obligation based on their position and level of AML risk exposure.

Most MSBs in the Philippines have very basic business structure wherein the owner usually operates the business through a hands-on approach. While this approach tends to mitigate the possibility of staff breaches, a correlated issue on the ability of MSBs to actually identify potentially suspicious transaction comes into play. Issues on integrity can be attributed to negligence/willful blindness of the staff or the lack of training to properly identify suspicious transactions. In the Philippine setting, the latter scenario is more appropriate given that it is only recently that MSBs have taken serious attention to AML/CFT activities in their businesses. An issue affecting this assessment would be the incomplete reporting tools available for the BSP. A standard report known as RCLs are submitted on a periodic basis to the BSP to identify potential/actual losses that entities may suffer due to various reasons. It was observed that RCLs related to internal crimes/losses are more often than not due to employee fraud. The report is an effective tool but can still be maximized since not all entities are required to accomplish the RCL. Specifically, for MSBs, only pawnshops are required to file the periodic RCL to the BSP through the Supervisory Data Center (SDC).

Ovality of CDD	Availability and Access to Beneficial Ownership information	Medium
Quality of CDD Framework (Medium)	Availability of Reliable Identification Infrastructure	Medium
(iviealum)	Availability of Independent Information Sources	Low

Input variables for Quality of CDD Framework follow the same assessment ratings as provided by the National Vulnerability and Banking Sector Vulnerability. However, as risk mitigants, bigger MSBs have implemented their own identification system by issuance of membership cards assigned with unique identifiers. The identification system employs its own image capturing technology to facilitate verification of identity of their clients. Clients are incentivized of availing membership since the cards are embedded with rewards and/or rebates every time their clients avail of their services. In certain entities, the membership card also serves as a repository of the permanent transaction records of the customer. The perpetual record of all transactions of the client can be easily extracted from the card

itself similar to the concept of the block chain. Such adds value to the use of the card since it facilitates monitoring of the clients' transactions even if the particular branch is temporarily disconnected from the network of the compliance office.

	Commitment and Leadership of Managements	Medium High
Quality of	Compliance Level of Staff	Medium
Operations (Medium)	Quality of CDD Framework	Medium
(Iviealum)	Effectiveness of Suspicious Activity Monitoring and Reporting	Very Low

The quality of operations can be seen on how well it is able to prevent the abuse of the sector for money laundering. It is a reflection of the commitment of management (Medium High) and the compliance level of staff (Medium). It also looks into how well the sector is able to identify its clients (Medium).

N	Total		
FXD/MC	FXD/MC/RA	RA	TOLAI
2,068	8,831	8,178	19,077

<sup>\*</sup>Physical offices (Head offices and branches)
BSP Statistics on Registered OFIs as of 31 December 2016

Table 6-4. AMLC Registration and CT/ST Reporting

Type of	Institution	Year	No. of entities registered with AMLC	No. of entities reporting CTRs/STRs	No. of STRs Submitted to AMLC	No. of CTRs Submitted to AMLC
		2014	237	28	173	2196
	Remittance	2015	240	30	2073	803
		2016	512	35	1681	2862
		2014	260	5	0	218
	Pawnshops	2015	287	3	0	174
		2016	447	3	0	842
MSBs	FX Dealers /	2014	159	8	0	296780
	Money	2015	165	11	148	103730
	Changers	2016	465	23	90	2825
	FX Dealers /	2014	103	19	4123	9623
	Money	2015	133	20	839	7665
	Changers / Remittance	2016	511	40	2453	40476
Dawnshan	Domittanco	2014	61	5	251	157
Pawnshop with	Remittance and FX/MC	2015	66	8	13	173
VVILII	allu FA/IVIC	2016	227	11	139	129
Non Stock	Cavings and	2014	49	28	4	33318
	Savings and Sociations	2015	51	29	111	45122
LUaiis As	Sociations	2016	57	32	86	54277

The very low effectiveness of suspicious activity monitoring and reporting is a result of the following:

1) transactional records not always available, or if available, is in a format that is inconvenient to analyze resulting to failed facilitation of AML screening and monitoring; 2) PEP screening and sanction screening not consistently performed and documented; 3) absence of alert parameters that would assist employees in effectively identifying and recording all complex, unusual, and suspicious transactions; and 4) lack of good understanding of the scope of their reporting obligations with regard to suspicious transactions and activities, including what activities are covered, or not covered, under laws and regulations.

Existing regulations require that only universal banks (UBs), commercial banks (KBs), and other entities considered as complex by the BSP to adopt electronic AML systems capable of monitoring risks associated with ML/TF as well as generating timely reports for the guidance and information of its board of directors and senior management in addition to the prescribed functionalities. For covered persons other than UBs, KBs, and complex entities it need not have an electronic system but must ensure that it has the means of complying with the monitoring and reporting requirement. This restrictive provision makes it hard to require MSBs with multiple branches of adopting electronic monitoring systems to enable and facilitate monitoring of client transactions and review against the clients' profiles. Since majority of the MSBs have less than 10 units, the use a manual system may not be effective since the use of manual systems is really appropriate only for single-unit businesses.

In sum, the vulnerabilities to ML/TF risks of NSSLAs, Stand-alone MSBs, and Pawnshops with corollary businesses are Medium, Medium High, and Medium High, respectively.

#### **ACTION PLAN**

Based on the identified weaknesses and deficiencies in controls of NSSLAs and MSBs, the following are the recommended action points:

ACTION PLAN	PRIMARY AGENCY	TIMELINE
Require technology dependent and/or high volume NSSLAs, stand—alone MSBs, and pawnshops to adopt an AML electronic monitoring		12 months
system, to improve the ability of entities to identify, monitor, and		
report suspicious activities and/or transactions.		
Creation of a standardized learning framework including the		12 months
accreditation of external training providers.		
Strict implementation of Enforcement Actions.	DCD	On-going
Require prudential reports (financial statements and reports on crimes and losses, among others) from stand-alone MSBs to improve oversight by the BSP.	BSP	12 months
Amend the Examination Procedures of ISD I to heighten monitoring of activities related to Terrorist Financing.		
Recommend an amended AML Risk Rating System that is commensurate to the size, operations, and complexity of ISD I supervised entities (NSSLAs, Pawnshops, and MSBs).		
Capacity build-up of the examination unit handling MSBs/NSSLAs.		

#### D. LENDING AND FINANCING COMPANIES

A **lending company** refers to a corporation engaged in granting loans from its own capital funds or from funds sourced from not more than nineteen (19) persons. It shall not be deemed to include banking institutions, investment houses, savings and loan associations, financing companies, pawnshops, insurance companies, cooperatives and other credit institutions already regulated by law. The term is synonymous with lending investors.<sup>160</sup>

The number of lending companies from 2014 to 2016, including their assets, is as follows:

**Table 6-5. Assets of Lending Companies** 

Year	Year No. of Lending Companies				
2014	1,633	8,871.96 Million			
2015	1,754	6,970.39 Million			
2016	Not available	Not available			

A **financing company**, on the other hand, is a corporation, except bank, investment house, savings and loan association, insurance company, cooperative, and other financial institutions organized or operating under other special laws, which is primarily organized for the purpose of extending credit facilities to consumers and to industrial, commercial, or agricultural enterprises, by direct lending or by discounting or factoring commercial papers or accounts receivable, or by buying and selling contracts, leases, chattel mortgages, or other evidences of indebtedness, or by financial leasing of movable as well as immovable property.<sup>161</sup>

Compared with the lending industry, financing companies have a smaller number. But owing to the higher capitalization required (paid-up of PhP10,000,000.00 in Metro Manila and first class cities, PhP5,000,000.00 in other cities, and PhP2,500,000.00 in municipalities) the combined assets of financing companies for the same period (2014 to 2016) is bigger than those of lending companies, viz:

**Table 6-6. Assets of Financing Companies** 

Year	No. of Financing Companies	Assets (PhP)
2014	610	262,134.50 Million
2015	622	224,808.63 Million
2016	Not available	Not available

With the enactment into law of Republic Act No. 10881 in 2016, foreign ownership of lending and financing companies is allowed up to 100%.

Based on the last assessment, the ML/TF vulnerability of the lending and financing industry was medium low.

<sup>&</sup>lt;sup>160</sup>Republic Act No. 9474, also known as An Act Governing the Establishment, Operation and Regulation of Lending Companies.

<sup>&</sup>lt;sup>161</sup> Republic Act No. 8556, also known as Financing Company Act of 1998.

Quality of AML	Effectiveness of Supervision/Oversight Activities	Medium Low
Supervision (Medium )	Availability and Enforcement of Administrative Sanctions	Medium

The SEC has limited resources in terms of personnel tasked to monitor compliance of lending and financing companies. On-site examinations are never done, except in cases where the company to be examined is: (1) the subject of a tip for irregularity and/or possible violation of laws and regulations, (2) the subject of a complaint, or (3) did not comply with regulatory requirements such as payment of annual fees and submission of reports.

Thus, the SEC limits itself to off-site or table examinations. But even in off-site or table examinations, its personnel can handle only up to a maximum of one hundred (100) entities per year. The number is prioritized according to parameters, namely: (1) walked-in request of the entity for a clearance, (2) letter-request of the entity for a clearance, (3) motu-propio on the part of the SEC because of the entity's non-payment of annual fees.

Thus, there is also no audit testing and/or validation of the AML Operating Manual and AML Compliance Forms that are required of lending and financing companies. This is the reason why no referral from the SEC has ever been received by the AMLC, within the period covered by the assessment, for investigation of possible violation of the AMLA, as amended.

Section 14.f of the AMLA empowers the AMLC to impose administrative sanctions upon any covered person, its directors, officers, employees or any other person in violation of the AMLA, as amended. The sanctions include monetary penalties, warning or reprimand. It also empowers the AMLC to promulgate rules on fines and penalties taking into consideration the attendant circumstances, such as the nature and gravity of the violation or irregularity. Pursuant to it, the AMLC promulgated the Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as amended. Section 3 of the Rules provides for a range of effective, proportionate and dissuasive administrative sanctions against covered persons depending on the gravity of violations.

The administrative sanctions under the AMLA, as amended, are without prejudice to the imposition of administrative sanctions by the SEC for violation of Republic Act Nos. 9479 and 8556, as the case maybe. However, given the absence of AML regulatory and supervisory framework that would complement the sanctions mechanisms, in terms of monitoring and detailed guidance of compliance with the AML and CFT regime, among others, the effectiveness thereof is mitigated.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of	Quality of AML Supervision (Intermediate	Medium
Managements	Variable)	Low
(Medium)	Availability and Enforcement of Criminal	Medium
	Sanctions	High

The management's commitment and leadership in addressing ML risks can be influenced by entry controls, AMLC supervision and criminal sanctions.

Pursuant to Republic Act Nos. 9479 and 8556, lending and financing entities are required to pass through the process of corporate registration under Batas Pambansa 68, also known as the

Corporation Code of the Philippines, before being issued secondary licenses for lending and financing operations. Though the processes for registration and issuance of secondary licenses take place simultaneously, they require different sets of documentary requirements that ensure the fitness of people desiring to be incorporators and directors.

The corporate registration of lending and financing companies, including the issuance of secondary licenses, is handled by four (4) staff members, who, through experience and training, have gained a degree of efficiency in the processing and scrutiny of registration and licensing.

**Quality of supervision** is rated at **Medium Low** considering that the SEC limits itself to off-site examination, without audit testing and/or validation of the AML Operating Manual and AML Compliance Forms.

With respect to criminal sanctions, Section 14(a)(b)(c)(d)(e) of the AMLA provides effective, proportionate and dissuasive criminal sanctions imposable both on natural and covered persons. Again, this is without prejudice to the criminal prosecutions for violation of Republic Act Nos. 9479 and 8556, as the case maybe. Given the absence of AML regulatory and supervisory framework that would complement the sanctions mechanisms the effectiveness thereof is mitigated.

Quality of AML Policies and Procedures (Medium)	Comprehensiveness of AML Legal Framework	Medium Low
	Commitment and Leadership of	Medium
	Managements (Intermediate Variable)	High
	Effectiveness of Compliance Function (Organization)	Low

Pursuant to Republic Act No. 9474, lending companies are regulated and supervised by the SEC. In like manner, under Republic Act No. 8556 financing companies, including the ten (10) bank- related and five (5) quasi-bank entities, <sup>162</sup> are regulated and supervised by the SEC. Thus, they are covered persons. In relation to the AMLA, as amended, the SEC issued Memorandum Circular No. 19 on 16 September 2014, requiring lending and financing companies to submit with the SEC, the AML Operating Manual, and notarized AML Compliance Forms every three (3) years. The circular imposes fine for every day of delay of submission. The AML Compliance Form is a sworn declaration by lending and financing companies of their observance of, among others, customer identification and due diligence, record keeping, and reporting of covered and suspicious transactions reporting that must be contained in their AML operating Manual.

Memorandum Circular No. 19, Series of 2014, however, does not provide a comprehensive AML/CFT regulatory and supervisory framework. Aside from the required submission of AML Operating Manual, it does not provide details on what the operating manual should contain. Neither does it provide a process that would ensure compliance with the AMLA, as amended, and its RIRR.

The *effectiveness of compliance function* in the organization is affected by the lack of AML/CFT regulatory and supervisory framework. This is also rated low given the absence of on-site examinations due to lack of manpower.

 $<sup>^{162}</sup>$  Bank-related financing companies are examined by the BSP. Those with quasi-banking license are regulated by both the BSP and SEC.

**Commitment of leadership** is rated at **Medium** given the high entry controls despite limited AML supervision and absence of AML regulatory and supervisory framework.

	Availability and Enforcement of Criminal Sanctions	Medium High
Compliance Level of Staff	Effectiveness of Compliance Function (Organization)	Low
(Medium Low)	AML Knowledge of Business Staff	Medium
	Integrity of Business Staff	Medium

**Compliance level of staff** is rated **Low** given that internal compliance function and AML knowledge is rated **Low**.

There is low effectiveness of internal compliance function given that the supervisory authority conducts limited off-site and does not conduct on-site examinations.

As to *AML knowledge of staff*, records of the AMLC Secretariat show that only three (3) lending companies attended trainings on the reporting procedure in 2015, while there was no attendance in 2014 and 2016. For financing companies there were sixty-six (66) entities that attended the same training in 2014, twenty-eight (28) in 2015 and forty-six in 2016. Compared with the number of lending and financing companies, this turnout is minimal.

Integrity of the staff of lending and financing companies is rated at Medium considering that that the SEC has reported incidents of excessive interest rate charging, especially after a default payment. It has also a criminal case filed against certain officers of a lending company for violation of Republic Act No. 3765, also known as the Truth in Lending Act. Though the excessive interest rate charging does not constitute a crime, given the suspension of the Usury Law, and the violation of the Truth in Lending Act is not a predicate offense to money laundering, the same reflect the possibility of officers and staff members undermining AML controls. It is worth to note though that the AMLC has no reported incident of dishonesty of directors, officers and staff that would warrant investigation for possible violations of the AMLA, as amended.

*Criminal sanctions* may be imposed under the AMLA, as amended. This is without prejudice to criminal prosecutions for violation of Republic Act Nos. 9479 and 8556, as the case maybe.

Quality of CDD Framework (Medium)	Availability and Access to Beneficial Ownership information	Medium
	Availability of Reliable Identification Infrastructure	Medium
	Availability of Independent Information Sources	Medium

Very few lending companies have corporate clients. One that was interviewed disclosed that pursuant to their AML Manual, the customer identification documents required for their corporate clients includes SEC Certificate of Registration, Articles of Incorporation, updated General Information Sheet (GIS), Bureau of Internal Revenue Certificate of Registration, and Secretary's certificate of board

resolution authorizing the availment of loan, among others. Similar information about documentary requirements appears in the website of another lending company that offers business loans to corporate clients. For financing companies, the same identification documents are the basic requirements for corporate clients. This is based on information reflected in their websites, and as confirmed by a financing company that was interviewed.

The said customer identification documents, particularly the Articles of Incorporation and GIS, would show verifiable beneficial owners of the transaction.

As to a *reliable identification infrastructure*, lending and financing companies have identified verifiable identification documents (IDs) that they require from individual clients. These documents are classified as primary and secondary. The primary IDs include Social Security System (SSS) identification Document (ID), Government Service Insurance System (GSIS) ID, Postal ID, Driver's License, Professional Regulation Commission ID, Passport, and Unified Multi-Purpose ID (UMID). While the secondary IDs include Pag-ibig ID, Philhealth ID, Barangay Clearance, company ID, and payroll, among others. For high risk products, like unsecured personal loans, companies require at least two (2) primary IDs and the same number of secondary IDs.

They strictly adhere to these identified documents as the same serve as protection against fraudulent transactions. According to the SEC, the requirement for IDs serve as the reason why some borrowers continue to patronize the quick five-six lending scheme.

With respect to *independent information sources*, lending and financing companies are required to participate in the credit information system created by Republic Act No. 9510. Under the law, lending and financing companies are required to submit basic credit data and updates of their clients to the Credit Information Corporation (CIC). The submission of basic credit data includes any negative and positive credit information that tends to update the credit status of borrowers. On the part of the CIC, it is mandated to collect and disseminate to other participating entities relevant credit information that will directly address the need for reliable credit information concerning the credit standing and track record of borrowers and to regularly update the basic credit data of the borrowers on at least a quarterly basis.

	Commitment and Leadership of Managements	Medium High
Quality of Operations	Compliance Level of Staff	Medium Low
(Medium Low)	Quality of CDD Framework	Medium
	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium Low

The quality of operations can be seen on how well the sector is able to prevent the abuse of the sector for money laundering. It is a reflection of the commitment of management (**Medium High**) and the compliance level of staff (**Medium Low**). It also looks into how well the sector is able to identify and check its clients (**Medium**).

With respect to suspicious transaction monitoring, there is a considerable disparity of number of lending and financing companies, vis-à-vis with those that are registered with AMLC for suspicious transaction reporting as shown in the table below. Again, this is due to the lack of adequate oversight over the industry:

Table 6-7. AMLC Registered and Covered and Suspicious Transaction Reporting

No. of No. of Lending No. of entities No. of STRs No.

Year	No. of Lending Companies	No. of Lending Companies Registered with AMLC	No. of entities Reporting CTRs/STRs	No. of STRs Submitted to AMLC	No. of CTRs Submitted to AMLC
2014	1,633	6	4	20	24,365
2015	1,754	91	51	330	8,505
2016	Not available	11	5	1,9130	37,069
Year	No. of Financing Companies	No. of Financing Companies Registered with AMLC	No. of entities Reporting CTRs/STRs	No. of STRs Submitted to AMLC	No. of CTRs Submitted to AMLC
2014	610	288	49	1,103	71,694
2015	622	299	57	498	73,462
2016	Not Available	304	59	938	89,149

### **Lending Companies**

A look at the websites and interview of some lending institutions disclose loan products consisting of personal loan, business loan, car loan, truck loan, overseas Filipino worker (OFW) loan, salary loan, and seafarers loan, among other things. The borrowers are all local-based, except OFWs who avail of loans normally for pre-deployment expenses, as airfares and placement fees. Common among the lending institutions is the observance of customer identification and due diligence as it assures them of protection against fraudulent loans.

Loan amounts are minimal, such as PhP10,000.00 to PhP200,000.00. Higher amounts, such as car loans, are always determined based on the borrower's capacity to pay that is determined through appropriate documentation. Some loans are backed by post-dated checks and co-maker undertaking, Automated Teller Machine (ATM) card, and passbook, among others. Those that are not collateralized are guaranteed by good earning capacity of clients, based on employer certifications and pay slip, and positive credit record from CIC, credit bureaus and Credit Management Association of the Philippines.

Depending on the amount, disbursement of proceeds is done through banks, i.e. credit to borrowers' account with partner banks, and check issuance for bigger amounts; or over-the-counter cash disbursement for smaller amounts. Repayment is done through banks, partner payment centers, remittance service providers, over-the-counter payments, or collection agents.

It is noted that some lending companies offer loan processing and approval online, but the same applies only to the initial submission, on-line, of application and information for advance evaluation of credit qualification. Once approved, the client is required to personally appear before an account officer for the customer identification that includes submission duly signed application form and IDs.

Records of the regulatory authority and the AMLC do not show of any typology involving the use of lending companies for ML/TF.

# **Financing Companies**

The products of financing companies, especially most of those non-bank affiliated, cover those that lending companies offer. They also provide real estate loan, corporate loan, and educational loan, and consumer loan (for gadget, appliances, and furniture), among others. On top of these, they provide the following sophisticated products and/or services:

- i. Financial leasing which is a mode of extending credit through a non-cancellable lease contract under which the lessor purchases, at the instance of the lessee, machinery, equipment, motor vehicles, appliances, business and office machines, and other movable and immovable property in consideration of the periodic payment by the lessee of a fixed amount sufficient to amortize at least seventy percent (70%) of the purchase price, including any incidental expenses and a margin of profit over an obligatory period of not less than two (2) years during which the lessee has the right to hold and use the leased property with the right to expense the lease rental paid to the lessor and bears the cost of repairs, maintenance, insurance and preservation thereof, but with no obligation on his part to purchase the leased property from the owner-lessor at the end of the lease contract; 163
- Receivable financing which is a mode of extending credit through the purchase by, or assignment, to, a financing company of evidence of indebtedness or open accounts by discounting or factoring;<sup>164</sup>
- iii. Discounting which is a receivable financing whereby evidence of indebtedness of a third party, such as installment contracts, promissory notes, and similar instruments, are purchased by, or assigned to, a financing company in an amount or for a consideration less than their face value;<sup>165</sup>
- iv. Factoring which is a type of receivables financing whereby open account, not evidenced by a written promise to pay supported by documents such as but not limited to invoices of manufacturers and suppliers, delivery receipts and similar documents, are purchased by, or assigned to, a financing company in an amount or for a consideration less than the outstanding balance of the open accounts.<sup>166</sup>

Disbursement of loan proceeds and repayment thereof are done in the same manner as those in lending companies.

So far, there has been no reported abuse of financing companies for ML/TF.

Given the low ratings on sectoral variables associated with oversight and regulatory matters, the overall ML/TF vulnerability of the sector is **MEDIUM** 

## **ACTION PLAN**

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Adoption of SEC AML/CFT regulatory and supervisory framework for lending and financing companies	SEC	AMLC	12 months
Regular on-site and off-site examinations of lending and financing companies			12 months
Creation of an AML unit		DBM and CSC	2 years
Coordinated efforts of CGFD and AML unit about to be established		AMLC	2 years

<sup>&</sup>lt;sup>163</sup> Rules and Regulations to Implement Republic Act No. 8556 (The Financing Company Act of 1998)

<sup>164</sup> Ibid.

<sup>165</sup> Ibid.

<sup>166</sup> Ibid.

#### E. NON-BANK E-MONEY ISSUERS

BSP Circular No. 649 defines e-money as a monetary value electronically stored in convenient payment instruments that consumers can use to buy or pay for goods and services, to transfer or remit funds, and/or to withdraw funds. E-money is the latest form of non-cash payment instrument recognized by the BSP in the Philippines, and comes after checks, credit cards, debit cards and stored value cards.

As a digital channel for retail payments, an e-money account is distinct from a deposit account to safeguard public deposits. It is non-interest bearing and not covered by deposit insurance, which allows non-banks like telecommunication subsidiaries to be licensed as e-money issuers (EMIs), subject to proportionate requirements in capital (e.g., PhP100 Million minimum paid-up capital) and licensing (e.g., licensed as remittance agent).

Outsourcing and agent accreditation is possible for all non-bank EMIs, provided they remain accountable to BSP for their counterparties' adherence to applicable regulations (e.g., KYC in every cash-in/cash-out transaction of agents; reporting of covered/suspicious transactions for AML/CFT) and appropriate risk management.

To ensure liquidity, the amount of electronic values issued by EMIs must be equivalent to the actual cash in bank and liquid investments like government securities. EMIs are likewise required to establish acceptable redress mechanisms for the resolution of e-money customer complaints.<sup>167</sup>

According to the 2016 BSP report, in 2016, the volume of electronic money transactions surged to PhP1.1 Trillion, which is more than triple the PhP348-billion level in 2013.E-money transactions coursed through non-bank EMIs amounted to PhP72.1 billion in 2016 and accounted 15 percent of the total net inflow of e-money transactions. The other 85.0 percent or PhP405.7 Billion cover the e-money transactions coursed through banks.

BSP Circular No. 942 defines e-money issuer (EMI) as an entity authorized by the BSP under the Subsection X780.2 of MORB, which provides money transfer or remittance services using electronic stored money value system and similar digital financial services.

During the last assessment, the ML/TF vulnerability of the e-money sector, owing to the adequate controls in place, was **Low**.

Quality of AML	Effectiveness of Supervision/Oversight Activities	High
Supervision (Medium High )	Availability and Enforcement of Administrative Sanctions	Medium High

Non-bank EMIs are subject to the BSP's periodic and special examinations on matters relating to AML/CFT requirements and related BSP issuances. Non-bank EMIs, just like any other covered persons, are mandated to comply with the obligations under the AMLA, as amended, particularly, customer identification and due diligence, record keeping, reporting of covered and suspicious transactions, and regular training for its personnel. The BSP is authorized to conduct on-site and off-site surveillance on business relating to payment cards and/or mobile/payment systems of non-bank EMIs and service providers.

<sup>&</sup>lt;sup>167</sup> Part VII. Electronic Banking Services and Operations, MORB.

Cash-in/cash-out agents are subject to due diligence during the accreditation process conducted by non-bank EMIs. Non-bank EMIs are required to submit the list of their counterparties, including accredited agents, to the BSP. Likewise, the BSP may spot-check accredited agents during an on-site examination.

For non-compliance, e-money issuers may be subject to administrative sanctions. The administrative sanction system applied to non-bank EMIs is deemed appropriately serious to positively influence behavior of directors, officers and employees and to ensure that they maintain high AML/CFT standards.

For BSP, Circular No. 950, as amended, in relation to BSP Circular No. 649, provides for the following sanctions and penalties:

- 1. Written reprimand;
- 2. Restriction on certain licenses/product, as appropriate;
- 3. Suspension or removal from the office they are currently holding; and/or
- 4. Disqualification from holding any position in any covered institution for director/officer involved.

In addition to the non-monetary sanctions stated above, BSP may also impose monetary penalties computed in accordance with existing regulations. This is without prejudice to the power of the AMLC to impose administrative sanctions under Section 14.f of the AMLA and the Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as amended. (Section 3 of the Rules provides for a range of effective, proportionate and dissuasive administrative sanctions that depend on the gravity of violations.

Commitment and	Availability and Effectiveness of Entry Controls	Very High
Leadership of	<b>Quality of AML Supervision</b> (Intermediate Variable)	Medium High
Managements Medium High)	Availability and Enforcement of Criminal Sanctions	Medium High

**Commitment of leadership** to address ML risks is influenced by entry controls, AML supervision and criminal sanctions.

Pursuant to Section 3 of BSP Circular No. 649, all non-bank EMIs and service providers are mandated to secure approval from the BSP prior to transacting any business. They are likewise required to register with the BSP as a money transfer agent in accordance with the provisions of Section 4511N of the MORNBFI. To qualify for registration, non-bank EMIs must comply with the requirements detailed in Section 5 of BSP Circular No. 649. The PhP100 million capitalization requirement significantly impairs the entry of fly-by-night players.

**Quality of AML supervision** is rated at **Medium High** given that e-money issuers are subject to the BSP's periodic and special examinations, and are subject to a range of effective, proportionate and dissuasive administrative sanctions that depend on the gravity of violations.

With respect to *criminal sanctions*, Section 14(a)(b)(c)(d)(e) of the AMLA provides effective, proportionate and dissuasive criminal sanctions imposable both on natural and covered persons.

Quality of AMI Policies	Comprehensiveness of AML Legal Framework	High
Quality of AML Policies	Commitment and Leadership of	Medium
and Procedures (Medium High)	Managements (Intermediate Variable)	High
	Effectiveness of Compliance Function	Medium
	(Organization)	High

Primarily, BSP Circular No. 649 governs the issuance of electronic money (e-money) and the operations of EMIs in the Philippines. It places an aggregate monthly load limit of PhP100,000 on e-money, and requires EMIs to ensure compliance with AML requirements. Likewise, BSP Circular No. 950 specify requirements relating to customer due diligence (KYC), record keeping, and reporting of covered and suspicious transactions.

Further, EMIs need to adhere to all applicable law and regulations:

- Republic Act No. 10173 Data Privacy Act of 2012
- BSP Circular No. 942- Registration and operations of Remittance and Transfer Company (Remittance Agent, Remittance Platform Provider and E-Money Issuer)
- BSP Circular No. 704 Outsourcing of services by e-money issuers to e-money network service providers
- BSP Circular No. 808 Revised IT Risk Management Framework
- BSP Circular No. 859 Europay, Mastercard and Visa (EMV)<sup>168</sup> implementing guidelines
- BSP Circular No. 857 BSP Regulations on Financial Consumer Protection
- BSP Circular No. 949 Guidelines on Social Media Risk Management

**Commitment of leadership** is rated medium high given the very high effectiveness of entry controls and the conduct of regular supervision over the sector.

Internal compliance is assessed at medium high effectiveness as e-money issuers generally have risk-based and independent compliance functions, as required by the BSP. Compliance with AML rules and regulations is the primary task of the Compliance Office, headed by a compliance officer with several personnel, depending on the size, nature of operation and risk profile of the institution. The Compliance Office is responsible for ensuring compliance by the institution with the requirements under the MLPP. To this end, it has a direct reporting line to the board of directors for effective compliance reporting.

Non-bank EMIs are also required to designate two officers who are jointly responsible for the safekeeping of all records of transactions required to be retained by the AMLA, as amended. They have the obligation of making these documents readily available without delay during BSP examinations.

<sup>168</sup> International Card payment standard developed by Europay, MasterCard and Visa using chip/smart card technology. BSP issued this circular to mandate the migration of the card payment industry from magstripe technology to EMV by end of 2016.

Compliance Level of Staff (Medium)	Availability and Enforcement of Criminal Sanctions	Medium High
	Effectiveness of Compliance Function (Organization)	Medium High
	AML Knowledge of Business Staff	Medium High
	Integrity of Business Staff	High

**Compliance level of staff** to the AML legal framework and their institutional obligations is rated as Medium based on the interplay of the variables on criminal sanctions, internal compliance functions, AML knowledge and integrity of the staff.

Effectiveness of internal compliance function is rated medium high as the law sufficiently provides for a framework of compliance and e-money issuers follow this, as seen in BSP examinations. Criminal sanctions are seen as effective, proportionate and dissuasive and is imposable both on natural and covered persons.

Trainings attended by personnel of non-bank EMIs have been increasing from 2014 to 2016:

**Table 6-8. AML Trainings** 

Tuno of Institution	Voor	AMLC Data	base
Type of Institution	Year	No. of AML Trainings	No. of Participants
Non-Bank EMIs	2014	22	75
	2015	18	193
	2016	26	281

The foregoing data are in addition to the in-house trainings that non-Bank EMIs can provide to their officers, employees and external partners. In fact, they conduct a yearly training and cascading to all internal employees and external partners. They have also partnered with the AMLC for the conduct of specific AML training for external partners. Additionally, regular AML advisories are being sent-out to internal employees regarding relevant guidelines mandated by the AMLC. Further, EMIs are required to adopt and implement a comprehensive Money Laundering and Terrorist Financing Prevention Program (MLPP).

The Board of Trustees, Management and staff members are also generally regarded as having integrity to protect the interest of non-bank EMIs from known ML/TF related risks. In fact, there has been no reported incidents of any of the industry's officers and employees colluding with criminals or acting corruptly.

One of the major industry players has made compliance requirement a part of the overall Key Results Actions of each business unit in all its functions, projects and endeavours. This is to align and imbed in each of the personnel compliance with regulatory laws and regulations. For new employees, it has a stringent on-boarding process that includes AML and consumer protection training during the first week of hiring, thus ensuring their integrity.

Quality of CDD Framework	Availability and Access to Beneficial Ownership information	Medium High
	Availability of Reliable Identification Infrastructure	Medium High
( Medium)	Availability of Independent Information Sources	Medium

Since there is no available national ID system, non-bank EMIs chiefly rely on the identification document issued by an official authority in accordance with existing regulations. Some ID-issuing authorities have online verification facility to determine authenticity of IDs provided. They also rely on the usual customer identification or KYC procedures, as well as information from tipsters for the determination of beneficial ownership information.

However, it was noted there was lack of periodic monitoring and review on counterparties engaged in the conduct of KYC process such as face-to-face contact. More so, there is lax monitoring of outsourcing arrangements, particularly on the gathering of minimum information and documents of customers (incomplete information, duplicate records, and multiple customer profiles assigned to one customer). Input validation controls on batch upload processing of customer profiles in the KYC database are currently for enhancement.

Aside from the documents being submitted by their customers, non-bank EMIs use various government websites or databases such as SEC and Department of Trade and Industry (DTI) to determine if the potential partner is registered with the applicable government agency. Also, for pawnshops and MSBs, certificate of registration from BSP is required. For individual customer, EMIs utilize various AML monitoring tools, which are capable of screening customers against various local and international watch list.

	Commitment and Leadership of Managements	Medium High
Quality of	Compliance Level of Staff	Medium
Operations (Medium)	Quality of CDD Framework	Medium
	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium High

The quality of operations can be seen on how well the sector is able to prevent the abuse of the sector for money laundering. It is a reflection of the commitment of management to address ML risks in the industry (Medium High) and the compliance level of staff to AML obligations (Medium). It also looks into how well the sector is able to identify and check its clients (Medium). Quality of operations is also assessed based on the effectiveness of suspicious transaction monitoring and reporting.

Based on the dialogue with the non-bank EMIs, commissions are to be paid by customer at cash top up and/or cash withdrawal. The maximum in a month that a customer can top up to their electronic wallet is PhP100,000. This account has allowed them to send money up to a maximum of PhP50,000 per day, which can be a combination of utility bills payments, online payments, POS payments, airtime load purchases, subscription payments and ATM withdrawals. Hence, covered transactions are currently not likely in the case of non-bank EMIs. With respect to suspicious transactions, the occurrence thereof is monitored electronically.

In the case of one of the major industry players, it has established a more robust electronic AML system tool for monitoring and reporting of suspicious transactions. This is on top of the inherent controls and parameters that ensure its limited exposure, and its product, to ML/TF risks.

Below is summary of STRs filed by the two (2) major non-bank EMIs:

**Table 6-9. Suspicious Transaction Reports Filed** 

Type of Institution	Year	No. of STRs Submitted to AMLC
	2014	8
Non-bank EMI 1	2015	28
	2016	79
	2014	0
Non-bank EMI 2	2015	1
	2016	8

The total asset of non-bank EMIs is PhP17.609 Million, PhP4.477 Million, and PhP2.667 Million, as of 31 December 2014, 31 December 2015 and 31 December 2016, respectively. On the other hand, total transaction volume at the end of 2014 is PhP60.758 Million, at the end of 2015 is PhP64.875 Million, and at PhP72.147 Million the end of 2016. These assets and volume of transactions are just minimal compared to the total assets and transactions of the whole Other Financial Institutions (as shown below).

Total Assets<sup>169</sup>



Transaction Volume<sup>170</sup>

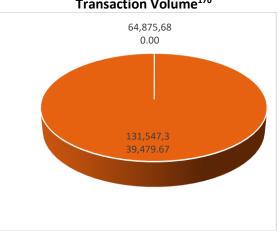


Table 6-10. Asset and Transaction Volume of EMIs

Assets							
	2016	2015	2014				
Non-Bank EMI	PhP2,667.64 (M)	PhP4,477.91 (M)	PhP17,609.50 (M)				
Other FIs		PhP438,613.272 (B)	PhP516,203.865 (B)				
Transaction Volume (in Millions)							
	2016 2015 2014						
Non-Bank EMI	PhP72,147.95 (M)	PhP64,875.68 (M)	PhP60,758.549 (M)				
NSSLAs	PhP167,180.77 (B)	PhP131,547.33 (B)	PhP142,552.46 (B)				

<sup>&</sup>lt;sup>169</sup> Based on the 2015 data on assets size.

<sup>&</sup>lt;sup>170</sup> Based on the 2015 data on transaction volume of Non-Bank EMI and NSSLAs. Only NSSLAs have available data on transactions volume.

Likewise, the number of STRs filed by the sector is relatively low as against the total e-money transactions.

The channels utilized to facilitate top up and/or withdrawal on electronic wallet are pawnshops, MSBs and other registered remittance agents. Non-bank EMIs remain accountable for their counterparties' adherence to applicable AMLT/CFT regulations (e.g., KYC in every cash-in/cash-out transaction of agents; reporting of covered/suspicious transactions for AML) and appropriate risk management. This contributes to the reduction of the risk of illicit funds being introduced into the financial system.

Further, the BSP placed an aggregate monthly load limit on e-money instruments amounting to PhP100,000. This account has allowed them to send money up to a maximum of PhP50,000 per day, which can be a combination of utility bills payments, online payments, POS payments, airtime load purchases, subscription payments and ATM withdrawals. These limits, both on the daily transactional amount and monthly top-up value deter potential money launderers. Hence, although transactions carried out in this sector are highly cash-intensive but, it is of relatively of small value.

The structure of the EMI business coupled with strict regulations issued by the BSP make it naturally not prone to ML transactions. This indicates the effectiveness of the framework of AML/CFT for emoney services.

Further, as per BSP Circular No. 649, e-money issuers are required to operate using Philippine currency, which may be used for domestic transactions only. Thus, majority of non-bank EMI's regular clients include local customers. The existence of cross-border transactions, which could expose the sector to TF risks, is not a concern, with the possibility for terrorist funds being channeled using e-money transfer very unlikely.

Hence, because of the strict regulation and supervision of the BSP, coupled with rigid obligations imposed under the AMLA, as amended, ML and TF risks for non-bank EMIs are relatively low.

All the transactions of this sector are handled by the majority of local customers and are cashintensive, but relatively of small value. The volume of transaction and the number of customers are increasing. Control measures are at a satisfactory level.

## Other vulnerable factors of EMIs

This variable assesses identified risks associated in the issuance of e-money as compared with cash.

- a. Anonymity
- b. Elusiveness
- c. Rapidity
- d. Lack of Oversight

In response to the aforementioned risks, regulators, as well as e-money issuers and service providers, collaborated in the implementation of sufficient controls as shown in the table below:

Table 6-11. Identified Risks and Controls of Cash vs. E-Money

Risk Type	Cash	E-Money	Controls
<b>Anonymity</b> - lack of identity of the customer	Anonymous	I -	KYC required during registration and/or when a transaction is allowed

Risk Type	Cash	E-Money	Controls
		that can trace and record transactions.	Transaction records secured and stored both electronically and physically for a minimum of 5 years
Elusiveness - to avoid the tracing of the origin of funds funneled through the financial system/ economy	Untraceable	E-money transactions are clearly traceable in the system. The unique handset ID, time, and amount of transactions are known.	Aggregate load limit of PhP100,000 per month.  Robust risk alert reporting system which includes, among others, velocity checks, trend analysis, and customer profiling
Rapidity - the speed by which funds are moved from one person to another	Slow due to the nature of cash which needs to be transported physically.	Over the distance, the electronic character of e-money can move transactions more effortlessly than cash. Rapidity is the biggest risk factor in e-money services in cases where there are no automated internal controls.	Aggregate load limit of PhP100,000 per month  Robust risk alert reporting system which includes, among others, velocity checks, trend analysis, and customer profiling  Real-time blocking and suspension of e-money transactions and accounts.
Lack of Oversight - failure to review, monitor, and supervise programs, activities, and policies governing e-money issuers	Difficulty in performing oversight activities in regulating the movement of physical cash	E-money issuers are regulated by the BSP.	Issuance of applicable regulations on e-money issuers (i.e., BSP Circular Nos. 471, 649, 704, 706, 808, 859, and AMLA RIRR)  Periodic audits conducted by the BSP

Additionally, e-money issuers are now exploring the use of social media platforms as channel to deliver their services to customers. Notable functionalities being currently utilized by e-money issuers and providers are video chat technology for the conduct of face-to-face KYC, and pay bill transaction using FB Messenger. This new channel could result to new challenges innate with the use of technology for certain processes.

In sum, the ML/TF vulnerability of non-bank EMIs is **MEDIUM**.

# **ACTION PLAN**

Taking into consideration the identified deficiencies in controls of EMIs, the following are the recommended actions:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Hold workshops for risk assessment and needed	AMLC		1 year
tools to standardize AML/CFT framework for		BSP	
covered persons			
Study the possibility of a central repository of PEP,	AMLC		
associates immediate family members, etc.		BSP	

Enhance licensing framework of non-bank EMIs to	BSP		2 <sup>nd</sup>
ensure that they will operate in a sound and secure		AMLC	semester,
manner			2017
Require additional details in the quarterly EMI	BSP		2 <sup>nd</sup>
Report beings submitted to BSP to have more			semester,
visibility on the status of operation of EMIs and		AMLC	2018
determine the level of remittances coursed through			
non-bank EMIs that are being used for ML/TF			
Provide periodic repository report on local ML/TF	AMLC	BSP	
Trends			
Set more refined red flags, including acceptable	AMLC	BSP	
ranges for thresholds, in line with parameter setting			

### VII. DESIGNATED NON-FINANCIAL BUSINESS AND PROFESSIONS

### **EXECUTIVE SUMMARY**

AML Combating controls	Casino	Lawyers and Notaries	Accountants	Dealers in Precious Metals	Company Service Providers	Car Dealers	Real Estate
Quality of General AML Controls	L	ML	ML	ML	L	L	L
Quality of Operations	ML	ML	ML	ML	L	L	L
Quality of AML Policies and Procedures	L	ML	ML	ML	ML	L	L
Quality of CDD Framework	МН	ML	М	L	ML	М	М
Compliance Level of Staff	ML	ML	ML	ML	M	L	L
Quality of AML Supervision	DNE	DNE	DNE	L	DNE	DNE	DNE
Commitment and Leadership of Management	ML	ML	ML	ML	L	L	ML
Inherent Vulnerability	Н	М	М	М	МН	М	М
Final Vulnerability	H	M	M	M	M	M	M

(H=High, MH=Medium High, M=Medium, ML=Medium Low, L=Low, DNE=Does Not Exist)

In 2013, R.A. No. 9160, or the "Anti-Money Laundering Act of 2001" was amended by R.A. No. 10365, thereby extending AML/CFT obligations to Designated Non-Financial Businesses and Professions ("DNFBPs"). The current legislation was able to include the dealers of precious metals and stones, lawyers and accountants, as well as company service providers under the country's AML Regime.

The first NRA's recommended action plan was to address the identified weaknesses by issuing implementing rules and regulations specific to DNFBPs. It was also part of the plan to further amend the AMLA to bring the casino, real estate brokers, and car dealers within the Philippines' AML regime.

The action plan was partially implemented when the President signed into law Republic Act No. 10927, designating casinos as covered persons under the AMLA, on 14 July 2017. A bill to include real estate brokers and dealers of high value items is still pending before the Senate of the Philippines.

Although the Revised Implementing Rules and Regulation (RIRRs) of the AMLA was issued, specific provisions for the DNFBPs were not included. Thus, the identified weaknesses of the covered DNFBPs remain. In fact, no significant changes were noted between the previous and this NRA. Only a slight improvement was noted on the real estate sector and on the dealers of precious metals and stones.

In this assessment, the following DNFBPs were examined and assessed:

Table 7-1. COMPARATIVE SUMMARY OF ASSESSMENT

SECTOR	VULNERABILITY			
	1 <sup>st</sup> NRA	2 <sup>nd</sup> NRA		
Casino	Very High	High		
Dealers in Precious Metals and Stones (DPMS)	Medium High	Medium		
Lawyers and Notaries	Medium	Medium		
Accountants	Medium	Medium		
Trust Companies	(Banks) Low	(Banks)		
Company Service Providers (CSPs)	Medium	Medium		
Car Dealers	Medium High	Medium		
Real Estate	Medium High	Medium		

The change in the casino sector's vulnerability rating from **VERY HIGH** to **HIGH** does not translate to a significant decrease in ML vulnerability.

The high vulnerability rating can be attributed to the inherent vulnerabilities and insufficient AML/CFT legal framework.

Casino gross gaming revenue represents around 5% of the annual budget of the government. Thus, the sector is very important and must be protected from criminal exploitation.

The following are some of the variables that increase the vulnerability of the casino sector:

- clients are usually those who have high net worth and are non-resident;
- transactions are usually done in cash;
- existence of proxy betting; and
- availability of non-face to face transactions.

The real estate sector has improved from its previous NRA rating of **MEDIUM HIGH** to **MEDIUM**. The improvement in the rating can be attributed to the latest data gathered from the Bangko Sentral Ng Pilipinas (BSP) where data show that majority of the real estate transactions are purchased through the real estate loan facilities of banks. Real estate transactions through banks are covered by their existing AML/CFT preventive programs. Thus, money laundering threats are mitigated.

A difference in rating the following variables across the different DNFBPS sector are based on the capacity and capability of the different sectors to access proprietary database or organization database as well as the inability of others to access any third party reliable source of identification and transaction database. Like for casinos, they have the capacity to engage the services of third party service providers, database, and can share information with other operators. While lawyers and accountants may have some issues regarding confidentiality of information that is inherent to the profession. On the other hand, DPMS has no available database and they also do not share information with other dealers. Car dealers have better rating because they are usually in partnership with covered financial institutions and therefore have access to personal information and financial transactions.

Table 7-2. Customer Due Diligence (CDD) Framework AML Controls

AML Controls	Casino	Lawyers	Accountants	Dealers in PM&S (DPMS)	CSP	Car Dealers
Availability and Access to Beneficial Ownership Information	МН	L	ML	L	ML	М
Availability Reliable Identification Infrastructure	Н	МН	МН	L	ML	МН
Availability of Independent Information Sources	VH	DNE	DNE	Close to Nothing	L	L

#### DATA AND INFORMATION COLLECTION

The data and information used in this assessment were collected from the following sources:

- A. Applicable laws, rules, guidelines, manuals and circulars
- B. Documents from different supervising authorities:
  - a. Annual Reports
  - b. Audited Financial Statements
  - c. Submissions of AMLC
- C. Data available at the Anti-Money Laundering Council Secretariat
- D. Open Sources:
  - a. News articles
  - b. Press releases
  - c. Internet articles

### E. Interview

Meetings, consultations, round table discussions, and phone interviews were conducted with the different stakeholders to validate information and to secure additional data and/or information.

# **LEGAL FRAMEWORK**

On 23 July 2012, Republic Act No. 10365 was approved by Congress. The legislation further amended Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act of 2001, as amended (AMLA), and included some Designated Non-Financial Business and Profession (DNFBP) under the coverage of the Philippines AML/CFT regime.

Under Section 3(a) of the said law, the following Designated Non-Financial Business and Professions (DNFBPs) were included under the coverage of the AMLA:

- "(4) jewelry dealers in precious metals, who, as a business, trade in precious metals, for transactions in excess of one million pesos (PhP1,000,000.00);
- (5) jewelry dealers in precious stones, who, as a business, trade in precious stones, for transactions in excess of one million pesos (PhP1,000,000.00);

- (6) company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; and
  - (7) persons who provide any of the following services:
    - i. Managing of client money, securities or other assets;
    - ii. Management of bank, savings or securities accounts;
    - iii. Organization of contributions for the creation, operation or management of companies; and
    - iv. Creation, operation or management of juridical persons or arrangements, and buying and selling business entities."

On 4 November 2017, the Implementing Rules and Regulation of R.A. No. 10927, the law designating casino as covered person under the AMLA, took effect. For easy reference, the Implementing Rules and Regulations is also known as the Casino Implementing Rules and Regulations (CIRR).

The Financial Action Task Force<sup>171</sup> (FATF) defines DNFBP as:

"Designated non-financial businesses and professions means:

- a) Casinos
- b) Real estate agents.
- c) Dealers in precious metals.
- d) Dealers in precious stones.
- e) Lawyers, notaries, other independent legal professionals and accountants this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.
- f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
  - i. acting as a formation agent of legal persons;
  - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

<sup>&</sup>lt;sup>171</sup> The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

- iii. providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- iv. acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; and
- v. acting as (or arranging for another person to act as) a nominee shareholder for another person."

### A. CASINO SECTOR

### **INTRODUCTION**

The vulnerability of casinos was recognized in the revision of the FATF 40 Recommendations, with obligations on casinos being significantly enhanced.

There is significant global casino activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. This assessment identifies significant gaps in awareness of money laundering (ML), gaps in regulatory and law enforcement responses, issues with controls over junkets / VIP programs.

The nature of the casino sector presents a number of challenges for AML implementation. Some of the challenges would include the following:

- Casinos are cash intensive business, often operating 24hrs per day, with high volumes of cash transactions taking place very quickly.
- Casinos offer financial services such as account remittance, foreign exchange, credit facilities, cash issuing, etc., but they are not regulated as financial institutions.
- The movement of funds associated with gaming-related tourism is poorly understood and may pose particular money laundering risk particularly on international movement of funds for casino junket operators.
- Casino staffs lacks competencies in detecting possible money laundering activities as a result of the absence of AML training programs.

There are currently three (3) government agencies in the Philippines that are authorized to engage in the operations and/or the regulation of both land and internet based casinos, the Philippine Amusement and Gaming Corporation (PAGCOR), Cagayan Economic Zone Authority (CEZA), and Aurora Pacific Economic Zone and Freeport (APECO).

# PHILIPPINE AMUSEMENT AND GAMING CORPORATION (PAGCOR)

The Philippine Amusement and Gaming Corporation (PAGCOR) is a wholly-owned government corporation created on January 1, 1977 by virtue of Presidential Decree (PD) No. 1067-A, which was later amended by PD Nos. 1067-B, 1067-C, 1399 and 1632. These were subsequently consolidated into one statute on July 11, 1983 under PD No. 1869, also known as the PAGCOR's Charter where PAGCOR was given the power to grant license to private operators. The 25-year franchise of PAGCOR expired on July 11, 2008. However, this was renewed by Congress for another 25 years, or until July 11, 2033, under Republic Act (RA) No. 9487. The authority of PAGCOR covers the whole Philippine archipelago except those that are within the jurisdiction of Cagayan Economic Zone Authority (CEZA) and Aurora Pacific Economic Zone and Freeport (APECO).

The three-pronged mandates of PAGCOR are:

- 1. to regulate all games of chance, particularly casino gaming in the country;
- 2. to raise funds for the government's socio-civic and national developmental efforts; and
- 3. to help boost the country's tourism industry.

In accordance with its Charter and other government laws, PAGCOR earnings are distributed as follows:

- 5 percent of winnings goes to the Bureau of Internal Revenue (BIR) as franchise tax;
- 50 percent of the 95 percent balance goes to the National Treasury as the National Government's mandated income share;
- 5 percent of the remaining balance after deducting the franchise tax and the National Government's mandated income share goes to the Philippine Sports Commission to finance the country's sports development programs;
- 1 percent of the net income goes to the Board of Claims, an agency under the Department of Justice, to compensate victims of wrongful detention and prosecution; and
- Cities hosting PAGCOR casinos are given fixed amount for their respective community development projects.

Aside from these, PAGCOR has also been tapped to provide funds for the implementation of vital laws such as the Early Childhood Care and Development program which promotes "the rights of children to survival, development and special protection with full recognition of the nature of childhood and its special needs."

PAGCOR also funds the Sports Benefits and Incentives Act which provides monetary rewards to athletes and coaches who win in international sports competitions. It likewise supports the National Cultural Heritage Act of 2009 which provides PAGCOR's mandatory funding.

On top of its mandatory remittances to various government entities, the state run gaming firm has also been actively implementing its own major Corporate Social Responsibility projects.

# **CAGAYAN ECONOMIC ZONE AUTHORITY (CEZA)**

Cagayan Economic Zone Authority (CEZA) is a government-owned and controlled corporation created under Republic Act No. 7922. CEZA is also known as Cagayan Freeport or Cagayan Cyber Park, and is located in the Northeast of the Philippines. CEZA possesses the power to operate on its own, either directly or through a subsidiary entity, or license to others. Tourism-related activities, including games, amusements, recreational and sports facilities such as horse racing, dog racing, gambling casinos, online casinos, golf courses, online gaming, and others are under priorities and standards set by the CEZA. CEZA is a government unit under the Office of the President that operates and manages the 50,000-hectare economic zone in Cagayan.

Casino gaming is regulated by CEZA through its mother licensor. To expedite the processing of gaming licenses, CEZA has the legal authority to independently approve applications without the prior acceptance from a national government agency, including PAGCOR. In fact, 90% of the locators in Cagayan's cyber park engage in gaming operations. Through virtual gaming or online gaming, clients may play the games through proxies without need of physical presence. CEZA issues internet gaming

licenses targeted toward international players. This has become an attractive business model for online gaming operators in Asian markets and the international gaming community. A number of local and foreign-owned online gaming companies have registered with CEZA including online casinos, online gambling, online betting, and more.<sup>172</sup>

To facilitate the efficient management and regulation of internet gaming, CEZA executed a License Agreement with First Cagayan Leisure and Resort Corporation (First Cagayan).

First Cagayan is a corporation duly organized and existing under and by virtue of the laws of the Republic of the Philippines and is a Cagayan Special Economic Zone and Freeport (CSEZPF) registered enterprise. It is at the forefront of the development of the gaming infrastructure in the Cagayan Special Economic Zone pursuant to Section 6 (f) of Republic Act No. 7922 (Cagayan Special Economic Zone Act.)

The License Agreement authorizes First Cagayan to develop, operate, and conduct internet and gaming enterprise and facilities in the CSEZPF and to have a "Master Licensor Certificate". The Certificate certifies that First Cagayan is duly authorized to regulate and monitor, on behalf of CEZA, all activities pertaining to the licensing and operation of interactive games, in accordance with the Interactive Gaming Act (2003).<sup>173</sup> Licenses are available for all forms of interactive gaming including: casinos, sports betting, lottery and lotteries.<sup>174</sup>

As of year-end of 2016, First Cagayan's roster of online licensees was 138. Based on the License Agreement First Cagayan has to pay CEZA the amount of P847,085,501, P718,467,635, and P605,002,530 in 2016, 2015, and 2014, respectively, representing 1% of the monthly gross winnings.

Licensees of CEZA, however, are not allowed to accept bets or wagers from the United States of America, Singapore and the Republic of the Philippines.<sup>175</sup>

For land based casino operations, CEZA entered into an agreement with North Cagayan Gaming & Amusement Corporation (NCGAC) to establish, operate and to supervise gaming-related activities of its appointed operators and/or agents.

The NCGAC is a privately owned corporation organized under the laws of the Republic of the Philippines. NCGAC has been licensed by the CEZA to establish and operate all forms of gaming enterprises and gaming support service facilities in the CSEZFP.

Under its license agreement with CEZA, NCGAC is also authorized to appoint suitable operators and/or agents and supervise their gaming and gaming-related activities.

NCGAC provides land based and online gaming, proxy betting, video streaming, and gaming support services. 176

Gaming operators and entities operating in the Zone enjoys numerous benefits and incentives inherent in Cagayan Economic Zone Authority (CEZA) registered enterprises - including the potential of positioning themselves as lead players in the Zone's ensuing global connectivity.<sup>177</sup>

<sup>&</sup>lt;sup>172</sup> http://kittelsoncarpo.com/tax-incentives/ceza/. Visited on 10 August 2017.

<sup>&</sup>lt;sup>173</sup> Consolidated Financial Statement of Leisure and Resorts World Corporation and Subsidiaries.

<sup>&</sup>lt;sup>174</sup> http://www.firstcagayan.com/fclrc/egaming.php. Visited on 9 August 2017.

<sup>&</sup>lt;sup>175</sup> http://www.firstcagayan.com/fclrc/operators.php. Visited on 10 August 2017.

http://www.northcagayan.com/, Visited on 27 September 2017.

<sup>&</sup>lt;sup>177</sup> http://www.firstcagayan.com/fclrc/index.php. Visited on 9 August 2017.

# **AURORA SPECIAL ECONOMIC ZONE AUTHORITY (APECO)**

The Aurora Pacific Economic Zone and Freeport, also known as APECO, was established by virtue of Republic Act No. 9490, otherwise known as the Aurora Special Economic Zone Act of 2007. It is being supervised and managed by the Aurora Pacific Economic Zone and Freeport Authority into a self-sustaining industrial, commercial, financial, and recreational center, with a suitable residential area, in order to create employment opportunities around Casiguran, and to effectively encourage and attract legitimate and productive local and foreign investments.<sup>178</sup>

APECO is authorized by law to operate on its own, either directly or through a subsidiary entity, or concession or license to others, tourism-related activities, including games, amusements and nature parks, recreational and sports facilities such as casinos, online game facilities, and golf courses.

Sometime in May 2016, APECO selected Pacific Seaboard Leisure and Entertainment as its master licensor (on-line and land-based) which will focus initially on issuing online gaming licenses. It aims to challenge the existing hubs of Manila and the Cagayan Economic Zone Authority, where First Cagayan Leisure and Resort Corp is overseeing a similar role. APECO said that, at later date, they will also venture on land-based casinos.

The cost of online operation will be US\$40,000 each year both for online casinos and live dealer gaming. Gaming tax will be set at two per cent of Gross Gaming Revenue or a US\$5,000-minimum levy per table. 179

### **Internet Casino**

Internet Casinos offered by licensees are not accessible in the Philippines and Filipinos are not allowed to participate wherever they may be located. PAGCOR, CEZA, and APECO, issue licenses to internet casino and internet casino service providers who operate in the Philippines. Licensees are either registered domestic companies or foreign registered companies with appointed domestic agents. Internet casinos are those who provide casino games including the receipt of bets/wagers and paying out of winnings while casino service providers are those who provide component services of internet casinos such as marketing support, server hosting, internet connectivity infrastructure, gaming software/platform, data/content and video streaming and other business process outsourcing services related to online or internet gaming activities.

### E-games

E-games or electronic gaming is an online gaming platform being offered by PAGCOR to online players in the Philippines. PAGCOR is an operator, regulator and e-games license issuer. E-games is the conduct of virtual games of chance, i.e. casino games and mixed games of chance and skill, and the taking of wagers through any computer or communication device connected to the internet or the use of internet-based technology and other communication devices that are necessary for gaming operations.

There are 196 e-games gaming site nationwide as of 31 December 2016. E-games are provided through a close system or are being played inside registered salons or e-game cafés. E-games providers have to comply with certain regulations such as the location of the establishment. Gaming

https://en.wikipedia.org/wiki/Aurora\_Pacific\_Economic\_Zone\_and\_Freeport#cite\_note-2. Retrieved 10 August 2017.

http://www.g3newswire.com/philippines-aurora-pacific-economic-zone-offer-online-licences-philippines/. Visited on 9 August 2017.

is regulated by PAGCOR and they are required to comply with an approved gaming manual which covers customer identification and record keeping, among others.

#### SECTOR VULNERABILITY ASSESSMENT

As of period covered by the 2<sup>nd</sup> NRA, the legal framework is not yet completed. Hence, some variables are considered "does not exist" given that there was no legal basis for the sector to adopt AML/CFT measures.

The assessment made is based on open source, official documents and data provided by the regulators. Interviews were also conducted on the officers of PAGCOR and First Cagayan. For APECO and CEZA, however, the data was sourced from open sources and official documents.

After considering the data gathered, the overall vulnerability of the casino sector is at HIGH.

Quality of CDD Framework (Medium High)	Availability and Access to Beneficial Ownership Information	Medium High
	Availability of Reliable Identification Infrastructure	High
	Availability of Independent Information Sources	Very High

### **Beneficial Ownership Information**

For casino patrons playing under junket arrangement, the actual players are required to undergo a system of customer identification process. All junket players are required to submit their passports for identification. As a procedure, junket players are required to submit their passports prior to their arrival or at least before they are allowed to play. Should the junket operators fail to submit to the casino and to the regulator a copy of junket players' passports before they play, they are only given a number of days to perform a late submission, otherwise, they will be subjected to corrective actions.

Junket operators are also required to undergo a system of fit and proper screening and in the process, individuals having interest in the junket company are identified and are also required to pass the fit and proper screening which includes criminality check.

Some casino offers proxy betting facilities; however, the proxy has to undergo the mandatory customer identification process first before they are allowed to participate remotely.

As regard to beneficial owners of casino operators, casinos and other gaming operators are required to register their company name with the appropriate government agencies before they can apply for a gaming license with their respective Supervising Authorities (SAs).

Company registry for corporations, Securities and Exchange Commission, require applicants to provide the list of the names of the shareholders and officers together with the amount of ownership in the company.

The applicants and license holders of casino gaming license must pass the standard probity check for suitability and to comply with all the documentary requirements of the SAs. The submission of a Personal Disclosure Statement is mandatory for all sole proprietor, partner, and board of directors of

all licensed casinos and casino license applicants. This requirement requires all casinos to disclose their beneficial owners.

A foreign national is not allowed to own a gaming site. If the foreigner will be a partner or shareholder of a partnership or a corporation, he/she must comply with the requirements of the Foreign Investments Acts of 1991, as amended.

The applicant has to undergo the strict background check that would require, among others, the declaration of any beneficial owner/s of a company being registered including other beneficial owners of corporations registered as stockholders up to the last level.

Applicants are even required to execute certain disclosures such as the disclosure of any litigation against the company and/or self.

# Reliable Identification Infrastructure

The Philippines do not have a national identification system. This, however, does not affect the efficiency of the casino operators to properly identify their players or patrons. In fact, no incident on the use of fake identification document has been reported by the gaming industry.

Patrons of casinos are required to present a government issued ID or a passport to comply with the identification requirements in joining membership programs of casino operators.

Further, casino operators have direct access to wide sources of information for identification process, such as international affiliate's database, proprietary database, and they can validate with other operators the identity of certain individuals, particularly those who are considered as high rollers which pose more risk for possible money laundering activities.

For foreign players, the operators are using a technology where information from the passports are read by their machine and are automatically logged in their casino management system and are crossed checked against any negative list.

# **Independent Information Sources**

Casino operators share information which are comprehensive enough as a source of historical financial information of clients.

The information can be accessed through database or can be inquired or requested via phone call or e-mail. The practice of exchanging financial history of casino clients is a part of their operation to make sure that clients are capable of paying any loans that may be extended by the operators and to make sure that they are playing within their profile.

### **PREVAILING PRACTICES**

A. Customer Identification and Verification (Know -your-customer Rule)

Even in the absence of AML casino regulations, casinos undertake a certain degree of know-your-customer procedures.

For casino patrons who are not playing on junket tables, customer identification is optional. According to the casino officers who were interviewed, players choose to

register with casino membership programs to avail of different promotional offers, in this case, patrons are required to present a valid government issued ID.

On the other hand, players on the junket tables are required to present their passports and undergo a certain level of customer identification and in some cases customer due diligence for purposes of extending credit. The customer information is saved on a database and are shared with the SAs.

For players of e-games, mandatory customer identification is required and a government issued id must be presented.

### B. Reporting of Covered and Suspicious Transactions

Casinos are not yet covered by the AML legal framework and are not required to file reports.

### C. Record Keeping

Although casinos are not yet covered by the AML legal framework, they are keeping customer information and transaction record for a minimum of six (6) years.

Compliance Level of Staff (Medium Low)	Effectiveness of Compliance Function	Does not exist
	Availability and Enforcement of Criminal Sanctions	Medium
	Integrity of Business/Profession Staff	High
	AML Knowledge of Business/Profession Staff	Low

Casinos are not considered as covered persons under the AMLA as of the period covered in this report. As such, the Compliance Function (Organization) for the Casino sector cannot be assessed at this moment.

# **Criminal Sanctions**

The Philippines has a legal framework that has sufficient criminal sanctions for money laundering and ancillary offenses that are dissuasive that would positively influence individual behavior patterns.

Existing AML law provides for an imprisonment of up to fourteen (14) years and a fine of not more than 200% of the money laundered as well as administrative penalty of not more than Five Hundred Thousand (500,000) pesos.

The AML legal framework applies to all individual who may commit money laundering and predicate offenses. Unfortunately, since casinos are not yet covered by the legal framework, it does not cover officers and employees of casinos should they fail to comply with Customer Due Diligence, Record Keeping, and Reporting requirements of the Anti-Money Laundering Act of the Philippines.

Sometime in March and April of 2016, cases of money laundering have been filed against bank officials and casino junket operators in relation to the US\$81 million representing a part of the proceeds of the Bangladesh heist, which was allegedly laundered in the casino.

# **Integrity of Business/Profession Staff**

Casinos have a very low incident wherein their staff are caught conspiring with criminals to undertake criminal activities or engaging in criminal activities within its premises.

Casino operators disclosed in one of the meetings, together with PAGCOR, that they are implementing a policy that criminal complaints are immediately filed against any employees who are caught conspiring with criminals or are engaged in criminal activities in the casino premises. The casino operators maintain a good relationship with law enforcement and give full cooperation in any criminal investigation that may involve their casinos and/or employees. In addition, employees of PAGCOR licensed casinos are required to secure a Gaming Employment License<sup>180</sup> (GEL) from PAGCOR, to check their capacity, competence, and integrity to ensure that they are able to uphold global gaming standards, before they are allowed to work in gaming related position. The GEL requirements are required for all executive, managerial, supervisory, and rank and file employees.

Under the GEL, the license shall be revoked under the following circumstances, in addition to other just and authorize causes under the Philippine Labor Laws:

- Game cheating;
- Fraud and/or estafa;
- Theft;
- Forgery or counterfeiting;
- Unlawful interference with a gaming equipment;
- Conviction of a crime involving moral turpitude;
- Use of camera or any electronic device to assist in projecting outcome of game;
- Acts of dishonesty amounting to grave or serious misconduct; and
- Violation of employment contract provision/policy on prohibition from playing in a gaming establishment.

On the other hand, PAGCOR's casino licensees' Board of Directors or their Nominees are required to submit, on an annual basis, as discussed above.

Mechanisms on the reporting of suspicious transaction including the protection of employees against any negative effect of reporting are not present.

# AML Knowledge of Business/Profession Staff

Some of the casino operators have existing AML training programs. The training programs, however, are limited to general principles of money laundering and do not include compliance requirements because of the lack of legal framework.

For some casino operators, the training programs are limited to key officials and senior officials only. Some are exerting efforts that trainings are provided to all employees.

Based on the interview, majority of the casino operators are aware of the vulnerability of some of their services to money laundering, while few are not.

<sup>&</sup>lt;sup>180</sup> Gaming Employment License, Handbook for Applicants and Employees, Version 2, April 2016.

On the other hand, employees of casinos handling supervisory function and up have AML/CFT knowledge, since most of them have previously worked for casinos in other jurisdictions who have AML/CFT legal framework. Further, there is a licensed casino who is an affiliate of a foreign casino and are required to comply with certain AML/CFT regulation. Considering, however, that casinos are not covered by AML/CFT compliance they are not required to comply with the AMLA. Consequently, AML/CFT knowledge in the casino sector is limited to few individuals.

Generally, however, AML training program cannot be made as a mandatory requirement due to lack of AML legal framework.

	Commitment AML		Effectiveness of Supervision/ Oversight Activities	Does not exist	
Quality of	and Leadership of Management		Does not	Availability and Enforcement of Administrative Sanctions	Does not exist
AML Policies and	(Medium Low)	Availability and Effectiveness of Entry Controls		High	
Procedures (Low)		Availability an	nd Enforcement of Criminal	Medium	
	Comprehensiv	veness of AML Legal Framework		Low	
	Effectiveness	Effectiveness of Compliance Function			

# <u>AML Legal Framework, AML Supervision/Oversight Activities, Administrative Sanctions, AML Compliance</u>

With the recent AMLA amendment and its implementing rules and regulation taking effect, casinos are now included as a covered person under the Philippines AML regime. The casino supervising authorities and the AMLC, however, are yet to issue guidelines that would complete the legal and regulatory AML framework of the casino sector. As such, the variables Comprehensiveness of AML Legal Framework is rated as Low, while Effectiveness of Supervision/Oversight Activities, Availability and Enforcement of Administrative Sanctions, Effectiveness of Compliance Function (Organization), including suspicious activity monitoring and reporting, are considered as "does not exist."

Specific guidelines are needed to effectively implement the legal framework covering AML preventive measures, AML supervision of casinos, as well as administrative sanctions in case of non-compliance. Procedures and guidelines for casino transaction monitoring and reporting of suspicious activities are yet to be issued by the supervisors and AMLC. Some of the licensees, however, have existing Casino Management System (CMS) that has AML monitoring system that can be configured, based on the requirements of the regulations that will be implemented by the AMLC and/or by the casino Supervising Authorities, to assist in the monitoring and reporting of Suspicious Activities.

As of writing, casinos are also not yet required to institute AML/CFT compliance measures. There is one licensee however which observes global compliance as this is a requirement of its mother company. As such, it has an existing AML internal compliance program although it is couched in general terms due to the incomplete AML legal framework in the country. All other licensees adopt only the brands of their mother companies, and are not required to observe global compliance.

Similarly, all other casino operators do not have internal compliance measures as there is no law mandating them to adopt one.

The bill that included the casino within the coverage of the Anti-Money Laundering regime of the country was only signed into law on 14 July 2017 and became effective on 29 July 2017, fifteen (15) days after publication in the Official Gazette. The corresponding implementing rules and regulation issued by the Anti-Money Laundering Council together with the appropriate government agencies became effective on 4 November 2017

# **Effectiveness of Entry Controls**

The Supervising Authorities has existing rules and regulation that has a fit and proper requirement to prevent criminals and their associates from being granted with license to operate casinos.

Supervising Authorities even engage the services of a third-party service provider to validate, vet, and conduct further due diligence. PAGCOR for example sets probity standards and measures to establish integrity, financial soundness, business ability and the suitability of those who are charged with the authority to control the licensees' operation. Under its guidelines, the Board of directors, partners and sole proprietors are required to submit and update their Personal Disclosure Statement (PDS) on an annual basis. Although this measure is not designed for AML/CFT compliance, it is a measure that would mitigate the possibility that criminals will be able to operate casinos.

Supervising Authorities, however, does not have the appropriate powers and sufficient staff and other resources to carryout AML function over their licensees because of the absence of legal and regulatory framework.

Also, existing entry policies does not have AML controls integrated with it and officers of the casinos are not required to possess AML understanding.

	Commitment and Leadership of Management	Medium Low
Quality of Operations	Compliance Level of Staff	Medium Low
(Medium Low)	Quality of CDD Framework	Medium High
	Effectiveness of Suspicious Activity Monitoring	Does Not Exist

### **Suspicious Activity Monitoring**

Casinos are considered as covered persons under the AMLA only on 14 July 2017, and thus no covered or suspicious transaction reports have been submitted for the period covered under the assessment.

Commitment and leadership of management, compliance level of staff and quality of CDD framework are all assessed in the above section.

<sup>181</sup> Responsible Gaming, Code of Practice, Version 5, Gaming and Licensing Development Department, March 2017.

#### INHERENT VULNERABILITY ASSESSMENT

The vulnerability factors assess the inherent factors that are specific to the casino sector. These factors are also called "inherent vulnerability variables". The following identified vulnerability factors have a specific impact on the assessment of AML vulnerability of the sector:

- 1. Total Size/Volume of the Business
- 2. Client Base Profile of the Business
- 3. Level of Cash Activity in the Profession
- 4. Use of Agents in the Profession
- 5. Possible Anonymous Use of the Product in the Profession
- 6. Difficulty in tracing the transaction records
- 7. Existence of ML Typologies on the Abuse of the Profession
- 8. Use of the Profession in Fraud or Tax Evasion Schemes
- 9. Non-face-to-face Use of the Product in the Profession
- 10. Cross-border international transaction

Information on these factors was obtained from the reports submitted by the regulators, open source, and from the meetings that were conducted for the purpose.

### 1. Total Size/Volume of the Business

This variable assesses the total turnover or the total value or amount of transactions handled by a particular business, which is indicative of the level of ML vulnerability that this business can introduce into DNFBP sector if the relevant risks are not mitigated.

#### 2. Client Base Profile of the Business

This variable assesses whether the type of client that generally uses the business being assessed increases the risks of money laundering abuse of the assessed business.

### 3. Level of Cash Activity in the Profession

This variable assesses the level of cash activity associated with a specific business, both whether the use of cash is permitted and to what extent that occurs.

# 4. Use of Agents in the Profession

ML vulnerability may be increased due to the weak AML systems of the agents or professional intermediaries (including weak systems of the countries in which they operate or reside).

### 5. Possible Anonymous Use of the Product in the Profession

Anonymous transactions are vulnerable to money laundering, as the beneficial owner(s) of the funds involved in the transaction is/are not known or are unverified.

### 6. Difficulty in tracing the transaction records

Assess whether transactions executed in the course of delivery of a product by the business are properly recorded and whether access to those records can be readily obtained for CDD/EDD.

# 7. Existence of ML Typologies on the Abuse of the Profession

Assess whether the business is known for abuse for ML purposes.

#### 8. Use of the Profession in Fraud or Tax Evasion Schemes

Assess the use of the business in fraud or tax evasion schemes or other predicate offenses. For this purpose, it may be useful to refer to crime and tax enforcement data to find the businesses that are most vulnerable to actual and potential misuse.

#### 9. Non-face-to-face Use of the Product in the Profession

Availability of non-face-to-face initiation of a business relationship with respect to a business raises ML vulnerability.

#### 10. Cross-border international transaction

Existence of cross border fund transfer facilities or services being provided by casinos increases ML vulnerability.

### Inherent Vulnerability of the Business (0.95) - HIGH

**INHERENT VULNERABILITY FACTORS OVERALL ASSESSMENT** Total Size/Volume of the Business High Client Base Profile of the Business High Level of Cash Activity in the Profession High Use of Agents in the Profession Medium high Possible Anonymous Use of the Product in the Business Available Difficulty in tracing the transaction records Difficult/Time-consuming Existence of ML Typologies on the Abuse of the Business Exist and significant Use of the Profession in Fraud or Tax Evasion Schemes Exist Non-face-to-face Use of the Product in the Business Available

Table 7-3. SUMMARY OF INHERENT VULNERABILITY

### Total Size/Volume of the Business (High Risk)

Cross-border international transaction

The gross gaming revenue of PAGCOR from its gaming operations reached 149.1 billion pesos in 2016 while CEZA received the amount of 847 million pesos from First Cagayan on the same year. APECO, on the other hand, is yet to generate income from its online licensing operations which started on the second semester of 2016.

Medium low

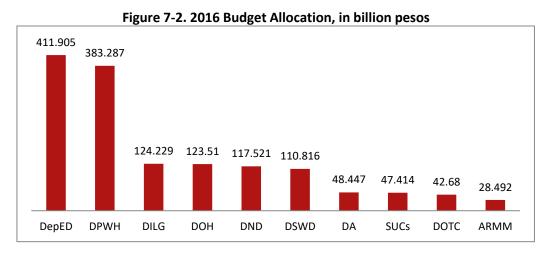
The gross gaming revenue realized by the gaming industry is almost 150 billion or around 5% of 3.002 trillion pesos, the approved national budget of 2016.

Value of the Casino Industry (in million Php) ■ PAGCOR (Gross Gaming Revenue) ■ CEZA (Gross Revenue) 149,120 133,276 116,420 95,364 84,709 605 718 847 2012 2013 2014 2015 2016

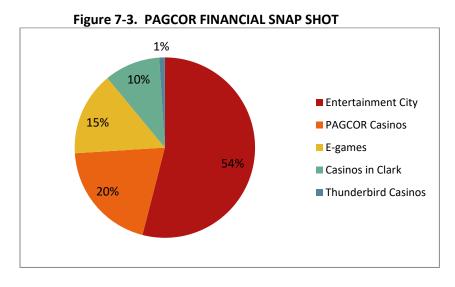
Figure 7-1. Casino Sector

Revenue generated by the gaming industry continue to stimulate economic activities which translate to job generation, infrastructure building, increase in tourism and hospitality related activities. The income generated by the gaming industry significantly contributes in nation-building through its remittances to the national government, funding of mandated beneficiary government agencies, and payment of franchise tax to the Bureau of Internal Revenue.

In fact, the gross gaming revenue being generated by the gaming industry is bigger than the total budget allocation for the Department of National Defense or combined allocations of other major department of the national government for 2016.



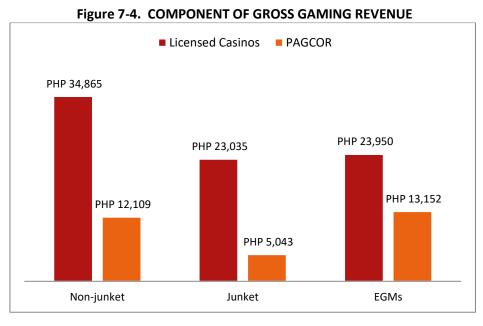
The gross gaming revenue of PAGCOR is largely from the casinos in the entertainment city, generating around 54%, while the remaining 46% are from PAGCOR operated casinos, 20%, e-gaming, 15%, casinos in Clark, 10%, and the remaining 1% is generated by Thunderbird casinos.



As of 31 December 2016, there are 196 e-game outlets, 10 licensed casinos, and 45 PAGCOR operated casinos around the country. While there are 8 (operational) and 138 on-line licensees being regulated by PAGCOR and CEZA, respectively.

Based on the gross gaming revenue posted by the PAGCOR's licensed casinos in 2015, PhP34.865 million of the revenue was from non-junket operations while PhP23.035 million was from junket operations and PhP23.950 million was from Electronic Gaming Machines (EGMs). On the other hand, PAGCOR's gets the bulk of its gaming revenue from EGMs.

Junket players are non-Filipino VIP players who are flown in by junket operators or by casino operators to play.



The gaming industry is also one of the top employment generator in the Philippines. It is estimated that casinos are employing more than 25,000 personnel and the business process outsourcing companies providing online gaming support may have several thousand employees more.

The importance of the gaming industry in fueling economic activities and funding the operation of the government is so significant that it merits attention and protection against criminals and money launderers to preserve its integrity. Considering the foregoing, the total value of the business is rated as **HIGH**.

# Client-base profile of the business (High Risk)

A third of the gross gaming revenue are from junket sourced VIP players. These players are flown in by junket operators or by the licensees and are extended with credit lines and luxury accommodations. The VIP players do not play along with the general and mass market patrons, but are playing inside VIP rooms.

The client mix of foreign players is of Koreans, Japanese, and Malaysians. <sup>182</sup> Koreans dominates the junket segment as far as oversees visitors are concerned. <sup>183</sup> The increase in Chinese tourist has also been noted. <sup>184</sup>

Players from China and Korea have also contributed to the increase in gaming revenue by participating on phone betting or proxy betting being offered by some licensees of PAGCOR. <sup>185</sup> Most of the players engage in proxy betting are from Macao. This may have been caused by the recent policy of Macao which prohibits or ban proxy betting operation. <sup>186</sup>

Some of the junket players are sourced by agents who are not required to conduct the necessary due diligence for AML compliance due to lack of legal framework.

Data from regulators revealed that in 2015 and 2016 the revenue earned from foreign players was 28.14% and 30.46%, respectively.

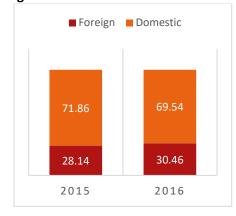


Figure 7-5. REVENUE MIX OF PLAYERS

http://www.bworldonline.com/content.php?section=Corporate&title=junket-operators-get-city-of-dreams-gig-&id=108149. Visited on 18 August 2017.

<sup>&</sup>lt;sup>183</sup> http://www.rappler.com/business/172487-resorts-world-manila-stocks-steady-since-attack. Visited on 18 August 2017.

<sup>&</sup>lt;sup>184</sup> http://www.businessmirror.com.ph/phone-betting-ups-laundering-ante/. Visited on 18 August 2017.

<sup>&</sup>lt;sup>185</sup> https://www.bloomberg.com/news/articles/2017-05-03/remote-control-bets-lift-money-laundering-risk-atmanila-casinos. Visited on 18 August 2017.

<sup>&</sup>lt;sup>186</sup> http://www.businessmirror.com.ph/phone-betting-ups-laundering-ante/. Visited on 18 August 2017.

<sup>&</sup>lt;sup>186</sup> https://www.bloomberg.com/news/articles/2017-05-03/remote-control-bets-lift-money-laundering-risk-atmanila-casinos. Visited on 18 August 2017.

Although domestic PEPs are not allowed by regulation to play in casinos in the Philippines, the licensees may fall short on identifying foreign PEPs because of lack of legal framework that would require them to monitor foreign PEPs.

Incidental to casino operations, clients with high net-worth are inherently considered as high risk considering the possibility that they can be used to undertake money laundering operations due to lack of AML legal framework.

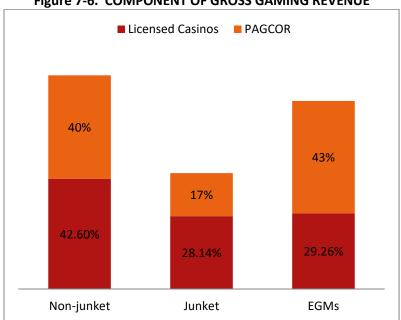


Figure 7-6. COMPONENT OF GROSS GAMING REVENUE

# Level of cash activity associated with the business (High Risk)

The casino industry is a cash driven sector. Transactions are mostly undertaken through cash.

Junket financial transactions with its clients cannot be ascertained because settlements are done in another jurisdiction. Usually at the country of residence of their players. Transactions between the junket and casino operators, however, are done in cash.

On the other hand, a small percentage representing the junket operations undertaken by the casino operators themselves are transacted through the banking system.

#### Other vulnerable factors of the business

• Use of agents (Proxy Betting) – (Medium High Risk)

Some of the casino licensees allow their junket operators to engage in proxy betting operations. It was noted that in some casinos, players are nowhere to be found in the VIP rooms reserved for high-spending gamblers. Instead, young men and women sitting at tables at the casino, many of whom are from china and dressed in smart black uniforms, are talking on mobile phone headsets, are placing bets on behalf of their long-distance clients. 187

<sup>&</sup>lt;sup>187</sup> https://www.bloomberg.com/news/articles/2017-05-03/remote-control-bets-lift-money-laundering-risk-atmanila-casinos. Visited on 18 August 2017.

Although, phone betting or proxy betting operation is not present in all casinos, the same is being allowed by some SAs. In fact, the increase in gaming revenue in 2016 was attributed to the proxy betting operations of some casinos and casino junket operators.

Telephone proxy betting provided a means for players to avoid the know-your-customer requirements associated anti-money laundering laws. Phone betting is banned in other gaming centers such as Singapore, Australia and Macau. 189

### Possible anonymous use of the product in the business (Available)

Proxy betting operations are actually products that are undertaken without face-to-face contact. Although, operators claim that a face-to-face identification process is required before a player is allowed to engage in proxy betting, ensuing transactions are already done without face-to-face contact. Thus, players giving instructions to agents through telephone may no longer be the same person who was subjected to the mandatory identification process. Hence, transactions can be undertaken by unknown individual. Thus, players can enjoy anonymity.

### Difficulty in tracing the transactions (Difficult / time consuming)

Casinos in the Philippines vary in size in relation to its operations. Those who have small operations does not have automated system or casino management system which would enable them to track and retrieve casino transactions. Thus, retrieving transaction history and other relevant information becomes difficult and time consuming.

It is different, however, for casinos in Metro Manila and those licensees who are required to install casino management system by their SAs because extracting information is fast and easy.

### Existence of ML typologies on the abuse of the business (Exist and Significant)

FATF and other AML related publications has identified the casino sector as vulnerable to money laundering abuse and identified different typologies.<sup>190</sup>

# Use of the business/profession in tax/fraud schemes – Electronic Commerce Act (Exist)

Criminal groups already took advantage of Philippine casinos to transfer "illicit proceeds from the Philippines to offshore accounts," the U.S. State Department

https://asia.nikkei.com/Viewpoints-archive/Viewpoints/David-Green-Just-deserts-arrive-late-for-Macau-junkets?page=2. Visited on 18 August 2017.

<sup>&</sup>lt;sup>189</sup> https://www.bloomberg.com/news/articles/2017-05-03/remote-control-bets-lift-money-laundering-risk-atmanila-casinos. Visited on 18 August 2017.

http://www.fatfgafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf,http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Casinos.pdf,https://www.cba.am/Storage/EN/FDK/Typologies/typology\_13\_on\_casinos\_eng.pdf,Visited on 18 August 2017.

said in its International Narcotics Control Strategy Report in March<sup>191</sup>, citing the country's gaming palaces "high risk for money laundering." In fact, in 2016, in one of the largest bank thefts in history, a ring of hackers stole \$81 million from Bangladesh's foreign reserves that were routed through a Philippine casino, a junket operator and a gaming-room promoter. <sup>192</sup>

### • Non-face-to-face interaction with the client (Available)

The proxy betting operations of some casinos and junket operators are conducted without face-to-fact interaction.

### • Cross-border international transaction (Medium Low Risk)

Very limited fund transfers are being undertaken in the casino industry. Most of the cross-border international transactions are undertaken by casino operators using the banking system for their transactions with their junket players.

Financial transactions of the junket operators do not involve actual fund transfer but are undertaken through offsetting of balance with their respective partners abroad. Their financial transactions are actually similar to a hawala system of money remittance.

### **ACTION PLAN**

Considering the general variables and the identified gaps and deficiencies, the following are the recommended action plan based on the prioritization result of the assessment tool.

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
<ul> <li>Effectiveness of Supervision and Oversight</li> <li>To issue the Implementing Rules and Regulation of R.A. No. 10927</li> <li>Creation of a group who will undertake or carry-out AML supervision.</li> <li>AML compliance guidelines</li> <li>Manual on risk based supervision and examination (offsite and on-site)</li> <li>AML/CFT Training Module.</li> <li>In depth analysis of ML risk of junket operations, internet gaming, e-junket, and proxy betting products or services.</li> </ul>	AMLC PAGCOR CEZA APECO AMLC	PAGCOR CEZA APECO	completed  AMLC - completed SAs - 31 January 2018 2 <sup>nd</sup> Qtr. 2018
<ul> <li>AML Knowledge of Business staff</li> <li>Conduct Training Need Assessment</li> <li>Validate and Improve the training module</li> <li>Conduct training for all casino operators</li> </ul>	AMLC PAGCOR CEZA	Casino Licensees	Last quarter of 2017

<sup>&</sup>lt;sup>191</sup> https://www.state.gov/documents/organization/268024.pdf. Visited on 18 August 2017

 $^{192}$  https://www.bloomberg.com/news/articles/2017-05-03/remote-control-bets-lift-money-laundering-risk-atmanila-casinos. Visited on 18 August 2017.

	APECO		
Effectiveness of Compliance Function of the Organization  • Prepare and implement Money Laundering Preventive Program.  • Check compliance and effectiveness of the money laundering preventive programs of the casinos.	Casinos  AMLC PAGCOR CEZA APECO		2 February 2018 2018
Effectiveness of Suspicious Activity Monitoring and Reporting  • Guidelines on ST reporting for Casino  • Configuration of the AML system based on the AML Compliance guidelines issued by the AMLC and AML/CTF Preventive Program of licensees  • Registration to AMLC reporting system	AMLC SAs Casino Licensees/ Operators	AMLC	4 <sup>th</sup> Quarter 2017 1 <sup>st</sup> Quarter 2018 November 2017
Availability and Enforcement of Administrative Sanctions  • Furnish the Supervising Authorities with a copy of the AMLC Administrative Sanctions for comment	AMLC	PAGCOR CEZA APECO	4 <sup>th</sup> Qtr. 2017

### **B. LAWYERS AND NOTARIES**

### INTRODUCTION

As financial institutions have put anti-money laundering (AML) measures into place, the risk of detection has become greater for those seeking to use the global banking system to launder criminal proceeds. Increasingly, law enforcement sees money launderers seeking the advice or services of specialized professionals to help them with their illicit financial operations. <sup>193</sup>

Typology suggested that criminals would seek out the involvement of legal professionals in their money laundering schemes, sometimes because a legal professional is required to complete certain transactions, but also, to access specialized legal and notarial skills and services which could assist in laundering the proceeds of crime and in the financing of terrorism.

While not all legal professionals are actively involved in providing these legitimate legal services which may be abused by criminals, the use of legal professionals to provide a veneer of respectability to the client's activity, and access to the legal professional's client account, is attractive to criminals.

There is also a perception among criminals that legal professional privilege/professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilize the services of a legal professional.

In terms of TF, while few case studies specifically mention the involvement of legal professionals, they do mention the use of companies, charities and the sale of property. As such it is clear that similar

\_

<sup>193 (</sup>Financial Action Task Force, 2004)

methods and techniques could be used to facilitate either ML or TF, although the sums in relation to the later may be smaller, and therefore the vulnerability of legal professionals to involvement in TF cannot be dismissed.<sup>194</sup>

Due to the vulnerability of the profession on April 2013, the Anti-Money Laundering Act of 2001 was amended by Republic Act No. 10365, which included the Lawyers and Notaries as covered person under the AMLA.

#### SECTOR VULNERABILITY ASSESSMENT

### Legal Framework

Section 3(a)(7) of Republic Act No. 9160, as amended by Republic Act No. 10365 designates, as covered person, "persons who provide the following services:

- (i) managing of client money, securities or other assets;
- (ii) management of bank, savings or securities accounts;
- (iii) organization of contributions for the creation, operation or management of companies; and
- (iv) creation, operation or management of juridical persons or arrangements, and buying and selling business entities."

Rule 3.E.4.c of the 2016 Revised Implementing Rules and Regulations of the Republic Act No. 9160, as Amended, provides that, "Persons, including *lawyers* and accountants, who provide any of the following services:

- i. Managing of client money, securities or other assets;
- ii. Management of bank, savings, securities or other assets;
- iii. Organization of contributions for the creation, operation or management of companies; and
- iv. Creation, operation or management of juridical persons or arrangements, and buying and selling business entities."

are covered persons.

The assessment made is based on the data gathered from previous assessment and updated using open source and official documents.

After considering data gathered, the overall vulnerability of the profession is at MEDIUM.

	Availability and Access to Beneficial Ownership Information	Low
Quality of CDD Framework (Medium Low)	Availability of Reliable Identification Infrastructure	Medium High
	Availability of Independent Information	Does not
	Sources	exist

<sup>194 (</sup>Financial Action Task Force, 2008)

-

The quality of CDD framework assesses whether the country has the legal, institutional and technical framework to identify and verify the identities of natural and legal persons. This also includes storing identification records to be used to facilitate the use of this information by the CPs and competent authorities.

# **Beneficial Ownership**

Due to the existence of lawyer-client privilege communication, the services of the lawyers are targeted by money launderers by engaging their services to be the nominees of their clients.

Beneficial ownerships in corporate clients may be established from the General Information Sheet filed with the Securities and Exchange Commission (SEC). However, for sole proprietorships and partnerships, lawyers have no access to any infrastructure to determine if these clients are engaging the lawyers' services in behalf of a beneficial owner.

Nonetheless, the fiduciary relationship between the lawyer and his clients, i.e. it involves trust and confidence, allows lawyers to learn a lot about the personal, business and professional circumstances about their clients, which may eventually lead them to the ultimate beneficial ownership information.

# **Reliable Identification Infrastructure**

Notwithstanding the lack of National ID System or other reliable public information system, lawyers can still conduct customer identification and verification by requiring the production of multiple identification documents and the sending of billing statements to the client's given address. Also, since law practice involves a fiduciary relationship between the lawyer and his clients, lawyers are in a unique position to learn a lot about the personal, business and professional circumstances about their clients.

### **Independent Information Sources**

Historical financial information is not available to lawyers as these are usually covered by confidentiality provision of laws or part of the contract between the financial institutions and their clients.

Compliance Level of Staff (Medium Low)	Effectiveness of Compliance Function	Does not exist
	Availability and Enforcement of Criminal Sanctions	Medium Low
	Integrity of Business/Profession Staff	High
	AML Knowledge of Business/Profession Staff	Low

Compliance level of business/profession staff assesses if the sector complies to the requirements under the AMLA and if they fully understand their institutional obligations.

### **Compliance Function**

The AMLA and the present RIRRs do not provide specific requirements for lawyers to have an AML compliance function. This is in addition to the general resistance, if not disregard, by the legal

profession with the requirement of the AMLA due to belief that the AMLA requirements for covered persons are in conflict with lawyer-client privilege communication. Thus, enforcement cannot be implemented.

### **Criminal Sanctions**

Sanctions against covered persons are available for a range of criminal violations under the AMLA, including money laundering offenses, malicious reporting and violation of confidentiality provisions. Thus, a lawyer, after proper investigation may be the subject of criminal cases under the AMLA without any legal impediment.

However, there is no record yet that a lawyer has been involved in money laundering in his capacity as a lawyer. Likewise, as a covered person, no lawyer has been investigated or prosecuted for failure to file covered or suspicious transaction reports, malicious reporting, or violation of confidentiality provision, as there is no enforcement of the AMLA in the legal profession due to lack of specific guidelines detailing its implementation.

### **Integrity of Business/Profession Staff**

The lawyers are required to observe the highest degree of legal and ethical standards. All its actions must be made within the bounds of law and propriety. As such, lawyers are very protective of their hard-earned privilege of being a member of the Philippine Bar and would not normally be willing to take the risk of being the subject of disbarment in exchange of money.

However, due to the nature of their work, which is offered to everyone who requires legal services and the presumption of innocence in criminal cases, lawyers may unintentionally or unknowingly be assisting money launderers.

# AML Knowledge of Business/Profession Staff

Most lawyers have a general overview or understanding of the AMLA only. Considering that AMLA is not a core subject in law school and MCLE courses, and that lawyers are just fairly recently designated as covered persons, exposure to AML laws, policies and procedures are very minimal or close to nothing, except for those who are handling money laundering cases. Although AML training programs and materials are readily in open sources, lawyers and their staff will not spend time to study these if it is not needed for an existing case or assignment. This is on top of the fact that there is no compelling reason for them to study AML as there is no regulation enforcing specific compliance on their part.

Commitment	Quality of AML	Effectiveness of Supervision/ Oversight Activities	Does not exist	
Quality of	and Leadership of Management	Supervision (Does not exist)	(Does not Administrative Sanctions	Low
AML Policies and	(Medium Low)	Availability and Effectiveness of Entry Controls		High
Procedures (Medium		Availability and E	Enforcement of Criminal Sanctions	Medium Low
Low)	Comprehensive	prehensiveness of AML Legal Framework		Medium
	Effectiveness of Compliance Function			Does not exist

### **AML Legal Framework**

In 2013, R.A. No. 10365 designated all persons, regardless of the profession, who provide any of the following services as covered persons under the AMLA:

- i. managing of client money, securities or other assets;
- ii. management of bank, savings or securities accounts;
- iii. organization of contributions for the creation, operation or management of companies; and
- iv. creation, operation or management of juridical persons or arrangements, and buying and selling business entities. 195

The said law essentially put lawyers who provide the foregoing services within the coverage of the AMLA. The 2016 Revised Implementing Rules and Regulations (RIRR) of the AMLA made it explicit by stating that persons, "including lawyers" who provide the foregoing services are covered persons.

As covered persons, lawyers who provide the foregoing services are required to comply with the provisions of the AMLA, its RIRR and all AMLC issuances, which include customer due diligence, record-keeping, and covered and suspicious transactions reporting. They are also required to register with the AMLC for reporting purposes, and may be subject to compliance checking by the AMLC to ensure effective implementation of the AMLA. However, a detailed regulation on how to implement the provisions of the AMLA with regard to lawyers is very limited as the RIRR merely provides the general legal framework for all covered persons. The absence of detailed guidelines on how exactly do lawyers comply with the requirements of the AMLA limits, if not totally discourages, compliance by lawyers.

#### **AML Supervision Procedures and Practices**

The AMLC is the AML regulator of the Philippines. It sets up regulations to implement the provisions of the AMLA, but it is the Supreme Court which exercises general supervision and control over the members of the Philippine bar, i.e. lawyers. In the exercise of its administrative function, it has the power to regulate the practice of law, including the power to promulgate rules for the admission to and continued exercise of the profession, and authority discipline erring lawyers. The Supreme Court usually concentrates on legal competence and ethics without particular emphasis on AML supervision. Thus, there is no dedicated and regular AML compliance checking on the legal profession. However, violations of law, including AMLA, and legal ethics may be reported to the Supreme Court any time for disbarment proceedings.

ML concepts, risks and compliance are not specifically identified as a function of the Supreme Court. Lawyers' exposure to ML-related topics and issues are only usually limited to Mandatory Continuing Legal Education (MCLE) sessions in which AMLA is rarely included as a subject; and during actual cases where the services of the lawyers are engaged by the clients. The Supreme Court may discipline lawyers for involvement in crimes, including ML, in cases of disbarment proceedings.

### **Administrative Sanctions**

The AMLC, may, upon its discretion, and after due notice and hearing, impose administrative sanctions for violations of the AMLA, its RIRR and all AMLC issuances. These sanctions are applicable to all covered persons, including lawyers.

<sup>&</sup>lt;sup>195</sup> Sec. 3(a)(7), Republic Act No. 9160, as amended by Republic Act No. 10365.

Also, there can be challenges in imposing administrative sanctions against lawyers. Although the AMLC is the AML regulator of the Philippines, it is the Supreme Court who has sole authority to discipline erring lawyers through disbarment proceedings. At the very least, the AMLC can make a determination if a particular lawyer has committed AMLA violations and impose the relevant sanctions, and refer it to the Supreme Court for implementation.

Considering the foregoing, lawyers generally do not comply with the requirements of the AMLA as the probability of them being sanctioned for administrative violations is very low.

### **Availability and Effectiveness of Entry Controls**

The Supreme Court has supervision and control on the admission to the practice of law, including the required educational background and bar examination. All applicants for bar examinations must comply with strict requirements of competency and ethics, including the submission of official transcripts of pre-law and law degrees; Sworn Certification by the School Registrar and noted by the Law Dean that the applicant graduated a four-year law course and that his name is included in the Legal Education Board (LEB) Certification; testimonials of good moral character from two (2) members of the Philippine Bar; and Certificate of No Derogatory Record from the Dean of the law school. Thereafter, the name of the applicants shall be published in a newspaper of general circulation to give the public an opportunity to oppose the application if there are any valid grounds.

After admission to the Philippine Bar, all lawyers are expected to observe the highest legal and ethical standards, and required to continually observe the Lawyer's Oath and the Code of Professional Responsibility for Lawyers, under penalty of suspension or disbarment. Lawyers are also required to finish thirty-six (36) hours of MCLE units every compliance period to be updated on the latest developments in the legal practice.

However, the AMLA is not a core subject in the law schools in the Philippines and in MCLE course. It is only usually discussed in the form of a briefer or quick lecture as part of the wider Commercial/Mercantile Law subject.

Notarial functions can only be performed by lawyers; thus they are bound by the same rules applicable to lawyers.

Quality of Operations (Medium Low)	Commitment and Leadership of Management	Medium Low
	Compliance Level of Staff	Low
	Quality of CDD Framework	Low
	Effectiveness of Suspicious Activity Monitoring	Does Not Exist

Commitment and leadership of management, compliance level of staff and quality of CDD framework are all assessed in the above section.

#### **Suspicious Activity Monitoring**

Lawyers do not comply with the requirement to report covered and suspicious transactions to the AMLC. The AMLA provides that they are not required to report covered and suspicious transactions if

the relevant information was obtained in circumstances where they are subject to legal professional privilege, which is their umbrella defense in not complying with the reporting requirements.

Given that there are no specific guidelines on how to implement the reporting requirements under the AMLA that will help lawyers determine if their services involve lawyer-client privilege communication, lawyers are discouraged to make suspicious transaction reports to the AMLC.

Inherent Vulnerability

### 1. Total Size/Volume of the Business (Low)

There are around 54,000<sup>196</sup> active lawyers in the country as of 2014. Additional 5,471 lawyers were added from 2016-2017.<sup>197</sup> Majority of lawyers are working with the government followed by solo practitioners with a handful working in the private sector and law offices.<sup>198</sup>

### 2. Client-base profile of the Profession (Medium)

The profession only has around 3.5% of its total legal services that involves international transaction and the number of PEP client is insignificant compared to the total number of clients. <sup>199</sup>

The percentage of legal professionals representing the 3.5% who are engaged in performing the activities covered by the AMLA, are as follows:<sup>200</sup>

- Managing of client money, securities or other assets 5.4%
- Management of client's bank, savings or securities accounts 2.1%
- Organization of contributions for the creation, operation or management of companies 9.5%
- Creation, operation or management of juridical persons or arrangements, and buying and selling business entities 11.5%
- Not offering the services 81.6%

Although the organization and creation of legal person is quite high at 9.5% and 11.5% respectively, current regulation on registration of legal person requires the disclosure of nominees and beneficial ownership. Further, it is still not significant considering that it is only a percentage of the 3.5% of the whole legal profession.

### 3. Level of cash activity associated with the profession (Low)

Due to the nature of their services (managing of client money, securities or other assets, management of client's bank, savings or securities accounts, organization of contributions for the creation, operation or management of companies, creation, operation or

<sup>&</sup>lt;sup>196</sup> Integrated Bar of the Philippine (Johas, 2014)

 $<sup>^{197}</sup>$  Based on the results of the 2015 and 2016 Bar Examinations.

<sup>&</sup>lt;sup>198</sup> Survey conducted by the NRA Sub-Group on DNFBPs during the 15<sup>th</sup> National Lawyers Convention, Waterfront Cebu City Hotel & Casino, Cebu City, March 20, 2015.

<sup>&</sup>lt;sup>199</sup> Survey conducted by the NRA Sub-Group on DNFBPs during the 15<sup>th</sup> National Lawyers Convention, Waterfront Cebu City Hotel & Casino, Cebu City, March 20, 2015.

<sup>&</sup>lt;sup>200</sup> Survey conducted by the NRA Sub-Group on DNFBPs during the 15<sup>th</sup> National Lawyers Convention, Waterfront Cebu City Hotel & Casino, Cebu City, March 20, 2015.

management of juridical persons or arrangements, and buying and selling business entities), payment through cash for the said services is not a usual practice.

#### 4. Other Vulnerable Factors of the Profession

# • Use of Agents (Not Analyzed)

Data is not available for this variable. However, due to the nature of the services, i.e. it need not be performed by a lawyer, it is highly probable that agents or staff of the lawyers may be the one performing the designated services.

### • Possible Anonymous Use of the Product in the Profession (Available)

Anonymous use of the services of lawyers is very possible as the services of a lawyer are available to everyone, especially for paying clients.

### Difficulty in tracing the transactions (Difficult/Time-consuming)

Lawyer-Client Privilege is the biggest hurdle in transparency when assessing or investigating the transactions of clients with their lawyers. This is, however, not absolute as the Revised Rules of Court and Code of Professional Responsibility do not allow lawyers to use privilege communication as a shield against reporting possible commission of crime, which include money laundering and all its predicate offenses.

### • Existence of ML Typologies on the Abuse of the Profession (Exist, but Limited)

Key ML typologies that commonly employ or, in some countries, require the services of a legal professional were identified as follows:

- a. Using lawyer's accounts to transfer dirty money to third parties
- b. Creation of corporate vehicles or other legal arrangements (e.g. trusts);
- c. Buying and selling of real property;
- d. Performing financial transactions, such as carrying out various financial operations on behalf of the client, (e.g. cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing checks, purchase and sale of stock, sending and receiving international funds transfers); and
- e. Gaining introductions to financial institutions

### Use of the Profession in Tax/Fraud Schemes (Exist)

Lawyers may provide financial and tax advice to criminals who are posing as an individual or business hoping to legitimately minimize a tax obligation or seeking to place assets out of reach in order to avoid future liabilities.

# Non Face-to-face Interaction with the Client (Available, but Limited)

The services of a lawyer may be engaged even without having face-to-face contact. The use of telephone or other Information Technology is available for clients to reach their preferred lawyers.

#### **ACTION PLAN**

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
<ul> <li>Coordinate with Supreme Court for possibility of including AML in the subjects in law school</li> <li>Coordinate with MCLE Board to require</li> </ul>	AMLC, SC	MCLE Board	Q4 2017
<ul><li>MCLE Providers to include AML in the subjects</li><li>Create AML training modules for lawyers</li></ul>			
<ul> <li>Meet with SC and/or IBP to discuss terms of reference for the creation of a joint plan to identify areas where both parties can improve the implementation of AMLA in the law profession.</li> <li>Create AML training modules for lawyers</li> <li>Expedite drafting of AMLC Inspection/Examination Manual</li> </ul>	AMLC, SC	IBP	Q4 2017
Coordinate with Supreme Court on the possible setup in the implementation of administrative sanctions under the AMLA	AMLC, SC		2018 Q3 2017
<ul> <li>Create dedicated Administrative Investigation Unit to expedite the evaluation of ROEs and ROCs</li> <li>Enforcement of the Rules on the Imposition of Administrative Sanctions</li> </ul>	AMLC, BSP		
Formulate detailed Guidelines on the implementation of the AMLA and its RIRR for the regulated services enumerated under the AMLA for Designated Non-financial professions.	AMLC, SC		Q4 2017 – Q2 2018

# C. ACCOUNTANTS

#### **INTRODUCTION**

Accountants covered under the law refer to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

Accountants in business are referred to professional or other alternative sources of Guidance, on the appropriate action to take in relation to suspected illegal activity by their employer or a third party.

Accountants in practice may provide a very wide range of services, to a very diverse range of clients. For example, services may include (but are not restricted to):

• Audit and assurance services.

- Book-keeping and the preparation of annual and periodic accounts.
- Tax compliance work, and advice on the legitimate minimization of tax burdens.
- Internal audit, and advice on internal control and risk minimization.
- Regulatory and compliance services, including outsourced regulatory examinations and remediation services.
- Insolvency/receiver-managers/bankruptcy related services.
- Advice on the structuring of transactions, and succession advice.
- Advice on investments and custody of client money.
- Forensic accountancy.

In many countries, accountants are the first professional consulted by many small businesses and individuals when seeking general business advice and a wide range of regulatory and compliance advice. Where services are not within their competence, accountants advise on an appropriate source of further assistance<sup>201</sup>.

Some of the functions performed by accountants that are the most useful to the potential launderer include:

- a) Financial and tax advice Criminals with a large amount of money to invest may pose as individuals hoping to minimize their tax liabilities or desiring to place assets out of reach in order to avoid future liabilities.
- b) Creation of corporate vehicles or other complex legal arrangements (trusts, for example)
   such structures may serve to confuse or disguise the links between the proceeds of a crime and the perpetrator.
- c) Buying or selling of property Property transfers serve as either the cover for transfers of illegal funds (layering stage) or else they represent the final investment of these proceeds after their having passed through the laundering process (integration stage).
- d) Performing financial transactions Sometimes accountants may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.).
- e) Gaining introductions to financial institutions.<sup>202</sup>

# **SECTOR VULNERABILITY ASSESSMENT**

### Legal framework

Section 3(a)(7) of Republic Act No. 9160, as amended by Republic Act No. 10365 designates, as covered person, "persons who provide the following services:

(v) managing of client money, securities or other assets;

-

<sup>&</sup>lt;sup>201</sup> The European Federation of Accountants (FEE) has issued a study on market access across the Member States of the European Union, which gives an indication of the types of services provided by accountants, and the ways in which they can vary between countries.

<sup>&</sup>lt;sup>202</sup>(Financial Action Task Force, 2008)

- (vi) management of bank, savings or securities accounts;
- (vii) organization of contributions for the creation, operation or management of companies; and
- (viii) creation, operation or management of juridical persons or arrangements, and buying and selling business entities."

Rule 3.E.4.c of the 2016 Revised Implementing Rules and Regulations of the Republic Act No. 9160, as Amended, provides that, "Persons, including lawyers and accountants, who provide any of the following services:

- i. Managing of client money, securities or other assets;
- ii. Management of bank, savings, securities or other assets;
- iii. Organization of contributions for the creation, operation or management of companies; and
- iv. Creation, operation or management of juridical persons or arrangements, and buying and selling business entities."

are covered persons.

The assessment made is based on the open source documents and official documents as well as the input of Mr. Tan Torres of the Board of Accountancy, Professional Regulations Commission.

After considering data gathered, the overall vulnerability of the profession is at Medium.

Quality of CDD	Availability and Access to Beneficial Ownership Information	Medium Low
Quality of CDD Framework (Medium)	Availability of Reliable Identification Infrastructure	Medium High
	Availability of Independent Information	Does not
	Sources	exist

The quality of CDD framework assesses whether the country has the legal, institutional and technical framework to identify and verify the identities of natural and legal persons. The information and identification records which can facilitate the use of this information by the AMLC, competent authorities and authorized parties for AML purposes.

### **Beneficial Ownership Information**

Due to the professional secrecy being observed by accountants, particularly the PICPA members, the services of CPAs are targeted by money launderers by engaging their services to be the nominees of their clients.

Beneficial ownerships in corporate clients may be established from the General Information Sheet filed with the Securities and Exchange Commission (SEC). However, for sole proprietorships and partnerships, CPAs have no access to any infrastructure to determine if these clients are engaging the accountants' services in behalf of a beneficial owner.

### **Reliable Identification Infrastructure**

Notwithstanding the lack of National ID System or other reliable public information system, accountants can still conduct customer identification and verification by requiring the production of multiple identification documents and the sending of billing statements to the client's given address.

# **Independent Information Sources**

Historical financial information is available to accountants as they are usually the ones tapped by clients to prepare their financial documentation. However, for big corporate clients who have their own internal auditors, a CPA who was hired as an external auditor may only do the reconciliation of records based only on the documents provided to him, which may already be compromised.

	Effectiveness of Compliance Function	Does not exist
Compliance Level of Staff	Availability and Enforcement of Criminal Sanctions	Medium Low
(Medium Low)	Integrity of Business/Profession Staff	High
	AML Knowledge of Business/Profession Staff	Low

#### **Compliance Function**

With the absence of regulations specifying what exactly are expected from accountants with regard to compliance with the AMLA, and the fact that AML is just a small part of the accounting services in the Philippines, accountants do not have sufficient reason to spend resources for the establishment of an AML compliance function. Thus, private practitioners and firms do not find it necessary to check and monitor their own AML compliance.

Big auditing firms that plan to expand its services to include AML audit would be forced to conduct AML compliance function as it is necessary in its business. However, since this plan is still in the establishment stage, there is no available information yet as to its effectiveness.

# **Criminal Sanctions**

Criminal violations of the AMLA are applicable to all covered persons without any legal impediment for as long as evidence warrants. However, the sector is yet to be involved in any report that would suggest the direct participation of CPAs in money laundering and/or its predicate offenses.

#### **Integrity of Profession Staff**

CPAs are required to observe professional ethics in the exercise of their profession. As such, Accountants are very protective of their hard-earned privilege of being licensed as a CPA and would not normally be willing to take the risk of being the subject of administrative case.

However, due to the nature of their work, which is offered to everyone who requires accounting services, CPAs may unintentionally or unknowingly be assisting money launderers.

# **AML Knowledge of Profession Staff**

Considering that AMLA is not a core subject in accounting and COPE courses, and that accountants are just fairly recently designated as covered persons, exposure to AML laws, policies and procedures are very minimal or close to nothing. Although there is an abundance of AML materials from open sources, generally, accountants do not find the necessity of learning about it, unless it is directly related with their assignments, like in the case of recent plans to expansion the services being offered by big auditing firms which already include AML compliance audit. Contributory to the lack of interest to learn about AML is the general impression that accountants' services are covered by privilege communication, which should be addressed by the AMLC by issuing guidelines.

	Commitment and Leadership of Management (Medium low)	Quality of AML Supervision (Does not exist)	Effectiveness of Supervision/ Oversight Activities	Does not exist
Quality of			Availability and Enforcement of Administrative Sanctions	Low
AML Policies and		Availability and Effectiveness of Entry Controls		High
Procedures (Low)		Availability and Enforcement of Criminal Sanctions		Medium Low
	Comprehensiveness of AML Legal Framework			Medium
	Effectiveness	of Compliance Function		Does not exist

The overall quality and comprehensiveness of the AML policy and procedures is assessed based on commitment and leadership of management in relation to the supervision and its compliance to AML.

### **Supervision/Oversight Activities**

The practice of accountancy is one of the highly regulated professions in the country. It is regulated by the Board of Accountancy (BOA) under the Professional Regulation Commission (PRC) by virtue of Republic Act No. 9298, otherwise known as the Philippine Accountancy Act of 2004, which amended Presidential Decree 692.

In 1975, with the accreditation by the PRC of the Philippine Institute of Certified Public Accountants (PICPA) as the *bona fide* professional organization representing CPAs in the country, BOA has coordinated with PICPA to further strengthen the profession. With PICPA, it has worked for the passage of The Accountancy Act of 1967; the issuance of the Code of Professional Ethics in 1978; the issuance of guidelines in 1987 for the mandatory continuing professional education (CPE) program for CPAs; the integration of the accounting profession completed in 1987; the biennial oath taking of new CPAs; standards setting for the profession through membership in the Accounting Standards Council and the Auditing Standards Practices Council; and the declaration of the Accountancy Week. However, membership in PICPA is voluntary in nature.

Both BOA and PICPA usually concentrate on best practices in accounting without particular emphasis on AML supervision. Thus, there is no dedicated and regular AML compliance checking on the accounting profession.

ML concepts, risks and compliance are not specifically identified as a function of BOA and PICPA. Accountants' exposure to ML-related topics and issues are only usually limited to CPE sessions in which AMLA is rarely included as a subject; and in those few big accounting firms that are providing third party AMLC compliance services. The BOA may discipline CPAs for involvement in crimes, including ML, in cases of administrative proceedings by suspending or cancelling their professional licenses.

#### **Administrative Sanctions**

The AMLC, may, upon its discretion, and after due notice and hearing, impose administrative sanctions for violations of the AMLA, its RIRR and all AMLC issuances.

Also, considering the absence of regular AML compliance checking, AMLA violations of CPAs are not reported to the AMLC for possible imposition of sanctions.

Considering the foregoing, accountants generally do not comply with the requirements of the AMLA as the probability of them being sanctioned for administrative violations is very low.

### **Effectiveness of Entry Controls**

PRC-BOA regulates the licensing of accountants. Accountancy graduates need to pass one of the toughest professional licensure examinations in the Philippines before becoming CPAs.

After receiving their licenses as CPAs, accountants are expected to observe ethical standards, and required to continually observe their Oath and the Code of Professional Ethics, in cases of PICPA members. CPAs are also required to finish one hundred twenty (120) hours of CPE units every compliance period to be allowed to renew their licenses.

However, the AMLA is not a subject in the accounting and CPE courses. It is only usually discussed in the form of a briefer for those who are interested in the topic due to the nature of their employment.

# **Criminal Sanctions**

Criminal violations of the AMLA are applicable to all covered persons without any legal impediment for as long as evidence warrants. However, the sector is yet to be involved in any report that would suggest the direct participation of CPAs in money laundering and/or its predicate offenses.

### <u>AML Legal Framework</u>

In 2013, R.A. No. 10365 designated all persons, regardless of the profession, who provide any of the following services as covered persons under the AMLA:

- (i) managing of client money, securities or other assets;
- (ii) management of bank, savings or securities accounts;
- (iii) organization of contributions for the creation, operation or management of companies; and
- (iv) creation, operation or management of juridical persons or arrangements, and buying and selling business entities.<sup>203</sup>

Like in the case of lawyers and notaries, it essentially put accountants who provide the foregoing services within the coverage of the Philippine AML regime. The 2016 Revised Implementing Rules and

<sup>&</sup>lt;sup>203</sup> Sec. 3(a)(7), Republic Act No. 9160, as amended by Republic Act No. 10365.

Regulations (RIRR) of the AMLA made it explicit by stating that persons, "including ... and accountants" who provide the foregoing services are covered persons, which must comply with AML laws and regulations.

As a covered person, accountants who provide the foregoing services are required to comply with the provisions of the AMLA, its RIRR and all AMLC issuances, which include customer due diligence, record-keeping, and covered and suspicious transactions reporting. They are also required to register with the AMLC for reporting purposes, and may be subjected to compliance checking by the AMLC to ensure effective implementation of the AMLA. However, a detailed regulation on how to implement the provisions of the AMLA with regard to lawyers is very limited as the RIRR merely provides the general legal framework for all covered persons. The absence of detailed guidelines on how exactly do lawyers comply with the requirements of the AMLA limits, if not totally discourages, compliance by lawyers.

The Securities and Exchange Commission (SEC) has launched a program which requires accreditation of auditors. Only those who are accredited by SEC are allowed to sign audited financial documents of legal persons and partnership under its jurisdiction. It is also worthy to mention that accounting firms are required to be registered with the BOA for monitoring and regulation.

#### **Compliance Function**

The effectiveness of compliance function is assessed under the overall Compliance Level. The absence of regulation and the lack of resources for the establishment of an AML compliance function, accountants/private practitioners thus find no reason to check or monitor their own AML compliance. On the other hand, big auditing firms have plans to expand their services to include AML audit; hence, they would be forced to conduct AML compliance function.

	Commitment and Leadership of Management	Medium Low
Quality of Operations	Compliance Level of Staff	Medium Low
(Medium Low)	Quality of CDD Framework	Medium
	Effectiveness of Suspicious Activity Monitoring	Does Not Exist

Quality of operations is affected by the management's commitment and leadership to AML, compliance level of its staff and the quality of CDD framework, which are all assessed in the above section, and effectiveness of suspicious activity monitoring.

#### Suspicious Activity Monitoring and Reporting

Accountants do not comply with the requirement to report covered and suspicious transactions to the AMLC. The AMLA provides that persons offering the relevant services are not required to report covered and suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy, which is the accounting sector's umbrella defense in not complying with the reporting requirements.

### **Inherent Vulnerability Factors**

### 1. Total Size/Volume of the Business (Low)

As of October 2016, there are around 179, 267 CPAs, $^{204}$  but as of 2014, only around 21,586 CPAs are affiliated with PICPA. $^{205}$ 

PICPA reported that accounting services was computed or estimated at around .03% of the nominal GDP of the country in 1998. The percentage appears to be not significant on the country's GDP.

# 2. Client-base profile of the Profession (Medium)

The data on the percentage of international transactions is not available, because accountants are of the position that this involves confidential information covered by accountant-client relationship. It may be assumed, however, that only few transactions may be conducted or related to foreign transactions because foreign clients also transact through their local representatives, thus, the transactions become domestic.

PICPA rated their sector Medium as regards to the percentage of clients who are PEP. The rating is based on the presumption that several government officials were charged with corruption cases and that their sector has no way of ascertaining the involvement of their sector on said transactions.

# 3. Level of cash activity associated with the profession (Medium Low)

Due to the nature of their services (managing of client money, securities or other assets, management of client's bank, savings or securities accounts, organization of contributions for the creation, operation or management of companies, creation, operation or management of juridical persons or arrangements, and buying and selling business entities), payment through cash for the said services is not a usual practice.

### 4. Other Vulnerable Factors of the Profession

#### Use of Agents (Not Analyzed)

Data is not available for this variable. However, due to the nature of the services, i.e. it need not be performed by an accountant; it is highly probable that agents or staff of the accounting firms may be the one performing the designated services.

# • Possible Anonymous Use of the Product in the Profession (Available)

Anonymous use of the services of accountants is very possible as the services of CPAs are available to everyone, especially for paying clients.

<sup>&</sup>lt;sup>204</sup>Based on the number of PRC Board Examination Passers [100,689 (1999 PRC Report); around 3,000 new CPAs annually from 2001-2004; 66,578 new CPAs (2000, 2005-2016]

<sup>&</sup>lt;sup>205</sup>ASEAN Federation of Accountants and World Bank Group, CURRENT STATUS OF ACCOUNTING AND AUDITING PROFESSION IN ASEAN COUNTRIES, September 2014, at http://www.aseanaccountants.org/files/afa\_report-printed\_version.pdf (last accessed on 25 July 2017).

## Difficulty in tracing the transactions (Difficult/Time-consuming)

Accountants give heavy premium of the confidentiality of accountant-client relationship, as required by PICPA's Code of Conduct, which adopted the International Ethics Standard for Accountants (IESBA) internationally appropriate Code of Ethics for Professional Accountants.

Under the code, PICPA members are required to undertake engagement acceptance procedure if the transaction would involve the holding of client's money. Accountants are required to inquire about the source of assets and consider all legal and regulatory obligations and to seek legal advice if necessary.<sup>206</sup>

Considering, however, the small number of PICPA members in relation to the total number of CPAs, the Code of Conduct cannot be implemented effectively to the entire accounting profession.

### • Existence of ML Typologies on the Abuse of the Profession (Exist, but Limited)

Key ML typologies that commonly employ or, in some countries, require the services of CPAs were identified as follows:

- a. use of client accounts
- b. purchase of real property
- c. creation of trusts and companies
- d. management of trusts and companies
- e. giving investment/financial advice

#### Use of the Profession in Tax/Fraud Schemes (Exist)

Considering that the services of accountants are usually tapped for the preparation of financial documentation, including for tax purposes, the probability that accountants are used for tax/fraud schemes is probable, especially for those business/clients that do not have automated issuance of receipts.

# • Non Face-to-face Interaction with the Client (Available, but Limited)

The services of accountants may be engaged even without having face-to-face contact. The use of telephone or other Information Technology is available for clients to reach their preferred accountants.

#### **ACTION PLAN**

Of the AML combating controls and factors assessed, the top 3 priorities are:

- 1. Effectiveness of Supervision/Oversight Activities
- 2. AML Knowledge of the Profession
- 3. Effectiveness of Compliance Function (Organization)

-

<sup>&</sup>lt;sup>206</sup>(Accountants, 2013)

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
<ul> <li>Coordinate with PRC-BOA for possibility of including AML in the CPA Licensure Exam and require AML in the subjects in CPD</li> <li>Create AML training modules for accountants</li> <li>Awareness Campaign</li> </ul>	AMLC, BOA		Q4 2017
<ul> <li>Meet with BOA to discuss terms of reference for the creation of a joint plan to identify areas where both parties can improve the implementation of AMLA in the accountancy profession.</li> <li>Expedite drafting of AMLC Inspection/Examination Manual</li> <li>For BOA and AMLC explore how the 'Non-Compliance with Laws and Regulations' (NOCLAR) in the code of ethics of accountants can be implemented in relation to AML Compliance.</li> </ul>	AMLC, BOA		Q4 2017
<ul> <li>Create DNFBP dedicated Administrative Investigation Unit for AML compliance issues</li> <li>Enforcement of the Rules on the Imposition of Administrative Sanctions</li> </ul>	AMLC, BOA		2018 Q2 2018
Formulate detailed Guidelines on the implementation of the AMLA and its RIRR for the regulated services enumerated under the AMLA for Designated Non-financial Businesses and Professions.	AMLC, BOA		Q4 2017 – Q2 2018

### D. DEALERS IN PRECIOUS METALS AND STONES

# **INTRODUCTION**

The FATF has identified dealers in precious metals and stones as particularly vulnerable to ML/TF. The high value per gram of gold and diamonds and the ease by which they can be transferred make them attractive to criminals. There are significant obligations imposed by the FATF Recommendations on dealers in precious metals and stones.

The AMLA, as amended by Republic Act No. 10365, which came into effect in April 2013 included "jewelry dealers in precious metals and precious stones" as covered persons.

This is merely an updating of the risk assessment conducted in 2014. The materials used to update this assessment are purely from open source and official documents.

#### SECTOR VULNERABILITY ASSESSMENT

#### **Legal Framework**

Section 3(a), paragraphs (4) and (5) of Republic Act No. 9160, as amended by Republic Act No. 10365, designate as covered persons:

- (4) jewelry dealers in precious metals, who, as a business, trade in precious metals, for transactions in excess of One million pesos (P1,000,000.00);
- (5) jewelry dealers in precious stones, who, as a business, trade in precious stones, for transactions in excess of One million pesos (P1,000,000.00);

Rule 3.E.4.a of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as amended, defines "dealer" as follows:

"Dealer" refers to an individual or entity who buys and/or sells precious metals, precious stones, and/or jewelry in the course of its business activities. The purchases or sales of precious metals, precious stones, and/or jewelry, as referred to herein, exclude those carried out for, connected with, or for the purpose of extracting precious metals or precious stones from a mine, or cutting or polishing precious stones.

### **Sectoral Vulnerability**

The vulnerability map, after assessing each input variable, showed an overall **Medium** sector vulnerability.

Quality of CDD	Availability and Access to Beneficial Ownership Information	Close to nothing
Quality of CDD Framework ( Low)	Availability of Reliable Identification Infrastructure	Low
( 2011)	Availability of Independent Information	Close to
	Sources	nothing

The quality of CDD framework assesses whether the country has the legal, institutional and technical framework to identify and verify the identities of natural and legal persons. The information and identification records which can facilitate the use of this information by the AMLC, competent authorities and authorized parties for AML purposes.

### **Beneficial Ownership Information**

Company registry for corporations, Securities and Exchange Commission, requires applicants to provide the list of the names of the shareholders and officers together with the amount of ownership in the company. The registry, however, does not check whether owners or shareholders have criminal records.

### <u>Identification Infrastructure</u>

Notwithstanding the absence of a National ID System or other reliable public information system, jewelry dealers can still conduct customer identification and verification by requiring the production

of multiple identification documents and the sending of billing statements to the client's given address.

### **Independent Information Sources**

Jewelry dealers do not have ready access to independent and reliable sources of information to determine transaction patterns of clients.

	Effectiveness of Compliance Function	Does not exist
Compliance Level of Staff	Availability and Enforcement of Criminal Sanctions	Medium Low
(Medium)	Integrity of Business/Profession Staff	Medium
	AML Knowledge of Business/Profession Staff	Low

### Compliance function

The sector is not yet being monitored or regulated for AML/CFT compliance due to the absence of the AML/CFT guidelines. Thus, the dealers are not yet required to comply with the AML compliance requirements including the appointment of an AML/CFT compliance officer and suspicious and covered transaction reporting.

#### **Criminal Sanctions**

Sanctions against covered persons are available for a range of criminal violations under the AMLA, including money laundering offenses, malicious reporting and violation of confidentiality provisions. Thus, a dealer, after proper investigation may be the subject of criminal cases under the AMLA without any legal impediment.

However, there is no record yet that a dealer has been involved in money laundering in his capacity as a dealer/employee of a dealer. Likewise, as a covered person, no dealer has been investigated or prosecuted for compliance concerns, as there is no enforcement of the AMLA in the sector due to lack of specific guidelines detailing its implementation.

# **Integrity of Business Staff**

Owners and employees are expected to act with integrity in conducting their businesses and would, generally, not allow their businesses to be used in furtherance of an unlawful activity or money laundering. Their limited knowledge of the money laundering risk and the absence of AML measures in place makes them vulnerable and possibly be facilitating money laundering involuntarily or unknowingly.

### **AML Knowledge of Business Staff**

Since jewelry dealers are just fairly recently designated as covered persons, exposure to AML laws, policies and procedures is very minimal.

Further, the sector is not yet being monitored or regulated for AML/CFT compliance. The staff of the sector has no responsibilities under the AML regime; hence, they are not expected to understand AML risk.

Some of the owners and employees, however, have AML knowledge because they are also owners or employees of pawnshop and were required to undergo AML/CFT training.

Quality of AML Policies and	Commitment and Leadership of Management (Medium Low)	Quality of AML Supervision (Low)	Effectiveness of Supervision/ Oversight Activities	Very Low
			Availability and Enforcement of Administrative Sanctions	Close to nothing
		Availability and Effectiveness of Entry Controls		Medium Low
Procedures (Medium		Availability and Enforcement of Criminal Sanctions		Medium Low
Low)	Comprehensiveness of AML Legal Framework			Medium
	Effectiveness of Compliance Function			Does not exist

The effectiveness of criminal sanctions is previously assessed as one of the requirements under the compliance level of staff. There is no record yet that a dealer, in his capacity as a dealer/employee of dealer or as a covered person, has been involved in money laundering or has been investigated or prosecuted for compliance concerns, as there is no enforcement of the AMLA in the sector due to lack of specific guidelines detailing its implementation.

In relation to the compliance function, the sector is not being monitored or regulated for AML/CFT compliance due to the absence of the AML/CFT guidelines. The AMLC and the appropriate government agencies are drafting rules and regulations that would address these deficiencies.

### **Supervision/Oversight Activities**

Jewelry dealers in precious metals and stones are required to register their businesses either with the Securities and Exchange Commission (SEC) or the Department of Trade and Industry (DTI). Neither the SEC nor the DTI, however, regulates or exercises supervision over their operations. For purposes of AML/CFT compliance, however, the AMLC is vested with the power to ensure the compliance of the sector. The AMLC is already in the process of coming up with a specific guidelines and regulation applicable to the sector. Further, the AMLC will soon be expanding its manpower to perform the compliance function.

### **Administrative Sanctions**

The AMLC, upon its discretion and after due notice and hearing, may impose administrative sanctions for violations of the AMLA, its RIRR and all AMLC issuances.

Considering, however, the absence of regular AML compliance checking, AMLA violations of jewelry dealers are not reported to the AMLC for possible imposition of sanctions.

# **Effectiveness of Entry Controls**

Jewelry dealers in precious metals and stones are required to register their businesses either with the Securities and Exchange Commission (SEC) or the Department of Trade and Industry (DTI) before they can operate. Neither the SEC nor the DTI, however, regulates or exercises supervision over their operations.

The registration process does not have a criminality check component. The registrants, however, are required to supply personal information including details of a government issued identification document. Applicants are also required to undertake an oath that the information supplied are true and correct, otherwise, they will be charged criminally, civilly and administratively.

#### AML Legal Framework

As a covered person, jewelry dealers in precious metals and stones are required to comply with the provisions of the AMLA, its RIRR and all AMLC issuances, which include customer due diligence, record-keeping and covered and suspicious transaction reporting. They are required to register with the AMLC for reporting purposes, and may be subjected to compliance checking by the AMLC to ensure effective implementation of the AMLA. However, a detailed regulation on how to implement the provisions of the AMLA with regard to dealers in precious metals and/or stones is very limited as the RIRR merely provides the general legal framework for all covered persons. The absence of detailed guidelines on how exactly do lawyers comply with the requirements of the AMLA limits, if not totally discourages, compliance by said dealers.

	Commitment and Leadership of Management	Medium Low
Quality of Operations (Medium Low)	Compliance Level of Staff	Medium Low
	Quality of CDD Framework	Low
	Effectiveness of Suspicious Activity Monitoring	Does Not Exist

# **Suspicious Activity Monitoring**

The sector is not yet being monitored or regulated for AML/CFT compliance due to the absence of the AML/CFT guidelines. Thus, no record as to the registration with AMLC and/or reporting of suspicious and covered transactions have been filed by dealers.

### Summary of Inherent Vulnerability Factors

#### Total Size/Volume of the Business (Low)

The jewelry sector is currently unregulated as an industry, particularly for AML purposes. Thus, it is difficult to get accurate figures from the industry players. The reports submitted to the Bureau of Internal Revenue are also not accurate because it has become difficult to determine if a business is involved in trading jewelry, precious metals or stones. Industry players are now registered as trading companies. Registered names would also not include anything that would identify them to be engaged in the trade of jewelry, precious metals or stones. Information available from the Bureau of

Investment (BOI) is also not representative of the sector because only those who are interested in taking advantage of BOI programs are submitting documents where information on imports and exports can be determined.

The Philippine jewelry industry is a fragmented industry composed of around 10,000 cottage-type firms. Majority of the manufacturers are small, with just five (5) to ten (10) workers and minimal tools and equipment. Only a few firms are corporations as majority are single proprietorships.

Data from the PSA show that the annual domestic turnover of the sector for 2012 was only at PhP3.93 Billion for fine jewelry and PhP1.22 Billion for costume jewelry, while export was at PhP1.1 Billion or USD24.77 Million. These figures are far from the figures used in the previous mutual assessment. Based on preliminary figures from the PSA covering the period from January to May 2017, export of fine jewelry is at USD11.69 Million.

### 2. Client-base profile of the Profession (Medium Risk)

The sector representatives during the 2014 risk assessment did not discuss the profile of their clients for various reasons. However, they disclosed that their more expensive products that may be used for money laundering are those individuals who have high net-worth. There are also substantial number of non-resident clients.

# 3. Level of Cash Activity Associated with the Business (Medium)

Payment method is a mix of cash, checks and credit card. There is no legal frame work that limits cash transaction, thus it is possible that some high net-worth clients are paying in cash.

### 4. Other vulnerable factors of the Profession

### Use of Agents (Medium)

It is a practice that jewelries are being sold through agents.

# Possible Anonymous use of the product in the profession (Available)

The lack of specific AML/CFT guidelines for the sector, the dealers are not performing any CDD when they are selling high value items. Thus, it is possible that precious metals or stones are being sold to fictitious or anonymous customer.

### Difficulty in tracing the transaction records

The dealers are not required to keep the record of their transactions other than those which are necessary for documenting sales for purposes of accounting and tax compliance. Thus, it is difficult and time consuming to perform the required CDD using the records or document being kept by the dealers.

# • Existence of ML typologies in the Abuse of the Profession

FATF has identified some typologies involving the use of the sector. There are, however, no known typology that happened locally.

# Use of the profession in tax/fraud schemes

Some jewelry dealers are registered as trading companies. These registered names do not include anything that would identify the companies to be engaged in the trade of jewelry, precious metals or stones.

#### Non-face-to-face Interaction with the Client

Jewelry, precious metals and stones may be purchased even without having face-to-face interaction with clients.

#### **ACTION PLAN**

Based on the overall assessment of the strength of AML controls, all controls require immediate attention but the top three (3) priorities are:

- 1. AML Knowledge of Business/Institution Staff
- 2. Effectiveness of Supervision/Oversight Activities
- 3. Effectiveness of Compliance Function (Organization)

	ACTION PLANS	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
•	AMLCS and Confederation of Philippine Jewelers, Inc. will coordinate as to schedule and other logistic details of orientation seminars.  Formalization of the AMLC Compliance group to undertake compliance monitoring and supervision.  Preparation of AML/CFT supervision and monitoring manual.  Preparation of AML/CFT preventive manual.  Appointment of a AML/CFT compliance officer  Registration with AMLC for reporting and training on reporting procedure  Review the applicability of the existing manual on	AMLC	Covered Person	1 <sup>st</sup> Quarter to 2 <sup>nd</sup> Quarter of 2018
	administrative sanctions			

# E. COMPANY SERVICE PROVIDERS

#### **INTRODUCTION**

The term Company Service Providers was part of the "Trust and Company Service Providers" term used and defined by the FATF in Recommendation 12 and the Glossary to the FATF 40+9 Recommendations referring to "all those persons and entities that, on a professional basis, participate in the creation, administration and management of trust and corporate vehicles."

Despite the essential and legitimate role of corporate vehicles, they can be used and have been used for unlawful purposes, including money laundering and terrorist financing, by disguising or converting the proceeds of unlawful activities. It has been said that this could be prevented if information on the legal and beneficial owner and the source of the corporate's assets.

The FATF Recommendations require countries to ensure that adequate, accurate and timely information on the beneficial ownership of corporate vehicles is available and can be assessed by competent authorities in a timely fashion. Otherwise, this may facilitate ML/TF by disguising the identity of known or suspected criminals, the true purpose of an account or property held by a corporate vehicle and/or the source of funds or property associated with a corporate vehicle. There is a need to have a regulatory and supervisory framework for CSPs

# Legal framework

In 2013, Republic Act No. 10365, otherwise known as An Act further strengthening the Anti-Money Laundering Law, amending for the purpose Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001", as amended, was passed, wherein the Philippines extended AML/CFT obligations to the Designated Non-Financial Businesses and Professional ("DNFBPs") sector, specifically the Company Service Providers ("CSPs") by including it as one of its covered persons.

Company Service Providers (CSPs) are now included in the AML regime of the country specifically transactions arising from the following:

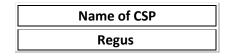
- (i) acting as a formation agent of juridical persons;
- (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons;
- (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and
- (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person.

#### Sectoral Vulnerability

The assessment made is based on the information gathered from Regus, Inc. ("Regus"), a company identified by the Securities and Exchange Commission ("SEC") as a CSP, and information gathered from the internet.

This assessment is limited to CSPs providing a registered office, business/administrative address or accommodation of a company.

Based on internet research, there are numerous companies in the Philippines that provide shared and virtual offices. Information on these companies is still being gathered by the group. All of these companies provide virtual office and serviced office services, while only five (5) of them acts as a formation agent by providing incorporation and compliance services.



Alchemy Business Center
Ascott Business Solutions
Cavali Business Center
CEO Suite
KMC Solutions
Makati Corp
MyOffice
New Wave Business Center
ProAccess Business Services
Servcorp
Towers Office
V Office
Worldnet Business Center
On Point Offices
Incubation Office Cross Coop
The Executive Center
Global Hub Serviced Offices Inc
Crosscoop Manila
OneAsia Center
Corporate Executive offices Inc.
eOffice.net
O2space.ph

Regus is the first CSP that provided information on the transactions being made by it. Their transactions are either through bank remittance, bank deposit (check or deposit to account) or credit card and no cash transactions are being made. As to the value, big payments were done through wire transfer and majority is international.

Despite the fact that the AML law is yet to be implemented in the sector, they are currently performing due diligence on their client as well as record keeping as a part of their international compliance considering that most of them have operations in other jurisdictions that requires AML compliance.

Reporting procedure, however, is not yet implemented in the sector. They believe that since their transactions passed through banks, the banks already reported the transactions as covered or suspicious, as the case may be.

Information on PEP clients is not yet available because this is not yet part of their monitoring procedure.

With regard to other companies, best efforts are being exerted by the group to gather additional information about the services they offer and the transactions made by them.

After considering data gathered, the overall vulnerability of the business is at MEDIUM HIGH.

Quality of CDD Framework (Medium Low)	Availability and Access to Beneficial Ownership Information	Medium Low
	Availability Reliable Identification Infrastructure	Medium Low
	Availability of Independent Information Sources	Low

# **Beneficial Ownership**

Though one of the documents being asked, a comprehensive information on the structure, management, control, and beneficial ownership in corporations, trusts and similar vehicles of their clients (limited to SEC documents) are not easily and readily available to CSPs. The CSPs, sometimes, act they no longer require this as part of their Customer Due Diligence requirements.

## Identification Infrastructure

The Philippines has no national identification system in place. Though the CSPs no longer verify the documents submitted by their potential/existing clients, the CSPs could write the authorities about the government-issued identity documents.

## **Independent Information Sources**

Independent and reliable sources of information to determine transaction patterns of their clients are not readily available and CSPs cannot easily access them. CSPs also not identify or verify their clients' transactional patters and commercial history.

Compliance Level of Staff	Effectiveness of Compliance Function	Low
	Availability and Enforcement of Criminal Sanctions	Medium Low
(Medium)	Integrity of Business/Profession Staff	Medium
	AML Knowledge of Business/Profession Staff	Medium Low

# **Compliance Function**

The CSPs do not have MLPPs, no compliance officer and no compliance department. However, they comply with the minimum information requirement and Record Keeping and follows the global policies on AML/CFT set by their parent company.

# **Criminal Sanctions**

The CSPs were considered as CPs in 2013 and are required to comply with the AML laws. Though general criminal sanctions are provided in the law, it was only in 2017 where the 2016 RIRRs are made effective. Thus, no criminal enforcement actions were done against CSPs or its individual members of management or staff in case of non-compliance with AML obligations.

# **Integrity of Business/Profession Staff**

There was no reported incident that the directors, managers and staff of CSPs were involved in any money laundering activity. However, information on vetting and training programs, and incidence of disciplinary actions for breach of integrity related rules of the staff were not provided.

## AML Knowledge of Business/Profession Staff

There are no appropriate AML training programs and materials. The last AML training that was conducted was two years ago. The management and staff are not aware of AML compliance, particularly its reporting obligations. However, global policies set by their parent company are being observed/followed.

	Commitment	Quality of AML	Effectiveness of Supervision/ Oversight Activities	Does not exist
Quality of	and Leadership of	Supervision (Does not exist)	Availability and Enforcement of Administrative Sanctions	Low
AML Policies and	Management (Low)	Availability and Effectiveness of Entry Controls  Availability and Enforcement of Criminal Sanctions		Low
Procedures (Medium Low)				Medium Low
Lowy	Comprehensiveness of AML Legal Framework			Medium
	Effectiveness of Compliance Function			Low

# Supervision/Oversight Activities

The AML supervision/oversight activities to be performed by a supervisory body are not specified/identified in the laws and regulations, particularly on clear supervision policies, procedures and manuals.

## **Administrative Sanctions**

The CSPs were considered as CPs in 2013 and are required to comply with the AML laws. Though general sanctions are provided in the law, it was only in 2017 where the 2016 RIRRs are made effective. Thus, no administrative enforcement actions were done against CSPs or its individual members of management or staff in case of non-compliance with AML obligations.

Also, considering the absence of regular AML compliance checking, AMLA violations of CPAs are not reported to the AMLC for possible imposition of sanctions.

## **Entry Controls**

There is no licensing body identified in the law that effectively carries out licensing and entry control duties. In fact, CSPs are only required to register with SEC and no secondary license is required to perform the services.

# <u>AML Legal Framework</u>

The CSPs are covered persons by virtue of RA 10365, which was made effective in 2013. Thus, the CSPS are required to comply with the provisions of the AMLA and of the 2016 Revised Implementing Rules and Regulations. However, the 2016 RIRRs do not provide specific rules and regulations for CSPs, particularly supervision over CSPs for AML compliance.

Effectiveness of compliance function and criminal sanctions are previously assessed under the AML combating factor - compliance level of staff.

	Commitment and Leadership of Management	Low
Quality of Operations	Compliance Level of Staff	Medium Low
(Low)	Quality of CDD Framework	Medium Low
	Effectiveness of Suspicious Activity Monitoring	Does not exist

## **Suspicious Activity Monitoring**

The CSPs do not have adequate and appropriate AML-monitoring and STR reporting systems. They still do not have a good understanding of the scope of their reporting obligations on suspicious transactions and activities, including what activities are covered or not covered.

Commitment and leadership of management, compliance level of staff and quality of CDD framework are assessed above.

# **ACTION PLAN**

Of all the AML combating controls assessed, the top 3 priorities include:

- 1. Effectiveness of Supervision/Oversight Activities
- 2. AML Knowledge of Business/Institution Staff
- 3. Effectiveness of Suspicious Activity Monitoring and Reporting

ACTION PLANS	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
AML knowledge of business and staff  • Information drive on AML risk	AMLC		3 <sup>rd</sup> Quarter of 2018
Comprehensive legal framework	Congress	AMLC	During the 17 <sup>th</sup> Congress

#### F. CAR DEALERS

#### **INTRODUCTION**

There are three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. The first is through the use of the financial system; the second involves the physical movement of money (e.g. through the use of cash couriers); and the third is through the physical movement of goods through the trade system. In recent years, the Financial Action Task Force has focused considerable attention on the first two of these methods. By comparison, the scope for abuse of the international trade system has received relatively little attention.

The international trade system is clearly subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist financiers. In part, these arise from the enormous volume of trade flows, which obscures individual transactions; the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements; the commingling of legitimate and illicit funds; and the limited resources that most customs agencies have available to detect suspicious trade transactions.

For the purpose of this study, trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.<sup>207</sup>

Studies in other jurisdictions revealed that one of the most prevalent property subject of a trade based money laundering is the sale of high value items more particularly motor vehicle, thus the conduct of this assessment on the sale of motor vehicles.

## SECTOR VULNERABILITY ASSESSMENT

The assessment is performed using official documents and data from open source. The vulnerability map, after assessing each input variable, showed an overall **MEDIUM** sector vulnerability.

Quality of CDD Framework (Medium)	Availability and Access to Beneficial Ownership Information	Medium
	Availability Reliable Identification Infrastructure	Medium High
	Availability of Independent Information Sources	Low

<sup>&</sup>lt;sup>207</sup> (Financial Action Task Force, 2006)

## **Beneficial Ownership Information**

Company registry for corporations, Securities and Exchange Commission, requires applicants to provide the list of the names of the shareholders and officers together with the amount of ownership in the company. The registry, however, does not check whether owners or shareholders have criminal records.

## **Identification Infrastructure**

The Philippines do not have a national identification system. This, however, does not affect the efficiency of the sector in identifying its customers by relying on government issued ID. It is also unusual for clients of car dealers to use fake identification documents because they will also have to undergo the mandatory CDD requirements when they purchase insurance coverage for the motor vehicle purchased.

## **Independent Information Sources**

Transaction pattern is not available, unless the transaction will be on credit. If the transaction will be on credit, the financial institutions who will undertake the transaction share a credit database.

## **PREVAILING PRACTICES**

A. Customer Identification and Verification (Know -your-customer Rule)

It is mandatory to take Identification requirements, because it will be used for registration process.

B. Reporting of Covered and Suspicious Transactions

This sector is not yet covered by the AML legal framework and is not required to file reports.

# C. Record Keeping

The sector is not yet covered by the AMLA, thus, they are not required to keep record of their transactions. They are, however, required to keep their record as required under the Tax Code.

Compliance Level of Staff (Low)	Effectiveness of Compliance Function	Does not exist
	Availability and Enforcement of Criminal Sanctions	Medium
	Integrity of Business/Profession Staff	Medium
	AML Knowledge of Business/Profession Staff	Close to nothing

## **Criminal Sanctions**

The Philippines has a legal framework that has sufficient criminal sanctions for money laundering and ancillary offenses that are dissuasive that would positively influence individual behavior patterns.

The AML legal framework applies to all individuals who may commit money laundering and predicate offenses. Unfortunately, since car dealers are not yet covered by the legal framework, it does not cover officers and employees of car dealers should they fail to comply with Customer Due Diligence, Record Keeping, and Reporting requirements of the Anti-Money Laundering Act of the Philippines.

# **Integrity of Business/Profession Staff**

Owners and employees are expected to act with integrity in conducting their businesses and would generally not allow their businesses to be used in furtherance of an unlawful activity or money laundering. Their limited knowledge of the money laundering risk and the absence of AML measures in place makes them vulnerable and possibly be facilitating money laundering involuntarily or unknowingly.

# AML Knowledge of Business/Profession Staff

The sector is not being monitored or regulated for AML/CFT compliance. The staff of the sector has no responsibilities under the AML regime; hence, they are not expected to understand AML risk.

	Commitment	Quality of AML Supervision	Effectiveness of Supervision/ Oversight Activities	Does not exist
Quality of	and Leadership of	(Does not exist) Availability and E		Does not exist
AML Policies and	Management (Low)	Availability and Effe	ctiveness of Entry Controls	Very Low
Procedures (Low)		Availability and Enfo	orcement of Criminal Sanctions	Medium
(2011)	Comprehensive	veness of AML Legal Framework		Does not exist
	Effectiveness o	of Compliance Function		Does not exist
	Commitment and Leadership of Management			Low
Quality of	Compliance Level of Staff			Low
Operations (Low)	Quality of CDD Framework			Medium
(2000)	Effectiveness o	f Suspicious Activity N	Does Not Exist	

# <u>AML Legal Framework, Supervision/Oversight Activities, Administrative Sanctions, Suspicious</u> Activity Monitoring

The sector is not currently being monitored and regulated for AML/CFT compliance and is not considered as a covered person under the AMLA.

# **Effectiveness of Entry Controls**

The sector is unregulated and only requires a business registration to operate the business. The business does not have a fit and proper requirement for its owner or officers other than the legal requirements on capitalization and other mandatory requirements.

**Criminal sanctions and effectiveness of compliance functions** are both assessed under the compliance level of staff.

#### INHERENT VULNERABILITY ASSESSMENT

## 1. Total Value of the Business – (Medium Low)

The automotive industry is estimated to have generated around 500,000 jobs for Filipinos and contributes PhP30 billion in annual taxes with investment of around PhP120 billion.

In 2016, around 360,000 new automotive vehicles were sold for an estimated value of PhP660 billion pesos or representing around 22% of the national budget for 2016.

In 2014 it was estimated that there were more than 270 dealers of brand new vehicles who are members of (Chamber of Automotive Manufacturers of the Philippines, Inc. (CAMPI) and around 200 independent dealers of second hand vehicles.

The importance of the automotive industry in fueling economic activities is significant that it merits attention and protection against criminals and money launderers to preserve its integrity. Considering the foregoing, the total value of the business is rated as **Medium Low**.

# 2. Client-base profile of the business (Low)

Based on the survey conducted by Carmudi<sup>208</sup>, buyers of new and used cars are attracted to the price range of around PhP800,000.00 or between PhP1.3 – PhP1.6 million marks. Analyst says that the market appears to be either younger nouveau rich or established individuals showcasing their wealth by buying higher priced vehicles.

Only few cars are sold to foreigners and according to dealers, they have not encountered clients who are purchasing vehicles on behalf of a beneficial owner.

## 3. Level of cash activity associated with the business (Medium)

Exact figure on how much cash transactions are received annually is not available. It is clear, however, that vehicle dealers accept payment in cash without regard to its source. For 2015-2016, however, majority of the vehicles sold were through bank financing.

In fact, data of the Bangko Sentral ng Pilipinas shows a yearly increase in the auto loan portfolio of the banking system in 2014, 209 2015 210 and 2016. 211

<sup>&</sup>lt;sup>208</sup> An online flat form for selling cars.

<sup>&</sup>lt;sup>209</sup> http://www.bsp.gov.ph/banking/pbs\_archives/2014/9.htm

<sup>&</sup>lt;sup>210</sup> http://www.bsp.gov.ph/banking/pbs\_archives/2015/9.htm

<sup>&</sup>lt;sup>211</sup> http://www.bsp.gov.ph/banking/pbs\_archives/2016/9.htm

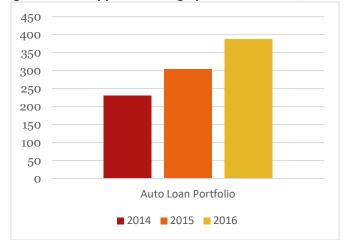


Figure 7-7. Philippine Banking System Auto Loan, in billion pesos

## 4. Other vulnerable factors of the business (High)

# Use of agents (High)

Some sales are generated by freelance agents who have no regard to AML/CFT risks.

# • Possible anonymous use of the product in the business (Not Available)

Clients have to be identified for purposes of registration and for processing of loan if it is purchased through bank financing.

# Difficulty in tracing the transactions (Easy to trace)

Dealers are required to keep their sales records and the purchases are required to be registered with the Land Transportation Office.

# • Existence of ML typologies on the abuse of the business (Exist but limited)

FATF and other AML related publications has identified the car dealers sector as vulnerable to money laundering abuse and identified different typologies.

# Use of the business in tax/fraud schemes – Electronic Commerce Act (Exist)

An incident was reported wherein criminal groups took advantage of the automobile industry as a means to defraud individual purchasers that also affected the car financing and vehicle insurance sector. The incident involved a syndicate who would induce individuals to purchase cars through financing and promise the car owners substantial monthly rental in addition to the monthly amortization that has to be paid, by allowing them to include their vehicle on an alleged fleet of vehicles that would be used for business. However, the cars will eventually be sold by the syndicate and will no longer pay the original owners.

# Non-face-to-face interaction with the client (Available)

It was learned in the interview of several sales executives and dealers that some do not verify the identity of their clients and that they accept payments in cash. For some cash transactions, purchases are done through representatives that would no longer require the physical appearance of the real purchaser. Customers only undergo robust Customer Due Diligence (CDD), which includes face-to-face if purchases of vehicle are through loan. The CDD, however, is due to the fact that banks and loan institutions are covered by the AMLA.

#### **ACTION PLAN**

Of the 12 variables assessed, the top 3 priorities are:

- 1. AML Knowledge of Business/Profession Staff
- 2. Effectiveness of Supervision/Oversight Activities
- 3. Comprehensiveness of AML Legal Framework

Considering the above priority variables, and the other identified gaps and deficiencies, the following are the recommended action plans:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
AML knowledge of business and staff  • Information drive on AML risk	AMLC		3 <sup>rd</sup> Quarter of 2018
Comprehensive legal framework	Congress	AMLC	During the 17 <sup>th</sup> Congress

# G. REAL ESTATE AGENTS (BROKERS)

#### **INTRODUCTION**

The Financial Action Task Force (FATF) recommended the inclusion of Real Estate Agents as part of the Designated Non-Financial Businesses and Professions (DNFBP) because of its inherent vulnerability to ML/TF. In the Philippines, however, only real estate brokers can engage in the business of acting as an agent of a party in a real estate transaction more particularly if it has to do with sale, purchase, exchange, mortgage, lease or joint ventures, or other similar transactions on real estate or any interest therein. This assessment is focused on real estate brokers.

Investment in the real-estate sector offers advantages both for law-abiding citizens and for those who would misuse the sector for criminal purposes. Real property has historically appreciated in value. Most importantly for misuse by criminals, however, is the facility the sector may provide for obscuring the true source of the funds and the identity of the (ultimate) beneficial owner of the real asset, which are two key elements of the money laundering process.

The real-estate sector is therefore of extraordinary importance to the economy in general and the financial system in particular. The widespread use of mechanisms allowing households to access the property market, the elimination of personal limitations on property ownership, the economic development and growth of tourism in many regions have all led to exponential growth in the number of financial transactions linked to real-estate. The extraordinary range of possibilities for misusing these processes also allows suspected criminals to integrate and enjoy illegally obtained funds.

Through the implementation of international standards in recent years, countries have put various measures into place within their formal financial sector — which includes, among others, banks and credit unions — in order to prevent money laundering and terrorist financing. Because of the tendency for illegal activity to move to other financial / economic areas that may have less formal oversight or where there is relatively less potential for detection, we must consider extending AML/CFT measures to other parts of our economies, if we want to respond successfully to this threat. For the real-estate sector, this would necessarily include such key players as real-estate brokers.<sup>212</sup>

<sup>&</sup>lt;sup>212</sup> (Financial Action Task Force / Organisation for Economic Co-operation and Development, 2007)

For purposes of this assessment real estate brokers will be assessed and not real estate agents because under Republic Act No. 9646, otherwise known as the "Real Estate Service Act of the Philippines", it is the real estate brokers who are allowed to facilitate the sale and purchase of real estate in the Philippines.

Real estate broker is defined under the law as:

a duly registered and licensed natural person who, for a professional fee, commission or other valuable consideration, acts as an agent of a party in a real estate transaction to offer, advertise, solicit, list, promote, mediate, negotiate or effect the meeting of the minds on the sale, purchase, exchange, mortgage, lease or joint venture, or other similar transactions on real estate or any interest therein.

#### SECTOR VULNERABILITY ASSESSMENT

The assessment is performed using official documents and data from open source.

Real AML regulation is absent in the real estate sector. Republic Act (RA) No. 9646 or the Real Estate Service Act (RESA) made the real estate profession a regulated profession just like doctors and lawyers. They are required to take a licensure exam with the Professional Regulations Commission (PRC) - Board of Real Estate Service and to adhere to their Code of Ethics and Responsibilities. The Board of Real Estate Service is tasked to be the policy maker, administrator of licensure examinations, promulgator, and enforcer of the rules and regulations necessary in carrying out the provisions of the law. Real Estate Broker License of has to be renewed every three (3) years. Those already licensed by the Department of Trade and Industry (DTI) at the time the law was passed were required to secure their licenses from the PRC without taking the examination. Section 14 of RESA lists having earned at least 120 units of Continuing Professional Development (CPD) education from an accredited real estate service training provider and passing the Professional Regulation Commission (PRC) licensure examination as requirements for a broker's license. In terms of other scholastic attainments, holding a relevant bachelor's from a state university or college or other educational institution duly recognized by the Commission on Higher Education (CHED) was enough to make a licensure application. "

However, as of May 2016, only Bachelor of Science in Real Estate Management (BS REM) degree holders are now qualified to take the broker's licensure exam. This is due to the additional condition in the RESA Law that should a course resulting in a bachelor's degree in a real estate service be implemented by the CHED, it subsequently become one of requirements for taking the licensure exam.

In October 2011, CHED Issued Memorandum Order No. 28, which had guidelines for the implementation of BS REM, a course aimed to develop real estate practitioners that are globally competitive and in pace with the business environment. As it was initially offered in select schools in 2012, a BS REM degree officially became a requirement for examinees upon the graduation of the course's first class in 2016. Because of this, in May 2016, there were only 39 BS REM graduates, with only 21 passing the exam. This is a far from the 5,499 passers out of 9,749 examinees in February 2016, the last time that non-BS REM degree holders were allowed to take the licensure exam.

As of 25 August 2017, the PRC-Board of Real Estate Service said that there are 30,232 registered real estate brokers.

The Real Estate Brokers Association of the Philippines, Inc. (REBAP), an association registered as an organization with the Securities and Exchange Commission reported that currently they have around

1,200 active members spread in their 27 chapters in the country. On the other hand, the Philippine Association of Real Estate Board (PAREB) have a membership of around 3,600. REBAP and PAREB are just two (2) of the many organization of real estate practitioner in the Philippines. These two have larger membership than other real estate practitioner in the Philippines. Both have the vision to promote, develop and advance the concepts and ideals of real estate practitioner in the Philippines.

The volume of turnover based on the statistics of Philippine Statistics Authority (PSA) is around P357 billion and P400 billion in 2013 and 2014, respectively. This volume translates to around 3% of the country's nominal GDP for 2014. While in 2016 the top real estate developers posted a net income of over PhP72 billion or 2.4% of the 2016 national budget.

Table 7-4. Real Estate Developers
TOP 10 EARNING REAL ESTATE DEVELOPERS IN 2016

DEVELOPER	2016 NET INCOME	2015 NET INCOME	
SM Prime Holdings	17.895 billion	23.306 billion	-23.22%
Ayala Land, Inc.	17.403 billion	15.205 billion	14.45%
Megaworld Corp.	9.272 billion	8.352 billion	11.02%
Vista Land & Lifescapes, Inc.	6.381 billion	5.762 billion	10.74%
Robinsons Land Corp.	6.150 billion	5.701 billion	7.88%
Federal Land, Inc.	4.629 billion	4.633 billion	-0.08%
Filinvest Land, Inc.	3.462 billion	3.244 billion	6.70%
8990 Holdings, Inc.	3.189 billion	3.166 billion	0.72%
Shang Properties, Inc.	2.461 billion	2.329 billion	5.66%
Belle Corp.	1.584 billion	1.023 billion	54.79%

Periods reported are year-to-date ending September 30, 2016, except for Robinsons Land, which is full fiscal year ending September 30, 2016. Figures are based on full disclosures made to the Philippine Stock Exchange.

The sector predominantly conducts business using non-cash transactions such as check or other services provided by banks. Cash payment is generally discouraged for control purposes. Internal financing arrangements also requires the posting of postdated checks that will be drawn against client's bank deposits. Cash transaction however, is not absent specially for those who are selling their own properties.

According to the Bangko Sentral ng Pilipinas' (BSP) report on total loans released by universal and commercial banks to the real estate sector, a total of PhP1.31 trillion loans were extended to borrowers by the end of the first quarter of this year, which corresponds to an increase of 21.5 percent compared to the same period in 2016. This substantial increase shows that there are more people buying real estate and that these purchases are being financed by banks.<sup>213</sup> Loans to the real estate sector accounted for 19.5 percent of the big banks' P6.75-trillion loan portfolio (TLP), which included interbank loan receivables (IBL). Minus the IBL, loans to the sector accounted for 20.1 percent of P6.55 trillion of the TLP.

Almost 25 percent of the real estate loans (REL), or P322.90 billion, consisted of residential loans, while more than 75 percent, or P994.85 billion, were loans extended to land developers, construction companies and other commercial borrowers.<sup>214</sup>

<sup>&</sup>lt;sup>213</sup> http://www.lamudi.com.ph/journal/flight-to-economy-and-efficiency-pinnacles-second-quarter-report/

<sup>&</sup>lt;sup>214</sup> http://www.manilatimes.net/real-estate-q1-loans-swell-21-p1-3t/328510/

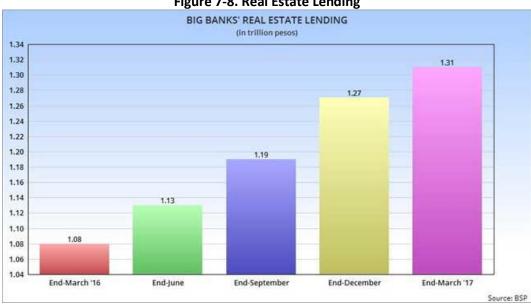


Figure 7-8. Real Estate Lending

According to the Philippine Statistics Authority (PSA), the volume of turnover of the sector is around PhP357 Billion and PhP400 Billion in 2013 and 2014, respectively. This volume translates to around 3% of the country's nominal GDP for 2014. On the other hand, Philippine banks' exposure to real estate as of end of 2012 was at PhP821.7 Billion and has grown to PhP1.5 trillion as of end of 2015. The difference in the amounts reported can be attributed to the loans granted by banks to both real estate developers and buyers. Further, this data supports the assumption that real estate purchases are predominantly made through the banking sector.

The PSA revealed that the Philippines' GDP grew by 6.6% in 4th quarter of 2016, driving the national GDP growth to 6.8 for the entire year. Three main industries contributed to this expansion, and one of them is the real estate, renting and business activities.

In recent years, the Philippine property sector proved itself to be a buoyant industry. It expanded by 9% in the 4th quarter of 2016, as compares to a 7.8% growth in 4th quarter in 2015. 215

In a survey conducted by the Urban Land Institute and Pricewaterhouse Cooper, Manila ranked fourth real estate investment destination in Asia-Pacific.<sup>216</sup> Aside from the fast growing economy and improvements in transparency and governance issues, the real estate sector is also seen to be benefitting from strong capital inflows from overseas Filipino workers (OFWs). According to KMC Mag Group's Midyear Report (2014), condominium production has shifted to serve the middle-income market, with OFWs comprising the bulk of the buyers from this bracket.

By end of 2016, there were 259,800 completed residential condominium units from the mid-range to high-end segments, of which around 6,600 completed in the fourth quarter of 2016.

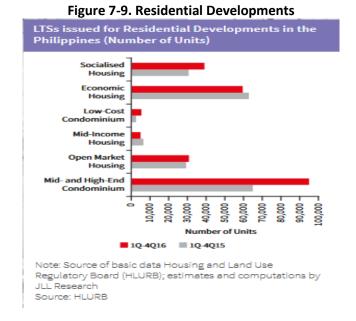
The number of licenses-to-sell (LTS) issued for residential developments in 2016, increased by 19% yo-y. It was observed that the LTS issued for mid to high-end increased by 46% y-o-y, while LTS issued for socialized housing grew by 27% y-o-y. On the other hand, LTS issued for other residential segments decreased with economic housing and open market housing down by 5% and 24% y-o-y, respectively.

<sup>&</sup>lt;sup>215</sup> https://www.openaccessbpo.com/blog/philippine-real-estate-sector-quick-guide-foreign-investors

<sup>&</sup>lt;sup>216</sup> Emerging Trends in Real Estate 2014,

 $https://www.pwc.com/sg/en/publications/assets/aprealestemerging\_2014.pdf.$ 

More than 700 projects were issued with LTS in 2016, totaling approximately to 235,000 residential units. <sup>217</sup>



The demand for residential condominium units across Metro Manila by sub-market was primarily sourced from starting families, young professionals, mid to high-income public and private local employees, local business people and local investors, especially for mid-range developments. Demand for residential condominium units maintained stable growth because of strong demand for residential condominium units from Overseas Filipino workers and expatriate employees/executives of MNCs.<sup>218</sup>

As a general rule, foreigners are not allowed to own real estate in the Philippines. The only exceptions are in cases where title passes through hereditary succession or in cases of condominium corporations, wherein foreigners can purchase not more than 40% interest as a whole in the condominium project.

Access on actual data as to the amount and frequency of international transactions relating to the sector are not readily available. However, it safe to assume that money coming from abroad are captured for AML reporting purposes by banks, wireless money transfers, and remittance agents.

Statistics on the number of PEPs who purchase real estate under their names is not readily available because monitoring is not required by law. Though the AMLA requires the Land Registration Authority (LRA) and all its Registries of Deeds to submit reports on all transactions in excess of PhP500,000.00, the AMLC do not receive reports from the LRA nor does it have direct access to such transactions. However, the AMLC can request information and relevant data from the LRA in the course of its ML investigations.

No ML activities involving real estate brokers have been reported. There are however, forfeiture proceedings on some real estate properties owned by individuals charged with ML and/or predicate crimes. As of December 2016 the total value of real properties subject of civil forfeiture was estimated at PhP402 Million, which is not significant in relation to the volume of turnover.

<sup>&</sup>lt;sup>217</sup> Philippine Property Digest Q42016, JLL Publication

<sup>&</sup>lt;sup>218</sup> Ibid

Considering all of the foregoing, plus factoring in the licensing requirements and the Code of Conduct for real estate brokers, offset by the fact that real estate brokers are not covered persons under the AMLA, as amended, the vulnerability of real estate brokers for ML is rated at **MEDIUM**.

The overall assessment of the strength of AML controls is anchored on the following 12 general input variables, considering guidelines based on applicable FATF Recommendations and result of self-assessment, as summarized in the table below:

# **Summary of AML Controls**

GENERAL AML CONTROLS	EQUIVALENT	
Comprehensiveness of AML Legal Framework	Does not exist	
Effectiveness of Supervision/Oversight Activities	Does not exist	
Availability and Enforcement of Administrative Sanctions	Does not exist	
Availability and Enforcement of Criminal Sanctions	Low	
Availability and Effectiveness of Entry Controls	Medium High	
Integrity of Business/Profession Staff	Low	
AML Knowledge of Business/Profession Staff	Close to nothing	
Effectiveness of Compliance Function (Organization)	Does not exist	
Effectiveness of Suspicious Activity Monitoring and Reporting	Does not Exist	
Availability and Access to Beneficial Ownership Information	Medium Low	
Availability of Reliable Identification Infrastructure	Medium High	
Availability of Independent Information Sources	Medium	

# **ACTION PLAN**

Of the 12 input variables assessed, the top 3 priorities are:

- 1. AML Knowledge of Business/Profession Staff
- 2. Effectiveness of Supervision/Oversight Activities
- 3. Comprehensiveness of AML Legal Framework

Considering the foregoing, the following are the recommended action plans:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
AML knowledge of business and staff	AMLC		3 <sup>rd</sup> Quarter of 2018
<ul> <li>Information drive on AML risk</li> </ul>			
Comprehensive legal framework	Congress	AMLC	During the 17 <sup>th</sup> Congress

#### VIII. FINANCIAL INCLUSION PRODUCTS

#### **EXECUTIVE SUMMARY**

In the BSP, financial inclusion is considered as a strategic objective that can be pursued alongside the traditional mandates of price stability, financial stability, and payment system efficiency. This is in recognition that "a strong and stable macroeconomic and financial environment, to be truly meaningful, needs to be inclusive, to create jobs, and to improve welfare."<sup>219</sup>

Recognizing that advancing financial inclusion requires a whole-of-government approach, the BSP together with fourteen (14) other government agencies launched the National Strategy for Financial Inclusion (NSFI) in 2015. The NSFI serves as a platform for public and private sector collaboration to harmonize initiatives and foster a more efficient process to achieve the shared vision of financial inclusion.<sup>220</sup>

As a policy objective, financial inclusion is considered inter-dependent with financial stability, financial integrity and consumer protection. The policymaking approach is to balance these objectives through proportionate regulations that enhance financial access; protect consumers' rights; and ensure safety, soundness and integrity of the financial system. Recently, the BSP together with the Consultative Group to Assist the Poor (CGAP) completed a research exercise analyzing how linkages among Inclusion, Stability, Integrity and Protection (I-SIP Framework) have been managed in the case of several policies such as microfinance, micro-banking office, e-money, and pawnshops.<sup>221</sup>

One of the findings in the I-SIP study is that the absence of a national identification (ID) system in the Philippines continues to present Know-Your-Customer (KYC) challenge for financial services providers. While the acceptance of alternative forms of identification for lower-risk products and the loosening of KYC requirements have been helpful, these have not been sufficient to facilitate expanding financial inclusion into unserved and underserved population segments.

The issuance of BSP Circular 950 (dated 15 March 2017) offers the potential to address existing barriers in customer onboarding. It allows BSP-supervised financial institutions to implement reduced KYC rules for certain low-risk accounts and use technology for face-to-face contact requirements. These amendments will facilitate frictionless onboarding which is currently a major pain point for those serving the low-income segment. The BSP is also closely coordinating with government on ways to develop a biometric ID system that will facilitate the provision of more efficient services, including financial services, especially to those who have been disenfranchised due to lack of an acceptable ID.

Looking at the range of financial services and considering the ones focused on financial inclusion that have significant presence in the country, the assessment in this section will cover the following specific financial inclusion products: 1) microfinance loans, 2) microdeposit accounts, 3) micro-insurance, 4) electronic money as a digital channel for retail payments, and 5) pawning and remittance services of pawnshops.

Using the assessment tool provided for these products, the general assessment is  $\underline{LOW}$  not only because of the small amounts (the products generally have threshold amounts) but also the very

<sup>&</sup>lt;sup>219</sup> BSP Governor Nestor A. Espenilla, Jr. in his inaugural speech as BSP Governor, 3 July 2017

<sup>&</sup>lt;sup>220</sup> Please see Annex for the list of financial inclusion stakeholders

<sup>&</sup>lt;sup>221</sup> Financial Inclusion, Stability, Integrity and Protection: Observations and Lessons for the I-SIP Approach from the Philippines (April 2017)

limited and well-defined product functionalities and target market that is typically the underserved local population. The data available also supports such assessment. The only product that has a low to medium assessment is the remittance service of pawnshops due to the ability to make cross-border payments without amount thresholds. The risks however are mitigated by existing mechanisms and proposed measures.

Product	ML Risk	TF Risk
Microfinance Loans	Low	Low
Microdeposits	Low	Low
Microinsurance	Low	Low
Electronic Money	Low	Low
Pawning	Low Low	
Remittance thru pawnshops	Low to Medium	Low to Medium

The abovementioned products and services are provided by institutions regulated by different authorities which highlight the importance of data sharing and inter-regulator coordination. The delivery of these products sometimes necessitates partnerships with other providers. As an example, micro-insurance provided by a licensed insurance company can be distributed through banks; and emoney issued by a licensed e-money issuer can use pawnshops as cash-in and cash-out points. These models allow for the more holistic view of provider ecosystems.

Moving forward, data on financial inclusion products will be continuously gathered to ensure that the ongoing understanding of the business models is accurate and can inform a proper ML/TF assessment. The product and technological innovations that are bound to spring forth from existing models will likewise be subject to the same approach as the assessed products in terms of balancing the objectives of inclusion with other policy objectives such as integrity. In terms of the product that was not considered low risk, particularly the remittance services of pawnshops, recent amendments to both the pawnshop and the remittance agent regulations have the potential to address such issues.

## **INTRODUCTION**

The definition of financial inclusion has two important components. "Effective access" means that financial services are not only available and accessible but also appropriately designed, relevant and of good quality to lead to actual usage that can benefit those accessing these services. "Wide range" refers to a full suite of basic financial services for different market segments, particularly those that are traditionally unserved/underserved by formal financial institutions. Such services include savings, credit, payments, remittances and insurance. The Philippine Development Plan 2017-2022 identifies financial inclusion as a component of the government's vision for the financial sector, to support the government's inclusive growth agenda.

Access to financial services is important for every household and business. Recent empirical evidence indicates that access to basic financial services such as savings, payments and credit make a substantial positive difference in people's lives. Financial inclusion therefore carries the potential of improving the well-being of the poor and the growth of micro, small and medium enterprises. This growing body of literature suggests that greater financial inclusion contributes to financial stability and economic development and is critical for achieving inclusive growth. An inclusive financial system is not only progrowth but also pro-poor, which can reduce income inequality and poverty.

Data on access and usage of formal financial services in the Philippines suggest that the country's financial system has become more inclusive over the years. In terms of access, the number of bank branches from 2015 to 2016 increased by 3.9% from 10,710 to 11,129 offices covering 64% of all cities

and municipalities in the country, while automated teller machines (ATMs) grew by 10.2% from 17,314 to 19,081 over the same period.<sup>222</sup> Non-bank financial service providers including credit cooperatives, non-stock savings and loan associations, microfinance non-government organizations, pawnshops, remittance agents, money changers, foreign exchange dealers and electronic money agents remain important access points especially in those areas without physical banking presence. Their presence translates to more than 60,000 access points in addition to banks. About 72% of cities and municipalities without banking offices are being served by these providers.<sup>223</sup>

Usage of formal financial products is generally increasing, as gleaned from the growth of the value of bank deposits, 13.8%, and loans, 17.8%, between end 2015 and end 2016. The total number of deposit accounts increased by 5% from 50.9 Million to 53.5 Million during the same period. In terms of microfinance delivery, significant strides have been achieved. Within a year from the time when microfinance has been recognized as a legitimate banking activity (2001), about 119 banks were extending microcredit worth PhP2.6 Billion to 390,635 borrowers. By end 2016, there are 168 banks serving 1.7 million clients with credit amounting to PhP13.7 Million. Microcredit has eventually expanded to include other products such as microfinance housing<sup>224</sup>, micro-agri<sup>225</sup>, and microfinance plus loans<sup>226</sup>, or those credit products with amounts higher than the value of traditional micro-loans.

Despite these gains, the use of formal financial services still leaves much to be desired. The National Baseline Survey on Financial Inclusion underscores that of those Filipino adults who save, 68% keep their savings at home. The 2014 World Bank Global Findex reports that the percentage of Filipino adults with an account with a formal financial institution increased to 31% from 27% in 2011. However, compared with its peers, the country is behind in the usage of formal accounts, while being slightly ahead with respect to formal credit.

#### **Regulatory Framework**

In 2014 to 2016, the Economist Intelligence Unit recognized the Philippines as the best in Asia and top three globally in terms of having a conducive environment for financial inclusion. This environment, characterized by enabling policies and regulations, catalyzes the development of a financial system that serves not only the relatively well-off clients and big businesses; but also the poor, low-income population that are currently unbanked or underserved.

Proportionality is the key in defining the regulatory approach for financial inclusion. Useful innovations need not be stifled but instead be allowed to operate in an environment where the risks associated with such innovations are adequately understood and addressed, and where there is a judicious and proportionate application of sound principles. For these to work, it is important that all players and financial service providers are properly and proportionately regulated to ensure consumer protection, financial system stability and integrity.

For the period 2015 onwards, the BSP issued the following policies and regulations supportive of financial inclusion:

<sup>&</sup>lt;sup>222</sup> Unless otherwise stated, all data are from Bangko Sentral ng Pilipinas (BSP).

<sup>&</sup>lt;sup>223</sup> Or 396 out of 595 unbanked cities and municipalities.

<sup>&</sup>lt;sup>224</sup> BSP Circular 678 dated 6 January 2010.

<sup>&</sup>lt;sup>225</sup> BSP Circular 680 dated 3 February 2010.

<sup>&</sup>lt;sup>226</sup> BSP Circular 744 dated 28 December 2011.

<sup>&</sup>lt;sup>227</sup> BSP National Baseline Survey on Financial Inclusion 2015.

Percentage of adult population in East Asia and Pacific with formal accounts is 69%; for lower income countries, 42.7%.

# I. Microfinance Regulations

- Circular 868 (26 January 2015) expands the range of services that can be delivered in micro-banking offices (MBOs) and waives the collection of processing fee for banking offices that will be established in unbanked cities and municipalities.
- Circular 901 (29 January 2016) amends Sec. X151 of the Manual of Regulation for Banks (MORB) to capture the entire procedure in opening micro-deposits in MBOs, including the approval and actual opening of accounts and being able to make an initial deposit, subject to appropriate internal controls.
- Circular 908 (14 March 2016) approves the adoption of the agricultural value chain financing framework as an effective and organized approach to channel financing to the agriculture and fisheries sectors and promote financial inclusion.
- Circular 929 (28 October 2016) amends Subsection X102.5 of the MORB to allow the conversion of microfinance-oriented thrift/rural banks/branches to regular banks/branches.

# II. Pawnshops and Money Service Business Regulations

- Circular 938 (23 December 2016) enhances existing regulations on pawnshops to ensure these entities are properly supervised for their effective compliance with AML and internal control rules and guidelines. Pawnshop operators are also now subject to stricter fit and proper rules and standards of corporate governance as applicable.
- Circular 942 (20 January 2017 2017) introduces the concept of Remittance and Transfer Companies (RTCs) which refer to any entity that provides Money or Value Transfer Services (MVTS) such as Remittance Agents, Remittance Platform Providers, and E-money Issuers; introduces a network-based approach to regulation wherein the entity that operates a remittance business shall be held responsible for the operation of its remittance network and accreditation of its Remittance Sub-agents (RSAs); amends the requirements for registration and adopting a classification of money service businesses (MSBs) based on benchmark capital, among others.

## III. Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)

 Circular 950 (15 March 2017) allows covered institutions to implement reduced Know-Your-Customer (KYC) rules for certain low-risk accounts and use technology for faceto-face contact requirements.

# IV. Digital Finance Ecosystem

Circular 940 (20 January 2017) allows banks to serve clients through cash agents which
can accept and disburse cash on behalf of the bank. Cash agents can also perform
Know-Your-Customer procedures as well as collect and forward application
documents for loan and account opening. They may also sell and service insurance as
may be authorized by the Insurance Commission. These cash agents are typically
cash-rich third party entities with many outlets that conduct regular business in fixed
locations anywhere in the country, such as convenience stores, pharmacies and other
highly accessible retail outlets.

• Circular 944 (6 February 2017) regulates entities that use virtual currency as the underlying instrument for remittance. Regulating virtual currency entities signifies the BSP's acknowledgement of virtual currency as an innovative instrument that can facilitate the speed and affordability of remittance and payment transactions.

## **FINANCIAL INCLUSION PRODUCTS**

In the Philippines, inclusion-friendly products include microfinance loans (microenterprise, micro-agri, housing microfinance, microfinance plus); microdeposits; microinsurance; pawning services; and low value payment services through electronic money (e-money) stored in a cash card or a mobile phone e-wallet.

#### A. MICROFINANCE LOANS

Target Clients. Microfinance loans are small value loans targeting microenterpreneurs. There are different types of loans depending on the activity that is financed (i.e., microenterprise loans, loans to growing microenterprises, housing microfinance loans, micro-agri loans). Clients are generally, poor and low-income microentrepreneur individuals, and those that come from basic sectors that are generally unserved/underserved by formal financial institutions (e.g., farmers and fishermen, urban poor, seasonal workers).

*Providers.* Microfinance loans are offered by three (3) types of entities collectively known as microfinance institutions (MFIs): 1. Banks with microfinance operations under BSP supervision; 2. Savings and credit cooperatives under the supervision of the Cooperative Development Authority (CDA); and 3. Microfinance non-government organizations registered under the Securities and Exchange Commission (SEC).

The regulatory environment for microfinance NGOs is strengthened by the passage of R.A. No. 10693 in November 2015, with its Implementing Rules and Regulations issued on 16 August 2016. The Microfinance NGO Regulatory Council has been created to institute a system of accreditation for microfinance NGOs and monitor their performance to ensure compliance with the provisions of R.A. No. 10693.

Microfinance loans can also be offered by financing companies and lending companies. R.A. No. 5980, as amended by R.A. No. 8556, or the "Financing Company Act," defines "financing companies" as "corporations, or partnerships, except those regulated by the BSP, the IC and the CDA, which are primarily organized for the purpose of extending credit facilities to consumers and to industrial, commercial, or agricultural enterprises, either by discounting or factoring commercial papers or accounts receivable, or by buying and selling contracts, leases, chattel mortgages, or other evidences of indebtedness, or by leasing of motor vehicles, heavy equipment and industrial machinery, business and office machine and equipment, appliances."

*Product Features*. The following are the features of each type of microfinance loan:

 Microenterprise Loans. Small, short-term loans granted to the basic sectors (as defined under the Social Reform and Poverty Alleviation Act of 1997), and to poor and low-income households, for their microenterprises and small businesses to enable them to raise income levels and improve their living standards. The maximum loanable amount is PhP150,000 and the basis for grant is the borrower's cash flow for their growing microenterprise and small business.<sup>229</sup> Loans are typically

<sup>&</sup>lt;sup>229</sup> Financial Inclusion in the Philippines. Issue No. 2, 2nd Quarter 2013. Bangko Sentral ng Pilipinas.

unsecured or use collateral substitutes like households assets. Amortization may be daily, weekly, bi-monthly or monthly, depending on the cash flow of borrowers. Interest rates are at par with prevailing market rates to enable lenders to recover financial and operating costs. Borrowers are exempted from the usual loan documentation requirements, given the lenders' well-defined microfinance policies, the close supervision of borrowers' projects, suitable loan tracking and monitoring system, and the adequate provisioning for loans classified as portfolio-at-risk.<sup>230</sup>

- Microenterprise Loan Plus. This is also called "Microfinance Plus." Targeted to clients that have a
  track record of at least two (2) microenterprise loan cycles in the PhP50,000 to PhP150,000 range;
  with demonstrated business success; increased credit demand; and subsequent increased
  capacity to pay. Loans range from PhP150,001 to PhP300,000 and the basis for the grant is the
  borrower's cash flow for their growing microenterprises and small business.<sup>231</sup> The borrower must
  also have a savings account.<sup>232</sup>
- Housing Microfinance Loans. Loans granted for home improvements, house construction or lot acquisition, based on the microfinance principles mentioned above. Targeted for existing microenterprise loan clients and new clients qualified for microfinance loans. Maximum loan amount is PhP300,000 for house construction or lot acquisition, payable up to 15 years. Maximum loan amount for house improvements is PhP150,000, payable up to five (5) years. Loan value may be up to 90% of the appraised value of real estate mortgage (REM) or of the acceptable valuation in cases of usufruct, lease, freehold, right to occupy or build. Amortization is frequent with amount not exceeding a reasonable percentage of the borrower's income, as determined through a cash flow analysis.<sup>233</sup>
- Micro-AgriLoans. Loans granted to small farmers with farm and off-farm income generation activities, based on the microfinance principles mentioned above. Targeted for existing microenterprise loan clients with good track record. Maximum loan amount is PhP150,000, payable up to 12 months; amortization is frequent, with option for lump sum payment of up to 40% of total loan amount, depending on the crop or production cycle.<sup>234</sup>

# **Money Laundering Risk for Microfinance Loans**

The ML risk for microfinance loans is generally **LOW**, not only due to the size of the loan and the prescribed threshold amounts, but also due to clearly defined product features and existence of risk-mitigants for the product. Microfinance loans are granted by providers licensed by government regulators. Anonymous use of the product is not possible since they are mandated to conduct KYC procedures prior to customer on-boarding. Transactions are generally face-to-face and often conducted onsite (in or near clients' place of residence) by authorized loan officers. Non-face to face account opening and doing of transactions are now allowed in view of BSP Circular 950. There is frequent interface and close relationship between loan officers and clients, given the microfinance product design, features, schedule of amortization, and loan monitoring requirements. The number of transactions are unlimited (e.g. no cap on loan cycles) but the amounts are generally low (e.g. average PhP5,000 – PhP15,000 depending on type of provider).

<sup>232</sup> BSP Circular 744.

<sup>&</sup>lt;sup>230</sup> Subsection X361, Manual of Regulations for Banks or MORB.

<sup>&</sup>lt;sup>231</sup> Ibid.

<sup>&</sup>lt;sup>233</sup> Subsection X361, MORB.

<sup>&</sup>lt;sup>234</sup> Subsection X361, MORB.

## **Terrorist Financing Risk for Microfinance Loans**

The TF risk for microfinance loans is generally **LOW** because loan products are availed of only by natural persons who are Filipino citizens and who are residing in the country. While banks with microfinance operations may rely on authorized third party entities or outsource their KYC, the decision to provide credit still rests with the bank. The credit cooperatives and microfinance NGOs only lend to their members within the communities they serve. Use of banking correspondents or agents is now allowed in view of BSP Circular 940. Since there is no cross-border transaction, there is no possibility of transactions to and from high-risk jurisdictions.

Notably, there is no history or record of financial crimes. Banks with microfinance operations, regulated and supervised by the BSP, have no cases of financial crimes related to microfinance loans in the past 14 years, as validated by bank examiners.

#### **B. MICRO-DEPOSITS**

Growth in the number of MBOs has contributed significantly to improved access to and usage of financial services in the Philippines.

One of the services being offered by micro-banking offices (MBOs) is micro-deposit. A micro-deposit account primarily caters to the banking needs and services of the basic sectors, low-income and unserved/underserved clients as well as the overseas Filipinos and their beneficiaries. Clients include those involved in the agriculture sector such as farmers and fishers, small entrepreneurs and members of the informal sector such as street vendors.

What makes it distinct from a regular deposit account, is that it has a minimum maintaining balance of not exceeding PhP100; not subject to dormancy charges; and has an average daily balance of not exceeding PhP40,000.<sup>235</sup>

Initially, MBOs were only allowed to perform customer identification process and facilitate account activation, but the approval and actual opening of deposit accounts were done only at the head office or branch. Thus, clients who want to transact in MBOs would therefore still need to go to a head office or branch to open a deposit account. This practice did not fully capture the potential of micro-banking offices as a banking presence in remote and rural areas where travelling to a bank branch may be prohibitive in terms of cost.

In 2016, MBOs have been allowed to approve, open and accept micro-deposits including initial deposits and service withdrawals thereof. Thus, MBOs have been allowed to complete the process of account opening from application up to the acceptance of initial deposit, provided that the necessary controls are in place.<sup>236</sup> This aims to expand the range of services that can be performed in MBOs in line with the BSP's thrust to promote greater access to a wide range of financial services for all Filipinos.<sup>237</sup>

Regular bank branches continue to rise in number but concentrated in Metro Manila. In that sense, MBOs being low-cost banking infrastructure, established in municipalities where it is not feasible to set up a regular branch, contributed more to financial inclusion by extending the reach of financial services to underserved and unserved areas.

\_

<sup>&</sup>lt;sup>235</sup> BSP Circulars 694, as amended by Circular 796.

<sup>&</sup>lt;sup>236</sup> BSP Circular 901, Amendment to Sec. x151 of the MORB on the Activities and Services Allowable for Micro-Banking Offices

<sup>&</sup>lt;sup>237</sup> Ibid.

Most municipalities that were previously unbanked are now enjoying access to banking services because of MBOs. Most MBOs are located in Calabarzon (Cavite, Laguna, Batangas, Rizal and Quezon), Bicol, Western Visayas and Mimaropa (Mindoro, Marinduque, Romblon and Palawan).

As of end 2016, there were 691 MBOs, an increase of 28% from 540 as of end 2015. The number of local governments units (LGUs) with MBOs grew by 24% to 418 in 2016 from 338 LGUs in 2015. To date, 84 municipalities are being served by MBOs alone.

The total amount of micro-deposits increased by 33% to PhP6.9 billion in 2016 from P5.2 billion in 2015. Micro-deposit accounts grew at an average year-on-year (2012-2016) rate of 31%, which is faster than the growth of other deposit products (6.5%).

## **Money Laundering Risk for Micro-deposits**

Despite the expansion of the functionalities of the MBOs, the ML risk for micro-deposit remains to be **LOW**. Primarily because of a low value threshold and because of the existence of risk mitigants.

Increase in the functionalities of the MBOs to facilitate completion of the account opening process are subject to conditions. MBOs shall only perform the transactional activities they have specifically applied for and had been authorized by the Bangko Sentral to perform. Subsequent enhancements are likewise subject to prior BSP approval.

The fact that micro-deposits are provided only by banks, which are prudentially regulated and supervised by the BSP, greatly contribute to the sustained low ML risk of micro-deposits. These accounts cannot be opened without KYC and face-to-face compliance, which may be done through outsourcing or third-party reliance. The decision to on-board a customer and open the account remains with the bank. The number of microdeposit transactions is unlimited, but the average daily balance threshold must be observed. Compliance is verified through supervision and examination.

# **Terrorist Financing Risk for Micro-deposits**

Likewise, the TF risk for microdeposits continues to be <u>LOW</u>. The value thresholds and the existing risk mitigants for the product significantly contribute for such continuity. This product is not offered to non-residents and cross-border transaction is not possible. Hence, there is no possibility of transactions to and from high-risk jurisdictions. Further, transfers to microdeposit accounts by a third party (e.g., overseas Filipino worker) are possible through electronic channels but the KYC aspect for the remitter is undertaken by remittance agents.

#### C. MICRO-INSURANCE

Micro-insurance basically refers to insurance products which are tailor-fitted to meet the risk protection needs of the low-income sector.<sup>238</sup> In the absence of ML/TF regulations particular to micro-insurance products, the general ML/TF rules applicable to insurance products are applied to micro-insurance.

To ensure that micro-insurance products remain affordable, premiums on a daily basis are mandated not to exceed 7.5% of the minimum daily wage rate of non-agricultural workers in Metro Manila.<sup>239</sup>

<sup>&</sup>lt;sup>238</sup> See also study of Asian Development Bank on Micro-insurance in the Philippines.

<sup>&</sup>lt;sup>239</sup> Based on the current rate of Php491, that would mean a daily premium of PhP37 or roughly PhP1,105 a month, maximum.

Correspondingly, micro-insurance products have maximum allowable benefits not exceeding 1,000 times the minimum daily wage rate of non-agricultural workers in Metro Manila. Given the transaction ceilings, micro-insurance businesses do not have covered transaction reports. <sup>241</sup>

Micro-insurance providers are given the prerogative to limit the number of micro-insurance policies that clients may avail of. However, clients may avail of various micro-insurance policies from more than one micro-insurance provider. Within a provider, the number of transactions is limited to three (3), but no limit was set on the access to different providers. It is generally offered to residents and citizens only due to its small value and the nature and purpose of the products. Hence, the client or customer risk is very low. Moreover, the risk of funds being received from high risk jurisdictions is almost negligible.

Since the premiums are relatively low, there is reduced customer due diligence in availing of micro-insurance products. However, anonymous purchases of a micro-insurance policy are not allowed as the client/applicant must personally fill up the application form and present one (1) photo-bearing identification card or any acceptable substitute document. The same relaxed procedure is observed for claims processing especially when the insured/beneficiaries are usually known to the management. Simplified claims requirements enable micro-insurance providers to comply with the regulation of settling claims within ten (10) working days upon filing of claim and submission of required documents.

Accredited insurance companies, cooperative insurance societies and mutual benefit associations provide micro-insurance products. The distribution of these products must be through licensed micro-insurance brokers or agents. Legal persons or entities such as microfinance institutions (MFIs) and cooperatives may also be licensed as agents provided that they offer or sell micro-insurance products to their customers or members only.<sup>242</sup> MFIs, including banks with MFI operations, may be licensed as agents of micro-insurance products, subject to regulations of both the BSP and the IC.<sup>243</sup>

While brokers and agents are aware of their CDD and reportorial obligations, there is a need to ascertain whether they undergo adequate training on how to identify unusual and suspicious transactions.

# Money Laundering and Terrorism Financing Risks for Micro-Insurance

The ML/TF risk for micro-insurance is generally <u>LOW</u> due to size, clearly defined product features suited to the target market, and existing risk mitigants. It is not offered to non-residents, and anonymous use of the product is not possible. The value and the number of the transactions (per provider) are limited and cross border transactions are not allowed.

Basic KYC, including face-to-face account opening, is required, although the process/documentation is simplified to accommodate the targeted low-income clients. Moreover, the product is generally offered to Philippine residents only.

The usage of micro-insurance products to perpetrate ML/TF activities is not known nor are there any reported cases that relate these products to financial crimes or activities. Micro-insurance products sold in the market must adhere to the rules and regulations set by the IC and must have an approval

<sup>&</sup>lt;sup>240</sup> About PhP491,000 based on the PhP491 minimum wage rate.

<sup>&</sup>lt;sup>241</sup> Sec. 3(b) and 9(c) of Republic Act 9160 or the Anti-Money Laundering Act, as amended defines covered transactions and reportorial requirements governing the same.

<sup>&</sup>lt;sup>242</sup>*Id*, note 6.

<sup>&</sup>lt;sup>243</sup>Subsection 2361.8, MORB.

prior to distribution. Given that there are strict procedures prior to the rolling out these products and that this product caters to the low-income sector, fraudulent activities using this product are very low. Notwithstanding the low risk, licensed agents or brokers for micro-insurance products should be trained more in ML/TF in order to identify and/or control possible ML/TF threats.

#### D. PAWNING AND REMITTANCE SERVICES OF PAWNSHOPS

In the Philippines, pawning<sup>244</sup> is the usual mode of having fast cash especially in cases of unforeseen and immediate need of the unbanked and under-banked sector. Pawnshops play a crucial role in filling in the gap between the demand for financial services and their accessibility in the countryside.

In 2016, BSP issued Circular 938<sup>245</sup> which replaced the existing implementing rules and regulations of Presidential Decree No. 114 also known as the Pawnshop Regulation Act.<sup>246</sup>

The new rules are designed to enhance consumer protection and foster confidence in the pawnshop industry by the pawning public. For instance, proprietors, partners, incorporators, directors, stockholders and officers of pawnshops must meet certain "fit and proper" standards to ensure that pawnshops are owned and run by people without any derogatory record and to promote good governance.

Under the new rules, there would be four classifications of pawnshop operator licenses. These are "A" for basic pawnshop business with not more than 10 offices; "B" for those with more than 10 offices and with or without BSP-registered corollary business activities excluding remittances; "C" for those with more than 10 offices and with remittance operations; and "D" for virtual operators or those engaged in electronic pawning.

The BSP requires a minimum paid up capital for P100,000 for class "A" pawnshops, P1 million for class "B", and P50 million for both "C" and "D." The existing statutory capital of P100,000 has become too small and it is susceptible to the proliferation of "fly-by-night" operators.

As a prerequisite for the issuance by the BSP of the authority to operate, proponents are required to attend a briefing on pawnshop regulations and a seminar on the Anti-Money Laundering Act.

Further, for transparency and to minimize malpractices, pawnshops will be required to post in their premises the Acknowledgement of Registration or Authority to Operate issued by the BSP, business days and hours of the pawnshop, their interest rate and charges for loans, among others.

Under the law, pawners have 90 days after maturity to redeem their pawned articles and pawnshops must notify their clients within the 90-day period before they can sell the pawned items in an auction. For the convenience of pawners, the new rules will require them to indicate in the pawn ticket their preferred mode of receiving the notice, whether by mail or courier to a given address, or by SMS or text through a specified mobile phone.

On the part of pawnshops, they will be required to comply with explicit "Know Your Pawner" procedures consistent with the requirements of the Anti-Money Laundering Act and to address concerns on the Anti-Fencing Law.

<sup>&</sup>lt;sup>244</sup> The practice of lending money and accepting and/or keeping gold and other personal properties of value as collaterals.

<sup>&</sup>lt;sup>245</sup> Amendments to the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) - Pawnshop (P) Regulations

<sup>&</sup>lt;sup>246</sup> Passed on January 29, 1973.

## **Money Laundering and TF Risks**

From the 5,934 registered pawnshops, only nine (9) entities reported covered and suspicious transactions for the period of January 2015 to December 2016. The ML and TF risks for the pawning service remain to be **LOW** because loans are secured by personal properties delivered to the pawnshops. These pawning loans are usually short-term, involving small amounts which are generally carried out by those from the low-income bracket. The value of the personal property that may be offered as collateral has no limit. In addition, no limit has been placed as to the number of transactions a customer may have for a particular period. This is considered reasonable since pawnshops cater primarily to low-income groups.

Non-face-to-face transactions are now allowed.<sup>247</sup> Basic KYC is required, but the process/documentation is simplified to fit the targeted low-income and small borrowers. Juridical persons are allowed to pawn, but since pawnshops cater primarily to low-income groups, borrowers are mostly natural persons. Cross-border transactions are not allowed.

One identified risk in pawning is the issue of ownership of the personal property offered as collateral. These include instances where personal properties obtained though robbery or theft were pawned. Under the Circular No. 938, pawnshops are required to comply with explicit "Know Your Pawner" procedures consistent with the requirements of the Anti-Money Laundering Act and to address concerns on the Anti-Fencing Law. The practice of conducting the necessary due diligence to determine ownership of the item to be pawned and blacklisting those who pawn items which are found to be sourced from illegal activities is considered an effective risk mitigant.

Recently, the BSP signed a Memorandum of Agreement with the Department of Interior and Local Government on the sharing of information between BSP and the city and municipal government units to ensure that only those that have the proper business permits and registered with the BSP are transacting with the public.

On the other hand, the ML/TF risks for remittance services by pawnshops are generally **LOW TO MEDIUM** because no cap has been placed on the amount of remittance and on the number of transactions. Big pawnshops have partnered with international remittance companies making it possible to remit money into and outside of the Philippines. While there is no limit on the amount and number of transactions, in general, the amount of these remittances are relatively low. Domestic remittances amount to around PhP2,000 and international remittances amount to around PhP5,000 to PhP100,000, which is typically the profile of remittances sent by Overseas Filipino Workers to their families. Some remittances also have regularity (i.e., twice a month) with recipients already known to the pawnshop.

STRs were submitted on individuals who made huge dollar payouts to Nigeria, a high-risk jurisdiction. There were also reports on internet purchase scams where fraudsters pretended to sell items online and use pawnshops to receive the payments. They presented fictitious IDs and use different names to avoid detection. The pawnshops were able to detect and report these suspicious transactions, indicating their ability to determine risks associated with transactions.

Enhanced CDD needs to be conducted on remittances involving large amounts especially on cross-border transactions. The blacklisting mechanism should be strictly enforced. BSP's recent amendments of pawnshop regulations, as well as remittance agent regulations, have potential to address these issues.

<sup>&</sup>lt;sup>247</sup> In e-pawning, proof of identification is submitted during online transaction and the identity of pawnshop client is verified when the item to be pawned is picked-up or delivered to the accredited outlet.

Existing pawnshop operators are given one year from the date of the effectivity of the Circular No. 938 to secure their BSP license to operate a pawnshop business.

It would be recalled the BSP revoked the licenses of Philrem Services Corp., Peso Remittance Express Inc. and Werquick Inc. for violations of section 451N of the Manual of Regulations for non-bank financial institutions and Circular 706 dated Jan. 5, 2011.

The three companies were implicated in the \$81 million bank heist wherein funds of the Bangladesh Bank were stolen and laundered in the country using Rizal Commercial Banking Corp. (RCBC) as a conduit. The bank was fined P1 billion.

As of end 2016, there were 16,698 BSP-authorized pawnshops consisting of 5,401 head offices and 11,297 branches nationwide. Of the total number, 6,847 are multi-functioning as foreign exchange dealer, money changer and remittance agent.

#### E. E-MONEY

The continued growth of digital technology is creating more opportunities and challenges to mobile operators in order to provide customers with better access to virtual financial services. The mobile industry is now widely established, bringing financial inclusion to a growing number of previously unbanked and underbanked populations.<sup>248</sup>

In 2016, there were 366 million e-money transactions generating PhP477.7 billion inflows and PhP478.4 billion outflows, with 85% coming EMI-Banks and 15% coming from EMI-Nonbanks.

BSP regulations define e-money as electronically stored monetary value; fully convertible to cash, and acceptable as payment for goods and services by participating merchants. As a digital channel for retail payments, an e-money account is distinct from a deposit account to safeguard public deposits. It is non-interest bearing and not covered by deposit insurance. This distinction allows even non-banks like telecommunication subsidiaries to be licensed as e-money issuers (EMIs), subject to proportionate requirements in capital (e.g., PhP100 Million minimum paid-up capital) and licensing (e.g., licensed as remittance agent).

The distinction also makes outsourcing and agent accreditation possible for all EMIs, whether bank or non-bank, provided EMIs remain accountable to BSP for their counterparties' adherence to applicable regulations (e.g., KYC in every cash-in/cash-out transaction of agents; reporting of covered/suspicious transactions for AML) and appropriate risk management.

To ensure liquidity, the amount of electronic values issued by EMIs must be equivalent to the actual cash maintained in a depository or settlement bank (e.g., for non-bank EMIs: cash in bank and liquid investments like government securities/for bank EMIs: e-money issued is booked as accounts payable). EMIs are likewise required to establish acceptable redress mechanisms for the resolution of e-money customer complaints.<sup>249</sup>

It may be noted that EMIs may offer products with transaction limits above the PhP100,000 threshold, subject to approval by the BSP to ensure that appropriate risk management mechanisms are observed. An example of this product is payroll e-money account of employees receiving monthly salaries above PhP100,000. The e-money accounts or "e-wallets" of cash-in/cash-out agents naturally have higher

<sup>248</sup> https://www.gsma.com/mobileeconomy/global/

<sup>&</sup>lt;sup>249</sup>Part VII. Electronic Banking Services and Operations, MORB.

transaction limits because they cater to a multitude of end-clients. These agents are subject to due diligence during the accreditation process conducted by EMIs. EMIs are required to submit the list of their counterparties, including accredited agents, to the BSP. The BSP may spot-check accredited agents during onsite examination.

At present, two of the most popular forms of e-money in the country are G-Cash of Globe Telecom and PayMaya Philippines Inc. of PLDT Smart Money.

PayMaya Philippines, Inc. (formerly Smart eMoney, Inc.) is the pioneer in mobile money and payments, having established brands such as PayMaya, the first prepaid online payment app that enables the financially underserved to pay online without a credit card; PayMaya Business, the company's system solutions provider that allows businesses to receive online and card payments anytime, anywhere; Smart Money, the world's first e-wallet linked to a mobile phone; and Smart Padala, the leading remittance network in the Philippines with over 15,000 agents across the country. PayMaya Philippines is a subsidiary of Voyager Innovations, the digital innovations company of PLDT and Smart.<sup>250</sup>

On the other hand, Globe Telecom started GCash in 2004, and established a subsidiary, called G-Xchange Inc. (GXI), which registered with the BSP as a remittance agent and is also now licensed as an e-Money issuer. For cash-in cash-out, it relies mostly on nonbanks and remittance agents such as pawnshops and money changers.

## **Money Laundering Risks for E-Money**

The ML risk for e-money is generally <u>LOW</u> because of a low value threshold and existence of risk mitigants. The BSP placed an aggregate monthly load limit on e-money instruments amounting to PhP100,000. EMIs are required to ensure compliance with AML requirements. They even provide training for individual retailers in compliance with the BSP rules and regulations. For products that do a non-face to face account transaction, the BSP-supervised financial institution (BSFI) is in possession of verifying the identification documents submitted by the prospective client prior to the interview and that the entire procedure is documented. Also, whenever customer cashes in and out in the e-money system, CDD procedures are performed. There is a PIN verification or a confirmation number per transaction. Customers also receive SMS notification for every transaction so they can track anything going on with their e-wallet. There is also a system in place to perform adequate customer profiling.

The number of STRs filed by the sector is relatively low as against the total e-money transactions. Nonetheless, potential exposure to financial crimes and abuse of the product for scam purposes remains a concern that regulators continue to address with commensurate consumer protection rules, advisories and financial education.

# **Terrorist Financing Risks for E-Money**

The TF risk for e-money is likewise **LOW** although the cross-border transaction could expose the sector to TF risks. It might be possible for terrorist groups to channel the funds for their activities using e-money transfer, although the proportion of ML/TF cases using E-money and the total E-money transaction is very negligible. Given a lower aggregate threshold amount per month and the current average transaction amount per area is very low, the risk of TF is reduced. EMIs are also required to have the capacity to monitor the transactions and make the necessary reports in compliance with the requirements of Recommendation 16 on wire transfers. Moreover, issuers have information on high

<sup>&</sup>lt;sup>250</sup> https://paymaya.com/about/

risk jurisdictions (as provided by MasterCard containing identified jurisdictions under OFAC) and have blocked transactions to these high risk jurisdictions.

# **ACTION PLAN**

Based on the identified risks on these financial products, the following are the recommended action points:

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Monitor the implementation of BSP Circular Nos. 938 and 942 to identify, measure and manage ML/TF risks for remittance services by pawnshops and MSBs	BSP		
Strengthen data collection to determine the level of remittances coursed through pawnshops and MSBs that are being used for ML/TF			

#### IX. TERRORISM AND TERRORIST FINANCING THREAT ASSESSMENT

## **EXECUTIVE SUMMARY**

Based on the overall assessment of factors, **terrorism financing vulnerability** of the Philippines is **HIGH**.

**Terrorism threat** in the Philippines is rated <u>HIGH</u> given the high number of violent incidents associated with terror/threat organizations. Prosecution of cases involving said groups are at a minimal level as compared to the number of incidents and victims recorded.

Similarly, **terrorism financing threat** is rated <u>HIGH</u> as terrorist/threat organizations in the country appear to have a systematic and established method of raising funds for their operations. Terrorist/threat organizations predominantly use illegal means to raise funds, with kidnap for ransom and extortion as the preferred means by terrorist/threat groups. While the total amount raised by these organizations remain largely unknown, the high number of threat incidents recorded indicate that these terrorist/threat organizations are well-funded.

Threat groups also resort to legitimate means to raise funds. Among the fundraising methods used are the use of non-profit organizations, family funding and legitimate business fronts.

Use of funds are generally for operational purposes such as purchase of arms and vehicles. Threat groups used part of the funds raised to support the communities wherein they operate. The groups provide for the basic needs, livelihood support and even educational opportunities to these communities. In turn, the communities shield them from government forces even if they know the nature and source of funds.

Cash transactions remain to be the preferred mode for transfer of value for Philippine terrorist/threat organizations. The physical movement of cash leaves no paper trail and is not hindered by AML/CFT safeguards present in the formal financial system. Remittance agencies have also been reported to be the channel by which funds are transferred, especially from abroad.

Despite the high number of threat incidents and the estimated amounts raised by the terrorist/threat groups, STR submissions by covered persons remain low. For the given period, total amount frozen compared to the estimated amounts raised is at minimal levels. Focus of intelligence gathering remains concentrated on terrorism and not terrorism financing. This results in limited appreciation of evidence useful for terrorism financing during the investigation on terrorism.

Domestic (and international) coordination is one factor that should be further strengthened in combating the financing of terrorism. Recent experiences have shown that close domestic coordination among the AMLC and relevant government agencies yields positive results.

## **DATA AND INFORMATION COLLECTION**

In the first NRA Report, the terrorism and terrorism financing threat assessment was integrated in the Threat Assessment Module by the World Bank Tool. In the 2015 World Bank Tool, terrorist financing risk assessment is undertaken separately. It consists of three areas of analysis, as follows:

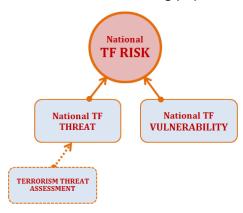


Figure 9-1. Structure of the Terrorism Financing (TF) Risk Assessment Module

The main objectives of the terrorist financing risk assessment are: (a) to identify the level of TF threat based on the terrorism threat; (b) to identify the direction of the financial flows, as well as its sources and channels; and, (c) to assess vulnerability.

The level of terrorist threat is assessed through the review of quantitative and qualitative information on terrorist acts in the jurisdiction, such as enforcement data, intelligence sources, and terrorism research. Studies, such as 2016 Regional Risk Assessment on Terrorism Financing, <sup>251</sup> which was spearheaded by the Australian Transaction and Analysis Centre (AUSTRAC) and the Pusat Pelaporan dan Analisi Transaksi Kuangan Indonesian (PPATK) were also considered in this assessment.

#### **LEGAL FRAMEWORK**

Acts of terrorism was criminalized in the Philippines with the passage of Republic Act 9372 or the Human Security Act (HSA) of 2007. It defined "terrorism" as acts punishable under specified provisions of the Revised Penal Code<sup>252</sup> and other special penal laws, committed for the purpose of sowing and creating a condition of widespread and extraordinary fear and panic among the populace, in order to coerce the government to give in to an unlawful demand. The law allows the police and other law enforcement authorities, duly authorized by the Anti-Terrorism Council, to conduct electronic surveillance as well as the examination of bank deposits of suspected terrorists upon judicial authorization issued by the Court of Appeals.<sup>253</sup>

Page 283 of 300

<sup>&</sup>lt;sup>251</sup> In 2015, the AUSTRAC and PPATK co-hosted the first South East Asia Counter-Terrorism Financing (CTF) Summit. A key outcome of the 2015 summit was the conduct of a regional risk assessment (RRA) of terrorism financing in South East Asia. The RRA team was comprised of the financial intelligence units (FIUs) of Australia, Indonesia, Malaysia, Philippines, Singapore and Thailand. The first RRA report was published in August 2016. <a href="http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL">http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL</a> 0.pdf

<sup>&</sup>lt;sup>252</sup> Article 122 (Piracy in the High Seas or in the Philippine Waters); Article 134 (Rebellion or Insurrection); Article 134-a (Coup d' Etat); Article 248 (Murder); Article 267 (Kidnapping and Serious Illegal Detention); Article 324 (Crimes Involving Destruction), or under Presidential Decree No. 1613 (Arson); Republic Act No. 6969 (Toxic Substances and Hazardous and Nuclear Waste Control Act of 1990); Republic Act No. 5207, (Atomic Energy Regulatory and Liability Act of 1968); Republic Act No. 6235 (Anti-Hijacking Law); Presidential Decree No. 532 (Anti-Piracy and Anti-Highway Robbery Law of 1974); and, Presidential Decree No. 1866, as amended (Decree Codifying the Laws on Illegal and Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunitions or Explosives).

<sup>&</sup>lt;sup>253</sup> Sections 27 – 31, RA 9372.

During the Second Round of the Mutual Evaluation<sup>254</sup> of the Philippines, the Assessors found that among the main shortcomings in the legal AML/CFT framework of the Philippines is the failure to make terrorism financing a stand-alone offense. This has an impact on multiple TF-related issues, including the lack of authority of law enforcement agencies to conduct TF investigations. Furthermore, while authorities have been able to freeze and confiscate terrorist funds on the basis of the crime of terrorism under the HSA, this was done on a legally tentative basis.<sup>255</sup> Thus, the enactment of legislation criminalizing terrorism financing and including it as a predicate offense to money laundering was of utmost priority of the Philippines.<sup>256</sup>

In 2012, Republic Act No. 10168 or "The Terrorist Financing Prevention and Suppression Act of 2012" was passed. The law penalizes the following:

- i. Financing of (a) terrorist acts, (b) terrorist organization, or (c) an individual terrorist;
- ii. Organizing or directing others to commit terrorist financing;
- iii. Attempt or Conspiracy to commit terrorist financing;
- iv. Participating as either an accomplice or an accessory to the crime of terrorist financing; and
- v. Dealing with properties or funds of a designated person.

The law further designates Terrorist financing as a predicate offense to money laundering<sup>257</sup> and gives the AMLC the power to inquire and freeze funds and properties related to acts of terrorism or terrorist financing without need of a court order. The freeze order issued by the AMLC shall have an initial validity of twenty (20) days, within which time, the AMLC may apply with the Court of Appeals to extend its effectivity for a period of not exceeding six (6) months. If however, the freeze order pertains to funds and properties of United Nations Security Council (UNSC) designated persons or organizations, then the freeze order shall be issued by the AMLC which shall be effective until the basis for its issuance have been lifted.<sup>258</sup>

With the enactment of the Terrorist Financing Prevention and Suppression Act, the Asia Pacific Group (APG) on Money Laundering found the Philippines to be compliant with the FATF technical requirements on terrorist financing. The 2012 APG Detailed Analysis Report states:

"12. x x x. The new TF offence criminalizes the provision or collection of funds for terrorist acts and further extends it to the financing of an individual terrorist or a terrorist organization with a wide definition of funds as encompassing assets of any kind, and providing for adequate sanctions and ancillary offences. It thus remedies the previously identified deficiencies. In the absence of previous criminalization, the question of effectiveness of the offence does not arise."

"13. In summary, compliance with SRII<sup>259</sup> has now been brought to a level equivalent to LC."

<sup>&</sup>lt;sup>254</sup> The Asia Pacific Group (APG) on Money Laundering, an autonomous international organization formed in 1997, implements and enforces Anti-Money Laundering and Combatting the Financing of Terrorism standards, particularly FATF's Forty Recommendations. Pursuant to APG rules, members mutually evaluate their peers to assess compliance with said international AML/CTF standards. The Philippines underwent MEs in 2003 and 2008.

<sup>&</sup>lt;sup>255</sup> 2009 Philippine MER, pages 9-10

<sup>&</sup>lt;sup>256</sup> 2009 Philippine MER, page 25.

<sup>&</sup>lt;sup>257</sup> Section 17, RA 10168

<sup>&</sup>lt;sup>258</sup> Section 11, RA 10168

<sup>&</sup>lt;sup>259</sup> Now FATF Recommendation 5 - Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of

#### **TERRORISM THREAT**

Currently, terrorist organizations are those that are designated under the United Nations Security Council Resolution (UNSCR) Nos. 1267/1373 and those that are proscribed under Section 17<sup>260</sup> HSA. Only the Abu Sayyaf Group (ASG) has been proscribed under the HSA. It is likewise a designated organization under UNSCR No. 1267.

With respect to terrorist financing however, the R.A. No. 10186 defines *Terrorist organization, association or a group of persons* as any entity owned or controlled by any terrorist or group of terrorists that: (1) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (2) participates as an accomplice in terrorist acts; (3) organizes or directs others to commit terrorist acts; or (4) contributes to the commission of terrorist acts by a group of persons acting with common purpose of furthering the terrorist act where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.<sup>261</sup>

Similarly, a *Terrorist* refers to any natural person who: (1) commits, or attempts, or conspires to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully; (2) participates, as a principal or as an accomplice, in terrorist acts; (3) organizes or directs others to commit terrorist acts; or (4) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.<sup>262</sup>

Terrorist acts,<sup>263</sup> in turn, are defined as:

- (1) Any act in violation of Section 3 or Section 4 of the Human Security Act of 2007;
- (2) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act;
- (3) Any act which constitutes an offense under this Act, that is within the scope of any of the following treaties of which the Republic of the Philippines is a State party:
  - (a) Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

<sup>&</sup>lt;sup>260</sup> **SEC. 17.** *Proscription of Terrorist Organizations, Association, or Group of Persons.* - Any organization, association, or group of persons organized for the purpose of engaging in terrorism, or which, although not organized for that purpose, actually uses the acts to terrorize mentioned in this Act or to sow and create a condition of widespread and extraordinary fear and panic among the populace in order to coerce the government to give in to an unlawful demand shall, upon application of the Department of Justice before a competent Regional Trial Court, with due notice and opportunity to be heard given to the organization, association, or group of persons concerned, be declared as a terrorist and outlawed organization, association, or group of persons by the said Regional Trial Court.

<sup>&</sup>lt;sup>261</sup> Section 3(j)(3)(k), RA 10168

<sup>&</sup>lt;sup>262</sup> Section 3(i), RA 10168

<sup>&</sup>lt;sup>263</sup> Section 3(j), RA 10168

- (b) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;
- (c) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;
- (d) International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;
- (e) Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980;
- (f) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;
- (g) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988;
- (h) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988; or
- (i) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

Given the foregoing definitions under the law, a group/organization/association not otherwise designated or proscribed may be consider a terrorist organization, for purposes of terrorist financing, if said group/organization/association is controlled by terrorists or is performing terrorist acts. These groups/organizations/associations that are not designated/proscribed but are performing acts of terrorism are labeled as "threat groups" by Law Enforcement Agencies.

In the Philippines, only the Abu Sayyaf Group is designated and proscribed as a terrorist organization. Other jurisdictions have also identified the Communist Party of the Philippines – New People's Army as a terrorist organization, albeit the same organization has not been proscribed in the country. LEAs have also identified threats groups, categorized as Daesh inspired groups, secessionist movements and insurgency movements.

For the given period, the PNP recorded 1039 incidents related to the ASG and identified local threat groups.

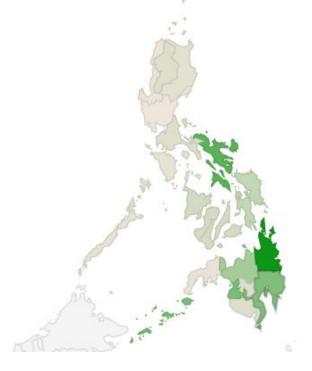


Figure 9-2. Heat Map of Threat Incidents in the Philippines

Based on the foregoing data, Regions XIII (CARAGA), Region V (Bicol Region), ARMM and Region XI (Davao Region) recorded the most number of incidents related to terrorist/threat groups.

# Abu Sayyaf Group (ASG) – Designated and Proscribed as a Terrorist Organization

The Abu Sayyaf Group (ASG) is an offshoot organization of Al Qaeda (AQ) and most of it members are composed of the remnants of Jemaah Islamiyah, rogue factions of the Moro National Liberation Front (MNLF) and lawless factions of the Moro Islamic Liberation Front (MILF). They have been designated as a terrorist group by the United Nations (UN), Australia, Canada, Indonesia, Malaysia, United Arab Emirates, United Kingdom, United States and the Philippines.

The ASG is a designated entity listed under entry no. QDe.001 of the United Nations Security Council Resolution (UNSCR) 1267/1989 (otherwise known as "The Al-Qaida Sanctions List") covering individuals and entities associated with Al-Qaida.

The ASG was listed in the Al-Qaida Sanctions List on 06 October 2001 for participating in the financing, planning, facilitating, preparing or perpetrating acts or activities in the name or in support of or otherwise supporting the acts or activities of Al-Qaida. ASG members have been trained by Al-Qaida (QDe.004) and Jemaah Islamiyah (JI) in guerilla warfare, military operations and bomb making.

ASG has been involved in a number of terrorist attacks, including assassinations; bombing civilian and military establishments and domestic infrastructure, including airports and ferries; kidnapping local officials and foreign tourists; beheading local and foreign hostages; and extortion against local and foreign businesses.

On 10 September 2015, a court in the province of Basilan declared the Abu Sayyaf Group as a terrorist organization under Section 17 of the HSA.

Isnilon Hapilon, the second most ranking ASG leader following their Emir, Radullan Sahiron, is considered as one of the most influential Islamic extremist leader. He has been reportedly elected as

"wali" (governor) of the Dawlatul Islamiyah Waliyatul Masrik (DIWM). The DIWM is a congregation of alleged local terrorist groups that are vying for the recognition of Daesh.

While its leaders have in recent years pledged allegiance to the Islamic State (ISIS) group, analysts say the group is mainly focused on a lucrative kidnapping business rather than religious ideology.<sup>264</sup>

## **Maute Group**

The Maute Group is a Daesh inspired group based in Butig, Lanao del Sur. The group consists of known clans in the Lanao del Sur area and is led by Abdullah Romato Maute a.k.a. Abu Hassan Al Filibini, assisted by his six (6) brothers as well as other relatives and personalities who act as sub-commanders. The group is supervised and financed by their parents – Engineer Cayamora Maute and their mother, Farhana Maute.

The group has been responsible for the killing of military personnel and civilians in Marawi City and in the Lanao del Sur area in general. The group gained notoriety when they launched an attack against a military detachment in Butig, Lanao del Sur in February 2016 and briefly occupied the said town. They became even more notorious as a local threat group when they kidnapped six (6) Christian sawmill workers in April 2016 and subsequently beheaded two (2) of them when the government failed to comply with their demand to release one of their captured members.

On 29 July 2016, intelligence operatives from the military, after the conduct of pursuit operations, captured a vehicle registered under the name of Farhana Ominta Maute. When the Maute members were cornered by the pursuing agents, they abandoned the vehicle. Firearms, ammunitions, ISIS inspired documents, military uniforms, bomb-making components/ equipment and an IED were recovered from the said vehicle.

On 23 May 2017, a soldier and eight others were killed due to a firefight between police and military against the Maute Group in Brgy. Basak Malulut in Marawi City.

The group of armed men are led by Basilan based ASG leader Isnilon Hapilon. It was reported that Hapilon left Basilan to establish a "wilayat" or province of the Islamic State in Lanao del Sur. Marawi City is near the town of Butig, the stronghold of the Maute.

The acts of the Maute Group in conniving and confederating with Isnilon Hapilon and the ASG in sowing fear, terror and causing numerous civilian casualties and damages to properties in Marawi City shows that the Maute Group have banded with the ASG.

On 28 May 2017, military authorities discovered numerous bodies of civilians that were killed and dumped by the Maute Group. The civilians appear to have been executed and were thrown in a ravine outside Marawi City. Most of them were shot in the head and their hands were tied behind their backs.

<sup>&</sup>lt;sup>264</sup>http://www.rappler.com/world/regions/asia-pacific/indonesia/bahasa/englishedition/146840-abu-sayyaf-ransom-indonesian-hostages. Last retrieved 12 August 2017.

# Other Threat Group designated by Foreign States as Foreign Terrorist Organization: Communist Party of the Philippines – New People's Army – National Democratic Front (CNN)

The CPP-NPA was designated by the U.S. State Department as a Foreign Terrorist Organization in 9 August 2002<sup>265</sup> and by the European Union as a Designated Terrorist Organization in 28 October 2002.<sup>266</sup>

In 1968, the Communist Party of the Philippines (CPP) was established for the purpose of establishing a new state to be led by the working class and free from any United States influence.<sup>267</sup> <sup>268</sup>The organization is influenced by China's Maoist oriented movement.<sup>269</sup>

In 1969, the New People's Army (NPA) was established. The NPA acts as the armed wing of the CPP. The two organization are so closely intertwined together that they are known as the CPP-NPA.<sup>270</sup> In 1973, in an attempt to unify and coordinate various leftist organization, the CPP-NPA founded the National Democratic Front (NDF). The NDF served as the umbrella organization for the CPP-NPA and other mass revolutionary organizations, and has been described as the CPP-NPA's political wing.<sup>271</sup>

The CPP-NPA is one of the most active armed organization in the country and has waged the world's longest Communist insurgency. A total of 802 incidents by CPP-NPA were recorded by the PNP from 2014 up to 2016. Notably, 596 or 74% were undertaken in the Bicol, Northern Mindanao, Davao, and CARAGA regions.

#### TERRORIST FINANCING THREAT

The high number of violent incidents carried out by a terrorist organization and local threat groups indicate that the presence of funds and material support for these groups. Likewise, an increase in the number of incidents also indicate that some of these organizations escalate their activities in order to pressure communities and victims to pay in exchange for peace.

# A. Sources of Fund/Material Support

# 1. Raising Funds through Criminal Activities

Terrorist group/threat groups in the Philippines primarily uses illegal means to raise funds.

<sup>&</sup>lt;sup>265</sup> "Foreign Terrorist Organizations". www.state.gov. Retrieved 19 September 2012.

<sup>&</sup>lt;sup>266</sup> "Council Implementing Regulation (EU) No 1285/2009". EUR-Lex. 2009-12-22. Retrieved March 18, 2010.

<sup>&</sup>lt;sup>267</sup> The Communist Insurgency in the Philippines: Tactics and Talks." International Crisis Group, 14 Feb. 2011. Web. 11 Aug. 2015.

<sup>&</sup>lt;sup>268</sup> Santos, Jr., Soliman M., and Paz Verdades M. Santos. Primed and Purposeful: Armed Groups and Human Security Efforts in the Philippines. Geneva: Small Arms Survey, April 2010. Print.

<sup>&</sup>lt;sup>269</sup> Rosca, Ninotchka, and Jose Maria Sison. Jose Maria Sison: At Home In the World—Portrait of a Revolutionary. Greensboro: Open Hand Publishing, LLC, 2004. Print.

<sup>&</sup>lt;sup>270</sup> Program For A People's Democratic Revolution." Communist Party of the Philippines, 26 Dec. 1968. Web. 11 Aug. 2015

<sup>&</sup>lt;sup>271</sup> National Democratic Front of the Philippines: Revolutionary united front organization of the Filipino people." National Democratic Front of the Philippines, International Information Office. Web. 11 Aug. 2015.

<sup>&</sup>lt;sup>272</sup> Mydans, Seth. "Communist Revolt Is Alive, and Active, in the Philippines." The New York Times, 26 Mar. 2003. Web. 11 Aug. 2015.

## **KIDNAPPING FOR RANSOM**

Kidnapping for ransom of both locals and foreign nationals is the primary source of funds for the Abu Sayyaf Group (ASG). From 2014 – 2016, it was reported that the ASG committed 37 kidnappings.

Governments have a "no ransom policy" and thus, have refused to negotiate with ASG for the release of their nationals. This however has not prevented individuals from negotiating secretly with the group.

Based on recorded data, approximately PhP68.75 Million has been paid as ransom for the years 2014 - 2016. According to news reports, however, the total ransom paid by mid-2016 alone is estimated at PhP354 Million (approximately US\$7.4 Million).<sup>273</sup>

In September 2015, three foreigners and a Filipina were abducted in a resort in Samal Island, Davao.<sup>274</sup> The victims were held for about a year. The Filipina was later released. One of the foreign captives was released in August 2016 after allegedly paying PhP50 Million (approximately US\$1 million) ransom money.<sup>275</sup> Reports reveal that another separatist movement who helped broker the release of the foreign captive also had a share in the ransom. The other 2 foreign captives were executed.

Newspaper account also claims that in 2016, the ASG was responsible for the abduction of at least 24 crew members from a neighbor country. It is also estimated that a total of PhP120 Million (approximately US\$2.5 Million) has been paid for the release of 17 crew members. This includes the PhP50 Million (approximately US\$1 million) ransom money paid for the release of ten (10) crew members abducted off the waters of Southern Philippines.

It appears that kidnapping for ransom remains to be a very lucrative business for the ASG, particularly the kidnapping of foreigners and foreign ships crew members.

## **EXTORTION/REVOLUTIONARY TAXES**

Several threat groups have also been known to resort to extortion or collection of "revolutionary taxes" to raise funds. The collection of the so called "revolutionary taxes" is in fact the main fundraising mechanism for a threat group with nationwide presence.

Demand for revolutionary taxes is normally relayed to "prospective targets" through letters. The taxes are collected from the residents and local businesses of the communities wherein the group operates. Bigger amounts however are collected from bus companies which pass through their controlled areas, mining firms, construction firms and telecommunications companies. Companies who refuse to pay taxes are punished by the group through burning of commuter buses, toppling of mobile phone relay towers, and similar destructive activities on mining, logging, and agricultural estates.

<sup>&</sup>lt;sup>273</sup> https://www.rappler.com/world/regions/asia-pacific/indonesia/bahasa/englishedition/146840-abu-sayyaf-ransom-indonesian-hostages

https://www.rappler.com/nation/106687-abduction-samal-island-davao-del-norte. Last retrieved 12 August 2017.

<sup>&</sup>lt;sup>275</sup>http://www.rappler.com/world/regions/asia-pacific/indonesia/bahasa/englishedition/146840-abu-sayyaf-ransom-indonesian-hostages. Last retrieved 12 August 2017.

<sup>&</sup>lt;sup>276</sup>http://www.rappler.com/world/regions/asia-pacific/indonesia/bahasa/englishedition/146840-abu-sayyaf-ransom-indonesian-hostages. Last retrieved 12 August 2017.

The total amount of funds raised in this manner remains unknown as "taxpayers" refuse to talk. However, the Secretary of National Defense, Delfin Lorenzana, estimates that in Eastern Mindanao alone, collection reached PhP1.2-billion per year.<sup>277</sup>

ASG and threat groups in Southern Philippines have long been suspected of engaging in drug trafficking but links with drug trafficking organizations have not been established. The threat group with nationwide presence has also been suspected of engaging in the sale of marijuana, particularly their units operating in mountainous region of Luzon and Region XI.

What is known is that members of these groups use drugs, particularly "shabu" to keep them awake during their operations. In June 2017 however, more than PhP375,000 worth of shabu and two (2) packs of cocaine were seized in a building in Marawi previously occupied by members of a threat group. Prior to that, soldiers reportedly found more than PhP100 Million worth of shabu in different houses members of the group used as hideouts as they laid siege to several barangays in Marawi City. <sup>278</sup>

## **OTHER CRIMINAL ACTIVITIES**

Threat groups also resort to robbery and carnapping, particularly of police/military establishments to get weapons, ammunitions and vehicles. The threat group with nationwide presence is able to acquire its weapons and armaments from the military through raids, battles and illegal purchases.

In Southern Philippines, other criminal activities committed by terrorist/threat groups are human trafficking, smuggling of rice, sugar, oil, weapons and other goods. Law enforcement agencies are still gathering information whether these activities are related to TF.

Based on a news article dated 4 July 2017, Maute and Abu Sayyaf militants stole an estimated half a billion pesos from three banks when they stormed Marawi City. <sup>279</sup> <sup>280</sup>

# FUNDING FROM FOREIGN TERRORIST ORGANIZATIONS

In recent years, Philippine authorities have also received reports that local threat groups are also receiving funding from external threat groups.

In the 1990s, it was reported that a threat group in Southern Philippines was receiving funding from Al Qaeda and from Mohammad Jamal Khalifa, Osama bin Laden's brother-in-law, who founded various charities that funneled money similar groups.<sup>281</sup>

Reports also claim that it is possible that JI is funding a threat group's bombing activities in Southern Philippines.<sup>282</sup> Some threat groups also provide safe haven to members of foreign terrorist groups in exchange for financial aids, arms, ammunitions and trainings.

<sup>&</sup>lt;sup>277</sup>http://www.philnews.xyz/2017/07/dnd-secretary-reveals-npa-raking-in-p1-2-billion-yearly-extortion-activities.html. Retrieved 31 July 2017.

<sup>&</sup>lt;sup>278</sup>http://www.philstar.com/nation/2017/07/04/1716355/over-p350k-worth-drugs-seized-building-occupied-maute. Posted on 4 July 2017. Last accessed on 30 July 2017.

http://gulfnews.com/news/asia/philippines/maute-abu-sayyaf-loot-500-million-pesos-from-three-marawicity-banks-1.2053058

<sup>&</sup>lt;sup>280</sup> https://www.pressreader.com/uae/gulf-news/20170705/281801398987994. Posted on July 5, 2017. Last accessed on 03 August 2017

<sup>&</sup>lt;sup>281</sup> https://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/309

<sup>&</sup>lt;sup>282</sup> Manila Times, AFP tags BIFF as Jemaah Islamiyah ally, June 12, 2014, accessed July 28, 2017

According to a report published by Rappler in 22 July 2017, a Malaysian professor arranged for funds to be sent from Syria through Indonesia and then on to the Philippines through a money service business. The main beneficiary is the Maute Group. It is estimated that ISIS channeled U\$600,000 through the Malaysian professor.<sup>283</sup>

## 2. Funds/Material Support through Legitimate Sources

While criminal activities remain to be the primary source of funds for terrorist/threat groups, legitimate fundraising methods are still used.

## **NON-PROFIT ORGANIZATIONS**

Non-Profit Organizations (NPOs) are unregulated for AML/CFT purposes. Anecdotal and intelligence information show that NPOs have been used to raise and funnel funds to terrorist/threat organizations. There is however no data as to the number of NPOs used for terrorist financing purposes or the extent of funds funneled through them for TF.

Some Madaris<sup>284</sup> in the Philippines which are run by Foundations have been used not only to raise funds but also to radicalize possible recruits into the group. It is unclear whether said Madrasis are registered with the Securities and Exchange Commission (SEC) or the Commission on Higher Education (CHED).

Aid given to an organization for the construction of socialized housing was also diverted to threat groups in Southern Philippines. The houses were constructed using sub-standard materials. Based on intelligence report, the "savings" were diverted to the threat group. The contractor for the said socialized housing is also suspected to be owned by a family member of one of the leaders of the threat group.

Law enforcement authorities have also monitored individuals soliciting funds on behalf of a charitable institution operating in Southern Philippines. Funds raised however are channeled to threat groups. It is unclear whether these individuals are really part of the charitable institution they alleged to represent. There are also reports that a foundation in Southern Philippines has been receiving funds from abroad to fund violent activities in the region.

These foundations and charitable institutions also serve a dual role for the terrorist/threat organizations. Aside from being used to raise funds, these NPOs are also used to create goodwill with communities wherein the terrorist/threat groups reside and operate. Intelligence reports indicate that threat groups establish charitable and educational institutions (which may or may not be registered with the SEC) to give out aid to the communities. The communities generally know that these organizations are fronts or are funded by the local threat groups. These communities however benefit greatly from the aid extended by these organizations, that they actually hide and shield members of the threat groups from government forces.

Some of the NPOs are said to be actively soliciting from foreign funders by submitting project proposals and feasibility studies. Once approved however, part of the funding would be funneled to

<sup>&</sup>lt;sup>283</sup> http://www.rappler.com/nation/176295-syria-isis-marawi-funding. Posted on 22 July 2017. Last accessed 30 July 2017

<sup>&</sup>lt;sup>284</sup> a college for Islamic instruction. These madrasas however are not registered with the Commission on Higher Education

threat organizations in the region. Funds received are then split between the NPO and the threat group.

## FAMILY FUNDING AND LEGITIMATE BUSINESS FRONTS

A Southern Philippine threat group who has recently gained national attention initially got its funding and logistical support from family members. The family is wealthy and with political ties.

The group, headed by brothers, was first funded by their parents and legitimate business fronts of their family members. One of the suspected business fronts of the family is a construction company which was used in the construction of socialized housing. It is suspected that these legitimate business fronts are also being used as fronts for drug trafficking. This however remains unconfirmed. Properties – land and vehicles – belonging to the family were also used to train fighters and carry out violent incidents in the region.

A company involved in the processing of papers for Middle East bound overseas workers is also suspected to be funding the same threat group. The owner of the company, a suspected member of ISIS, was arrested in the country and has been deported back to the Middle Eastern country.<sup>285</sup>

## B. Use of Funds

Funds generated by terrorist/threat groups are generally used to fund their operations. Weapons and ammunition are purchased, as well as materials used for bombs. It also goes into the training of members of the groups in military tactics and bomb-making. The ASG have been known to purchase fast moving sea vehicles to further perpetuate kidnapping in the high seas.

The ASG also distribute ransom collected to their members as a form of commission. Funds are also being used to support widows and the family of the members of the group. For another threat group, special funds are allocated to support the needs of families of senior members, like food and medical expenses. A certain percentage is also sent to exiled leaders abroad.<sup>286</sup>

Threat groups from Southern Philippines used part of the funds raised to support the communities wherein they operate. The groups provide for the basic needs, livelihood support and even educational opportunities to these communities. Since government aid do not reach these communities, they value the support extended to them by these groups. The groups in turn are able to recruit and get protection. The communities shield them from government forces even if they know the nature and source of funds.

A threat group also spends for social and economic projects such as communal farms and cooperatives, medical and health expenses, literacy and education programs, cultural activities and programs and mass movement, and agrarian reform. Aside from operational use, family and community support, this threat group allots resources for the recruitment and indoctrination of members.

http://news.abs-cbn.com/news/05/31/17/kuwaiti-owned-company-in-ph-may-be-funding-maute-lawmakers

What's the Source of Communist Rebels' Funds? | THE VINCENTON POST, 2010, https://fvdb.wordpress.com/2010/12/28/whats-the-source-of-communist-rebels-funds/. Retrieved 3 July 2017

#### C. Channels

The terrorist organization and threat groups in the Philippines use a variety of methods to move funds. In the case of the Philippines, physical movement of cash or cash couriers is the preferred mode to move money or transfer value. Informal remittance channels are also utilized. In the formal financial system, stand-alone remittances are preferred over the banking system.

The physical movement of cash leaves no paper trail and is not hindered by AML/CFT safeguards present in the formal financial system. It requires extensive intelligence work in order for it to be detected. In some cases, cash raised and moved throughout the threat group are at low amounts making detection more difficult.

"Revolutionary taxes" are paid in cash directly by the victims to the threat group. The amount raised are then directly distributed to the unit concerned for direct use in their operations and sustenance. Resulting transactions are most likely made purely in cash.

In cases of ransom paid for kidnapped victims, intelligence reports infer that ransom money may have been transferred through bulk cash smuggling as there are barely any TF-related suspicious transactions from the formal financial system. Cash may have been physically carried through the porous borders of Southern Philippines.

Another channel possibly exploited by threat groups in the Philippines is the alternative remittance channels (ARS) or the hawala system. The ARS provide for an efficient and cost-effective method for worldwide remittance. Parties are anonymous and transactions do not have paper trails, making transactions largely undetectable

In the formal financial system, the preferred channel for movement of funds/transfer of value according to intelligence reports is through stand-alone remittance agencies. Amounts remitted are usually small, falling way below the threshold set under the AMLA, as amended. The relatively small amounts of transactions also do not raise red flags with the remittance agencies, and thus, no suspicious transaction reports are submitted.

Remittance agencies have also been reported to be the channel by which funds are transferred to the family-led threat group in Southern Philippines. It was reported that fund transfers from Syria through another ASEAN country then on to the Philippines was facilitated through a known international money transfer agent.

In some instances, the banking sector has also been used as a channel for funds related to local terrorist/threat organizations. During the arrest of a known ASG leader in 2014, authorities were able to seize from him an ATM card for a deposit account from a local bank. Police authorities suspected that the said account may have been used as a conduit by the ASG in funding their activities. Police confirmed that apart from kidnapping for ransom and violent activities, the arrested ASG leader also solicited funds from ASG supporters in Saudi Arabia and served as the courier of funds to the former ASG leader. It is also believed that the arrested leader received PhP30,000.00 (approximately US\$643.00) from another ASG leader who is designated under QDi. 204 of UNSCR 1267/1989. The PhP30,000.00 was believed to be deposited in the bank deposit account represented by the ATM card.

Part of the ransom money for kidnapping committed by the ASG was also deposited in a bank. In a 2016 kidnapping committed by the ASG, ransom money was deposited to a local bank account. The deposit account involved an ATM joint savings account opened in 2001 in the names of alleged ASG members residing in Jolo, Sulu, Philippines. Investigation revealed that on 4 April 2016, the amount of

PhP1.01 Million (approximately US20,150.00) was credited to the subject deposit account through an inward remittance originating from the crew members' country.

#### TERRORIST FINANCING INVESTIGATION

The Philippine legal framework on terrorism financing has been assessed as "Largely Compliant" to the FATF standards with the passage of Republic Act No. 10168. The AMLC is authorized under the law to conduct investigations on terrorism financing, and to freeze, without delay, all funds or assets related to terrorism. It also provides for mechanisms to ensure that no assets are made available to, or for, the benefit of persons and entities designated by the UN Security Council under Chapter VII of the Chapter of UN specifically UNSCR 1267/1989 (Al Qaeda), 1988 (Taliban) and their successor resolutions, as well as UNSCR 1373 (2001).

For the period of 2014 – 2016, data shows that 986 incidents related to terrorist/threat groups are under investigation by law enforcement agencies, 104 cases have been referred to prosecutor's office, while 7 cases are filed in court. In comparison, the AMLC was able to investigate 18 cases of terrorism financing for the same period.

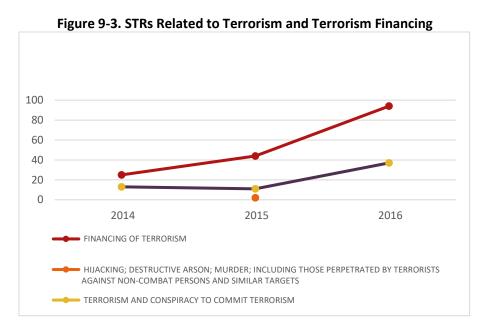
During the years 2015, 2016 and 2017, the AMLC was able to freeze cash in the aggregate amount of P52.68 Million, a real estate with an estimated value of PhP 7.2 Million and eighteen (18) motor vehicles.

The frozen amounts include the PhP52 million seized by the military in June 2017 in an abandoned house used by a threat group holding Marawi City. The recovered currency is also subject to civil forfeiture proceedings.

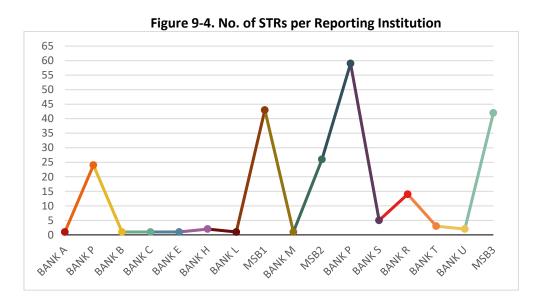
# STRs Related to Terrorism and Terrorism Financing

Despite the increasing incidents associated with the ASG and local threat groups, statistics show that not many STRs related to terrorism and terrorism financing were received by the AMLCS. In fact, it accounts only for 0.040%, 0.038% and 0.099% of the total STRs received for the period 2014 to 2016.

From 2014 –2016, there has been an increase in the no. of STRs received related to terrorism and terrorist financing accounting for an upsurge of 50% and 130%, respectively. The significant rise in the number of STRs received may be attributed to the submission of banks and money service businesses on the financing of an extremist terror group and certain individuals being linked to terror groups based in Australia and Indonesia accounting for 40% and 29% of the total STRs received from covered persons.



Transactions involved in the STRs related to terrorism and terrorism financing which were submitted by banks and MSBs are mostly withdrawals and remittances which were in amounts ranging from P500 to a high of PhP91.9 million.



Despite reports that stand-alone remittance agents are utilized more than banks in the movement of terrorist-related funds, only 3 MSBs submitted STRs for the given period. As TF-related transactions through MSBs usually fall below the threshold set by the law, it is not automatically captured by their AML systems. Reporting is then subject to the discretion of the MSBs.

The low number of reporting can be attributed to the fact that CPs are unable to detect Terrorism or TF-related transactions because they are unaware of specific indicators/typologies for said transactions to trigger reporting. There is thus a need to develop red flag indicators specifically for TF and cascade these indicators to CPs.

## Adequacy of Resources and Capacity of AMLC Secretariat personnel

The Financial Intelligence Analysis Staff (FIAS) is the primary unit tasked to collect and analyze all the STRs and CTRs deemed suspicious and submit their analysis reports to the Compliance Investigation Group (CIG) for further investigation. Presently, seven (7) analysts from the FIAS are conducting STR analysis, on top of their other equally important functions such as strategic analysis, data mining and operational/tactical analysis.

The Compliance and Investigation Group (CIG) of the Anti-Money Laundering Council Secretariat (AMLCS) is specifically tasked to handle money laundering (ML) and Terrorism Financing (TF) investigations. There are seven (7) subgroups comprising of 2-3 members, with each subgroup concentrating on specific predicate crimes defined under the AMLA, as amended. Only one (1) subgroup is handling TF cases.

The Legal Services Group (LSG) of the AMLCS has designated three (3) legal officers to handle litigation, two (2) of which have undergone training on money laundering and terrorism financing cases. The LSG evaluates the report of the CIG on terrorist financing cases and file the complaints with the Department of Justice (DOJ), which has created a task force composed of five (5) Prosecutors to evaluate and prosecute terrorism/terrorist financing cases.

# Focus of Intelligence

Military and LEAs have undergone formal training, albeit limited, on financial investigation relating to financing of terrorism. Focus of intelligence gathering of the military and LEAs is on terrorism and not on terrorism financing. This results in limited appreciation of evidence useful for terrorism financing during the investigation on terrorism. On the other hand, it is the mandate of AMLCS to investigate money laundering and terrorism financing.

## **Domestic Coordination**

Close cooperation with law enforcement agencies and other government agencies is essential in order to trace, seize and forfeit funds used or to be used for terrorist financing, and hurdle impediments such as bank secrecy laws to ensure successful prosecution of the said crime.

In May 2014, a Joint Terrorist Financing Investigation Group (JTFIG) was formed. The JTFIG is a task force composed of members from the anti-terrorism groups of the National Bureau of Investigation (NBI), Philippine National Police-Intelligence Group (PNP-IG), the PNP Criminal Investigation and Detection Group (PNP-CIDG), the PNP Directorate for Intelligence (PNP-DI), the PNP — Special Action Force (PNP-SAF), the Law Enforcement and Security Integration Office (LESIO), the Philippine Center on Transnational Crime (PCTC), the AMLC Secretariat and the US Federal Bureau of Investigation (US FBI).

The AMLC conducted financial investigation on the bank deposit account in relation to the ATM card recovered in one of the operations in June 2014. The subject account was ordered frozen for being owned and controlled by a UNSC designated entity, the Abu Sayyaf Group. As a result, the bank froze the funds in the subject bank deposit account. The AMLC Secretariat was also authorized to inquire into or examine the subject account.

AMLC investigation showed that the account was opened in 2011 using identification cards such as driver's license and social security card purportedly issued by the Land Transportation Office (LTO) and Social Security System (SSS), respectively. Verification by the AMLC with LTO and SSS revealed,

however, that the said government agencies have no record of such identification cards being issued by their offices, thus, the ID cards are fictitious.

During the course of the investigation, the LEAs and the AMLC were in close coordination and they continue to investigate other leads for the possible filing of civil forfeiture cases.

Close coordination with Philippine intelligence and law enforcement agencies, as well as intelligence authorities from a neighbor country was also key in the investigation of the kidnapping of 10 crew members from a foreign ship in 2016. The AMLC also takes an active part in the investigation of a Southern Philippines threat group who has recently gained national attention.

#### **CONCLUSION**

**Terrorism threat** in the Philippines is rated <u>HIGH</u> given the high number of violent incidents associated with terror/threat organizations. Prosecution of cases involving said groups are at a minimal level as compared to the number of incidents and victims recorded.

Similarly, **terrorism financing threat** is rated <u>HIGH</u> as terrorist/threat organizations in the country appear to have a systematic and established method of raising funds for their operations. The estimated amounts raised through illegal activities is very high. While the total amount raised by these organizations remain largely unknown, the high number of threat incidents recorded by the PNP indicate that these terrorist/threat organizations are well-funded.

Based on the overall assessment of factors, **terrorism financing vulnerability** of the Philippines is **HIGH**.

While remedies under the law are available to combat terrorism financing, the AMLC and law enforcement agencies are unable to utilize it due to several factors. The lack of resources and capacity impedes the ability to investigate and prosecute terrorism and terrorism-financing cases. For the given period, the AMLC was only able to investigate 18 TF cases and was able to freeze 43 bank accounts.

Another factor that contributes to the vulnerability of the Philippines to terrorism financing is the low number of reports submitted. This indicates a lack of awareness of covered persons in the detecting TF-related transactions.

Domestic (and international) coordination is one factor that should be further strengthened in combating the financing of terrorism. Recent experiences have shown that close domestic coordination among the AMLC and relevant government agencies yields positive results.

#### **ACTION PLAN**

ACTION PLAN	PRIMARY AGENCY	SECONDARY AGENCY	TIMELINE
Strengthen and maximize existing coordination mechanisms	Member	· · · · · · · · · · · · · · · · · · ·	Last
and ensure participation of relevant government agencies,	agencies		quarter of
through the execution of a Memorandum of Agreement for	of JTFIG		2017
information sharing among members of the JTFIG			
Develop red flag indicators/typologies on transactions	AMLC	BSP, SEC, IC	3rd
related to terrorism and terrorism financing, and			quarter of
disseminate to covered persons			2018

Creation of an inter-agency working group composed of the	AMLC,	1st
AMLC, BSP, BOC, CAAP, Coast Guard, for the enforcement of	BOC,	quarter of
cross border declarations and to combat physical smuggling	CAAP,	2018
of cash	Coast	
	Guard	

#### ANNEX A.

## **Financial Inclusion Stakeholders**

# **Government Institutions:**

Bangko Sentral ng Pilipinas (BSP)

Commission on Filipinos Overseas (CFO)

Cooperative Development Authority (CDA)

Department of Budget and Management (DBM)

Department of Education (DepEd)

Department of Finance (DOF)

Department of Social Welfare and Development (DSWD)

Department of Trade and Industry (DTI)

Insurance Commission (IC)

National Economic Development Authority (NEDA)

Philippine Deposit Insurance Corporation (PDIC)

Philippine Statistics Authority (PSA)

Securities and Exchange Commission (SEC)

Department of Agrarian Reform (DAR)

Department of Science and Technology (DOST)

# Associations of Financial Service Providers:

ABROI MCPI
APPEND MMCI
BAIPHIL NATCCO
BANGKOOP PCC
BAP PFCCO
BMAP RBAP

CTB VICTO National Cooperative Federation and

**Development Center** 

MASS-SPECC Cooperative Development Center

## Partners and Other Stakeholders:

Academe

Development Partners, International Organizations, Donor Agencies

Chambers of Commerce

Consumer Organizations or Stakeholder Organizations which refer to organized groups representing specific causes related to financial inclusion

NGOs or Foundations related to financial inclusion

Media Organizations

Source: National Strategy for Financial Inclusion