

ANTI-MONEY LAUNDERING COUNCIL

AMLC REGULATORY ISSUANCE (C) NO. 1 Series of 2018

Subject: AMLC Registration and Reporting Guidelines for Casinos

By the authority vested to the Anti-Money Laundering Council (AMLC) to implement measures as may be necessary and justified to counteract money laundering, in accordance with Section 7(7) of Republic Act (RA) No. 9160, also known as the Anti-Money Laundering Act of 2001, as amended (AMLA), the Council, in its Resolution No. 25, dated 19 February 2018, approved the adoption of the AMLC Registration and Reporting Guidelines for Casinos (ARRGC), and issue the same as an AMLC Regulatory Issuance (ARI).

Section 1. GENERAL PROVISIONS. -

A. Financial Action Task Force (FATF) Standards. -



The FATF is an inter-governmental policy-making body established in 1989 which sets the 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 financial system.

The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering, terrorist financing, and proliferation of weapons of mass destruction. These Recommendations form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally.

A key element in the fight against money laundering and terrorist financing is the need for countries' systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies (such as the Asia Pacific Group on Money Laundering [APG] of which the Philippines is a member-country), as well as the assessments conducted by the International Monetary Fund (IMF) and the World Bank (WB),

are vital mechanisms for ensuring that the FATF Recommendations are effectively implemented by all countries.

FATF Recommendation No. 24 requires that Designated Non-Financial Businesses and Professions (DNFBPs) shall be subject to regulatory and supervisory measures as set out below:

- 1. Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:
 - a. casinos should be licensed;
 - b. competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;
 - c. competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.
- 2. Casinos should ensure that other categories of DNFBPs are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations can ensure that its members to combat money laundering and terrorist financing.

B. Legal Framework. –

1. Anti-Money Laundering Act. –

RA No. 9160 or the AMLA was signed into law on 29 September 2001, and took effect on 17 October 2001. It was amended by RA Nos. 9194, 10167 and 10365, which took effect on 23 March 2003, 06 July 2012 and 07 March 2013, respectively.

The Implementing Rules and Regulations of the AMLA took effect on 02 April 2002. It was amended by the 2016 Revised Implementing Rules and Regulations (2016 RIRR), which took effect on 09 August 2017.

On 14 July 2017, RA No. 10927 was signed into law, designating casinos as covered persons under the AMLA. It took effect on 29 July 2017. The "Casino Implementing Rules and Regulations of Republic Act No. 10927" (CIRR) took effect on 04 November 2017.

2. Terrorism Financing and Suppression Act. -

RA No.10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA) was signed into law on 18 June 2012, and took effect on 05 July 2012. The Implementing Rules and Regulations of TFPSA took effect on 09 August 2017.

In relation to RA No. 10168, the AMLC issued Resolution Nos. TF-01 and TF-02, Series of 2012, directing the freezing without delay of property or funds, including related accounts, of designated terrorist individuals and entities named in the Al-Qaida Sanctions List pursuant to United Nations Security Council (UNSC) Resolution Nos. 1267/1989 and Taliban 1988 Sanctions List pursuant to UNSC Resolution No. 1988.

C. Covered Persons. –

The following are the Covered Persons (CPs) under the AMLA:

- 1. Banks, non-banks, quasi-banks, trust entities, pawnshops, non-stock savings and loan associations, electronic money issuers, foreign exchange dealers, money changers, remittance and transfer companies, and all other persons and their subsidiaries and affiliates, supervised or regulated by the Bangko Sentral ng Pilipinas (BSP).
- 2. Insurance companies, pre-need companies, insurance agents, insurance brokers, professional reinsurers, reinsurance brokers, holding companies, holding company systems, mutual benefit associations, and all other persons supervised or regulated by the Insurance Commission (IC).
- 3. Securities dealers, brokers, salesmen, investment houses and other similar persons managing securities or rendering services as investment agent, advisor, or consultant; mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities; other entities administering or otherwise dealing in commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or properties, supervised or regulated by the Securities and Exchange Commission (SEC).
- 4. The following Designated Non-Financial Businesses and Professions (DNFBPs):
 - a. Jewelry dealers, dealers in precious metals, and dealers in precious stones.
 - b. 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;
- 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.
- c. 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 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.

Lawyers and accountants who are: (1) authorized to practice their profession in the Philippines, and (2) engaged as independent legal or accounting professionals, in relation to information concerning their clients, or where disclosure of informatio would compromise client confidences, or the attorney-client relationship, are not covered persons.

- 5. Casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations.
 - a. 'Casino' refers to a business authorized by the appropriate government agency to engage in gaming operations:
 - i. 'Internet-based casinos' shall refer to casinos in which persons participate by the use of remote communication facilities such as, but not limited to, internet, telephone, television, radio or any

other kind of electronic or other technology for facilitating communication; and

- ii. 'Ship-based casino' shall refer to casinos, the operation of which is undertaken on board a vessel, ship, boat or any other water-based craft wholly or partly intended for gambling;
- b. 'Casino cash transaction' refers to transactions involving the receipt of cash by a casino paid by or on behalf of a customer, or transactions involving the payout of cash by a casino to a customer or to any person in his/her behalf; and
- c. 'Gaming operations' refer to the activities of the casino offering games of chance and any variations thereof approved by the appropriate government authorities.

D. Transaction Reporting Obligation. –

Section 9(c) of the AMLA requires all CPs to the AMLC all covered transactions and suspicious transactions within five (5) working days from occurrence thereof.

E. Covered Transaction Reports (CTRs). –

1. "Covered Transaction" refers to a single casino cash transaction involving an amount in excess of Five million pesos (P5,000,000.00) or its equivalent in any other currency.

"Casino Cash Transaction" refers to a transaction involving the receipt or payout of cash by and of a casino, paid or received by or on behalf of a customer, or such other cash transactions that may be determined by the AMLC and the AGA.

- 2. CTRs shall be filed within five (5) working days from occurrence of the transaction.
- 3. Submission of CTRs beyond 12:01 am of the day following the 5th working day from occurrence of the transaction shall be considered as non-submission of CTRs and may be subject to appropriate administrative sanction, if circumstances so warrant.

F. Suspicious Transaction Reports (STRs). –

- 1. "Suspicious Transaction" refers to a transaction, regardless of amount, where any of the following suspicious circumstances or indicators exists:
 - a. There is no underlying legal/trade obligation, purpose or economic justification;
 - b. The client is not properly identified;

- c. The amount involved is not commensurate with the business or financial capacity of the client;
- d. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
- e. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
- f. The transaction is in any way related to an unlawful activity or any money laundering activity or offense under the AMLA, that is about to be, is being or has been committed; or
- g. Any transaction that is similar, analogous or identical to any of the foregoing.
- 2. Recognizing Suspicious or Unusual Transactions.

Customer Identification Process (CIP), Customer Due Diligence (CDD) and Ongoing Monitoring of customers provide the basis for recognizing unusual and suspicious transactions and events. An effective way of recognizing suspicious activity is knowing enough about customers, their circumstances and their normal expected activities to recognize when a transaction or instruction, or a series of transactions or instructions, is unusual warranting the conduct of an internal inquiry, investigation and suspicious transaction reporting.

Likewise, it is essential for CPs to sufficiently know and understand the customer's business, to recognize whether a transaction or a series of transactions is unusual and, from an examination of the unusual transaction, whether there is a suspicion of money laundering. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, among other things, the transaction should be considered unusual and the covered person should be put on alert.

Where the inquiries do not provide a satisfactory explanation of the activity or transaction, an internal report should be made and properly escalated to the designated compliance officer and/or review committee to determine if there are grounds for suspicion warranting the filing of the STRs.

3. Alerts and Red Flags.

CPs should have systems in place that would alert its responsible officers of any suspicious circumstance or indicator that would give rise to a determination that a

suspicious transaction exists. The following is a list of non-exhaustive examples of situations or red flag indicators that may give rise to any of the suspicious circumstances or indicators:

- a. transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
- transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
- c. where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;
- d. where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
- e. where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;
- f. where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
- g. the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;
- h. transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and
- i. unnecessary routing of funds or other property from/to third parties or through third party accounts.

CPs are encouraged to develop their own list of alerts or red flag indicators taking into account the nature of their business, type of customers and risks involved.

5. Internal Analysis, Investigations and Escalation.

CPs shall formulate a reporting chain under which a possible suspicious transaction will be processed, analyzed and investigated. The reporting chain should include the designation of a Board Level or approval Committee or the Chief Compliance Officer

as the ultimate decision maker on whether or not the covered person should file a report to the AMLC.

The reporting chain, with reasonable timeframes starting from flagging, analysis, investigation, escalation and until the final decision is made, shall be clearly written in the covered person's Money Laundering and Terrorism Financing Prevention Program (MLPP). CPs should ensure that proper controls are in place to guarantee confidentiality of the process and that no "tipping-off" of customers will happen at all times during the entire proceedings. For this reason, the Compliance Officer shall have access to all customer information files and transactions through the electronic or manual customer monitoring system.

6. Timing and Manner of Submission of STRs.

CPs shall file STRs that are complete, accurate and timely in accordance with the following guidelines:

- a. CPs shall report to the AMLC all suspicious transactions within five (5) working days from the occurrence thereof.
- b. "Occurrence" refers to the date of determination of the suspicious nature of the transaction, which determination shall be made not exceeding ten (10) calendar days from date of transaction.
- c. Highly unusual or suspicious transactions, activities or circumstances conducted in the presence of, or immediately known or apparent to, the personnel handling the transaction shall be reported to the AMLC within five (5) working days from the date of the transaction. A "highly unusual" or suspicious transaction is one where, at the moment of transaction, the person handling the transaction has knowledge and reason to suspect that the funds being transacted are related to an unlawful activity.

Knowledge shall include:

- i. Actual knowledge;
- ii. Knowledge of circumstances which would indicate facts to a reasonable person; and
- iii. Knowledge of circumstances which would put a reasonable person on inquiry.
- d. For transactions triggered under an existing suspicious transaction monitoring system (TMS) where the suspicious transaction circumstances or indicators have been conclusively incorporated to the system, said

transaction shall be reported within five (5) working days from the date of transaction.

- e. Where the circumstances for filing an STR has no corresponding transaction, or when the TMS-generated alert is only a ground for the covered person to conduct an internal analysis, investigation and escalation, determination of the suspicious nature of the circumstances shall be made within a reasonable period of time. In such case, the covered person shall submit the corresponding STR using the "ZSTR" transaction code within five (5) working days after the said reasonable period, which in no case shall exceed sixty (60) calendar days from the time the circumstances were flagged. The report to be submitted in accordance with this item shall be comprehensive enough to establish the complete circumstances for the filing of the report.
- f. In cases where the transaction is in any way related to an unlawful activity, or the person transacting is involved in or connected to an unlawful activity or money laundering offense, the ten (10) calendar day determination period shall be reckoned from the date the covered person knew of, or should have known, the suspicious transaction indicator.

To determine whether the covered persons knew or should have known the suspicious transaction indicator, they shall be given reasonable period of time, which in no case shall exceed sixty (60) calendar days, to gather facts in order to enable the submission of a meaningful STR.

- g. The reasonable period shall be indicated in the covered person's MLPP. The MLPP shall be duly approved by the covered person's Board of Directors, as well as the designation of the Board approved Committee or Board Level Committee or duly authorized Senior Officer as the Body or Officer who shall make the final determination of whether or not an STR should be filed.
- 7. Uploading of KYC Documents is mandatory for transactions related to any of the following Predicate Crimes:

PC1	_	Kidnapping for Ransom
PC2	_	Drug Trafficking
PC12	-	Hijacking; destructive arson; and murder, including those perpetrated by terrorists against non-combatant persons and similar targets
PC13	-	Terrorism and conspiracy to commit terrorism
PC14	_	Financing of Terrorism

If the AMLC Secretariat, requests for the KYC Documents for STR previously filed with the AMLC, wherein, subject of the STR has an existing money laundering case, CPs should be able to upload said KYC documents.

See Section 4.B.3 of this ARI for the step-by-step procedure in the Uploading of KYC Documents.

- 8. Should a transaction be determined to be both a covered and a suspicious transaction, the CP shall report the same as a suspicious transaction.
- G. Guidelines in Reckoning CPs' Compliance with the Prescribed Reporting Period. -
- 1. The following non-working days are excluded from the counting of the prescribed reporting period:
 - a. weekend (Saturday and Sunday);
 - b. official regular national holiday; and
 - c. officially declared national holiday and workday suspensions
- 2. A "non-reporting day" may be declared by the AMLC Secretariat when the File Transfer and Reporting facility (FTRF), used by the CPs in transmitting their electronic reports to AMLC is unavailable to all CPs for at least five (5) consecutive hours during the day.
 - a. AMLC-declared "non-reporting day" is excluded from the counting of the prescribed reporting period.
 - b. The Executive Director or, in his absence, the Officer-in-Charge of the AMLC Secretariat is authorized to declare such day as a "non-reporting day.
- 3. Officially declared non-working days in localities or regions affected by natural calamities such as flood, typhoon, earthquake, etc. may be excluded from the counting of the prescribed reporting period for CPs located in the affected localities or regions subject to submission of deviation request by the CP.

CPs' request for deviation shall be subject to approval of the Executive Director or, in his absence, the Officer-in-Charge of the AMLC Secretariat.

H. Ensuring Accuracy and Completeness of CTRs and STRs. -

The Appropriate Government Agencies (AGAs) shall ensure that casinos, casino operators and licensees, and integrated resorts under their respective regulation shall install an anti-money

laundering/counter-terrorism financing (AML/CTF) reportorial system within a reasonable time, not to exceed ninety (90) days from publication of this ARI, upon consultations with the AMLC.

Section 29 of the CIRR states that CPs shall ensure the accuracy and completeness of CTRs and STRs, which shall be filed in the forms prescribed by the AMLC and shall be submitted in a secured manner to the AMLC in electronic form. Casinos shall ensure the accuracy and completeness of CTRs and STRs in accordance with the reporting procedures prescribed by the AMLC.

I. Applicability of the Rules on the Imposition of Administrative Sanctions. –

Violations of this ARI shall be subject to administrative sanctions, in accordance with the "Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as Amended", which took effect on 09 August 2017. The "Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as Amended", applies to casinos, pursuant to Section 37 of the CIRR.

Covered persons should note that non-filing, late filing, and filing of incomplete and/or inaccurate CTRs/STRS, among others, constitute violations of the AMLA and the CIRR.

J. Implementation. –

This ARI shall be implemented immediately after its effectivity, except for the provisions of Section 4 (Reporting System) hereof, which shall be implemented ninety (90) days after its effectivity.

To enable casinos to test their respective systems, the AMLC Secretariat undertakes to make itself available to accept reports sixty (60) days after publication of this ARI.

K. Effectivity. –

This ARI shall take effect fifteen (15) calendar days after its publication in a newspaper of general circulation, and filing with the Office of the National Administrative Register at the University of the Philippines Law Center.

Section 2. ONLINE REGISTRATION SYSTEM. -

One of the many functions of the Anti-Money Laundering Council (AMLC) is "To require and receive covered or suspicious transaction reports (CTRS/STRs) from covered casinos" (Rule IV, Section 7a).

In addition, Rule 8, Section 32 of the CIRR of the AMLA states that "All casinos shall register with the AMLC's electronic reporting system within ninety (90) days from the effectivity of this CIRR".

In order to transmit CTRs and STRs, CPs need to register with the AMLC in order to be given access to the AMLC Portal.

The Online Registration System for CPs will allow Compliance Officers to manage their user accounts as well as that of their alternates. The system will also provide a means of monitoring CP's user accounts by requiring Compliance Officers to update their information every two (2) years.

A. Guidelines. –

 Before proceeding with the Online Registration, Compliance Officers (COs)/Associated Persons (APs) /Primary Designated Officers (PDOs) should have document/s showing his/her designation. Documents should be uploaded in PDF format.

Notarized Secretary Certificate showing the appointment of the Compliance Officer, Rule V, Section 13 and 14 of the CIRR requires the designation of an AML Compliance Officer, who shall at least, be of senior management level.

- 2. COs should download the **Transaction Security Protocol Manual (Section 2 this ARI)** from www.amlc.gov.ph and perform the following steps:
 - a. Download the Gnu Privacy Guard (GPG) software from www.amlc.gov.ph under the Reporting Tools tab.
 - b. Install the GPG Software.
 - c. Generate public key.
 - d. Export public key (file extension is .asc).

Be ready with your exported asc file as this will be needed during online registration

- e. Get and save the AMLC public key (amlc.asc) fromwww.amlc.gov.ph under the Reporting Tools tab.
- f. Import the AMLC Public key (amlc.asc).
- g. Certify and Sign AMLC Public key.
- h. Back up of COs Public key.

- 3. Once Items 1-2 have been performed/accomplished, COs may now proceed with the Online Registration (https://portal.amlc.gov.ph).
- 4. Registration will be processed daily; cut-off time is 1:00 PM, registration received after 1:00 PM will be processed the following day.
- 5. The Secretariat will issue a Certificate of Registration, with the facsimile signature of the AMLCS Executive Director or the Officer-in-Charge to successfully registered Casnos, upon request. The said certification will be sent via email as a PDF file.
- 6. A two (2) year mandatory update of the registration via the Online Registration System is required. Failure to update the registration will result in the deactivation of the Casino's user access in the AMLC Portal.

Log-on to https://portal.amlc.gov.ph

Anti Money Laundering Cour X +				- 0	X
C 0 🔬 https://portal.amic.gov.ph/amic/		☆ 自	↓ 1		≡
Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit					
Welcome to the Anti-Money Laundering Council Portal! (Ver. 2.8.4) The facility allows Covered Persons (CPs) to accomplish the following: *Online Registration *Online Compliance Officers to register and attach supporting documents. Submission of hardcopy documents are no longer required. *Upload CIR/STR Files * Conversed Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) may be conveniently transmitted to the AMLC via this * View Nictory of Uploaded CIR/STR Files	User Login Institution Code: Username/Email: Password: EORGOT PASSV Note: CPs wth 11-digit Inst.	 <u>VORD</u> Code - 1st (5 digits	_	E
to download the validation messages. *View News Advisories - New and archived AMLC advisories may be accessed from this facility. *Upload Attachments to STRs - Digital attachments to Suspicious Transaction Reports (STRs) may be submitted through this facility. The STR should have been uploaded first prior to uploading of attachments.	CPs with 18-digit Inst. REGISTER Registration Status?	Code - 1st CLICK HERE	9 digits		
*View History of Uploaded Attachments to STRs - Access history and status of uploaded STR attachments.		AMLC © 2	010 . All	rights res	erved. •

1. Click on <u>Register</u>

Anti Money Laundering Cou 🗴 +			- 0	x
C 🖉 🔬 https://portal.amic.gov.ph/amic/	h 🗘	iê ↓ 1		≡
Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit				
<section-header><text><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></text></section-header>	User Login Institution Code: Username/Email: Password: EORGOT PASSWOR Note: CPs with 11-signt Inst. Coc CPs with 11-signt Inst. Coc Registration Status? CLI	D de - 1st 6 digits de - 1st 9 digits CK HERE		E ,
	A	MLC © 2010 . All	riahts rese	rved

2. Covered Person/Casinos Registration page will appear, please read the instructions first before proceeding to Step 1 of 3.



Step 1 of 3: Key in details of the Casinos and Contact Details of the Authorized Officer. Once step 1 of the Registration process is completed, click on Next to go to the 2nd step.

	COVERED PERSON REGISTRATION
	STEP 1 OF 3: COVERED PERSON
INFORMATION	
Institution Code:	
Supervising Agency:	PAGCOR
Industry Type: *	INTEGRATED RESORT
Institution Name: *	ABC CASINO
Address (Head Office): *	24TH STREET MANILA AVENUE
City/Municipality: *	MANILA
Zip Code: *	1200
CONTACT DETAILS	
Telenhone Number: *	02 0999999
	02 1234567
Fax Number:	02 8888888
	02 1234567
Name of President/ CEO/ Owner: *	JUAN C. DELA CRUZ
Desitions 8	First Name MI Last Name
Position: **	[PKE5IDENI]
	Next Clear Form Exit

Note: Be sure to have a scanned copy of your document/s stating your appointment as the CO; have generated your public key using Kleopatra and have your exported asc file before proceeding to the next page (Step 2 of 3).

3. Step 2 of 3 are the details of the CO, as well as the key details of their public key. This is also where the CO uploads supporting documents (PDF) of his/her appointment and his exported asc file. If there is no alternate, click "Done", otherwise click "Add Alternate".

STEP 2 OF 3: AUTHORIZED PERSONNEL			
COMPLIANCE OFFICER INFORMATIC	DN		
Institution Code: Title: * Full Name: *	MS JANE C. REYES		
Position: * e-Mail Address: * Telephone Number: *	First Name MI Last Name Make sure email address is unique; CHIEF COMPLIANCE OFFICER CO and alternate/s (if any) should have different email addresses 02 1234567		
Supporting Documents: *	02 1234567 Choose File BOARD RESOLUTION.pdf e.g. Board Resolution, DTI Certificate and etc. Doc/s showing appointment of Compliance Officer		
KEY DETAILS			
Key ID: * Generation Date: * Fingerprint: *	04B38546 Key details 04-24-2018 Can be seen 957798A09AF2370BCF89DD963BFE4B9704B38546 in Kleopatra		
Key (ASC) File: *	Choose File 957798A09AF4B38546.asc Exported asc file of the public key, created in Kleopatra		
	Previous Add Alternate Done Clear Form Exit		
	If CO has no alternate, Click Done; otherwise Click Add Alternate.		

4. Continue to add details of the alternate (if any). Public key (Key details) of the Alternate is optional.

	STEP 2 OF 3: AUTHO	RIZED PERSONNEL
ALTERNATE 1 INFORMATIO	N	
Title: *	MR.	
Full Name: *	MARK N. RIVERA	
	First Name MI Last Name	Make sure email address is unique
Position: *	AML ASSISTANT	CO and alternate/s (if any) should
e-Mail Address: *	mnrivera@yahoo.com	have different email addresses
Telephone Number: *	02 7654321	
	02 1234567	
KEY DETAILS		
	Previous Cancel Add Altern	ate Done Clear Form Exit
	If alterna	te has no generated
	public key	and there is only one
	alternate	Click Done: otherwise
		Alternate
	Click Add	Alternate

If alternate generated a public key, please continue with the key details

		STEP 2 OF 3: AUTHORIZED PERSONNEL
	ALTERNATE 1 INFORMATION	
	Title: * Full Name: *	MR MARK N. RIVERA
	Position: * e-Mail Address: *	AML ASSISTANT mnrivera@yahoo.com
	Telephone Number: *	02 7654321 02 1234567
	KEY DETAILS	
For	Key ID: *	E537B4C6
Alternate	Generation Date: *	04-24-2018
with	Fingerprint: *	E389094B4C77A36E59870552993618ECE537B4C6
Public	Key (ASC) File: *	Choose File E389094B4C7537B4C6.asc
key; check		
on Key details		Previous Cancel Add Alternate Done Clear Form Exit
		If there is only one alternate Click Done; otherwise Click Add Alternate

5. Step 3 of 3 shows the Summary of Registration, if all details are correct, Click "Save"; to edit details of registration, Click "Previous", to exit page without saving, Click "Exit".

		STEP 3 OF 3: SUMMARY OF REGISTRATION		
COVERED	PERSON INFORMATION			
Reference Institution C	Number: Code:	jcreyes@yahoo.com20180424221915-06c3d21ab4f9fa0645c7a09913fffc81		
Supervising Industry Typ Institution N	Agency: pe: lame:	INTEGRATED RESORT ABC CASINO		
raaress: City/Municip Zip Code:	pality:	MANILA 1200		
CONTACT	DETAILS			
Telephone N Fax Number Authorized F Position:	lumber: ": Person:	(02) 9999999 (02) 8888888 JUAN C. DELA CRUZ PRESIDENT		
COMPLIA	NCE OFFICER INFORMATI	ON		
Title: Full Name: Position:	MS. JANE C. REYES CHIEF COMPLIANCE OFFICE	R		
e-Mail Address: Telephone	jcreyes@yahoo.com (02) 1234567			
Number: User Name: Board	jcreyes@yahoo.com			
Resolution:	BOARD RESOLUTION.pdf			
KEY DETA	AILS			
Key ID: Generation	04B38546			
Date:	04-24-2018			
Fingerprint: Key (ASC) File:	957798A09AF2370BCF89DD	9638FE489704838546.asc		
0	I hereby declare that the detail information is found to be false	s furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of a or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.	y changes therein, immediately. In case any of the above	
ALTERNA	TE 1 INFORMATION			
Title: Full Name: Position:	MR. MARK N. RIVERA AML ASSISTANT			
e-Mail Address:	mnrivera@yahoo.com			
Telephone Number: User Name:	(02) 7654321 mnrivera@yahoo.com			
KEY DETA	AILS			
Key ID:	E537B4C6			
Generation	04-24-2018			
Fingerprint:	E389094B4C77A36E598705	52993618ECE537B4C6		
Key (ASC) File:	E389094B4C77A36E598705	52993618ECE537B4C6.asc		
	I hereby declare that the detail information is found to be false	s furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of an or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.	y changes therein, immediately. In case any of the above	
		Previous Save Exit		

Click check box to accept truthfulness of information

Click check box to accept truthfulness of information 6. After you click Save, a window will appear, showing that Registration has been successful. Please take note of your Reference No. You will need this to check the status of your Registration.

	REGISTRAT	ION SUCCESSFUL		
DEEEDENCE NO. 100	VES01201702101	51400-5736750165	4ca5a0h012e88f	5006c120
KEI ERENCE NO. JCKE	1201201702101	51429 5750756105	400300912000	50900120
Your registration has bee	n successfully submitt	ed for our review. Plea	ise take note of your	r Reference
Number and	regularly check your c	mail for the next instru	ctions. mank you.	
		Exit		
Dopublic of the Dhilir	aninon			
	upines	<u></u>		
Art Money Laundering Council	y Laundering Coun			
	s Financial intelligence On	u		
	REFERENCE NO: JCREYES01	Are you sure you want to leave this page?	a5a0b912e88f5096c120	
	Your registration has been succe Number and regular		take note of your Reference	
		OK Cancel		

7. To verify if your Registration has been successful, please check your registered email and click the link to verify your email address.

Subject:	Email Address Verification
From:	NoReply@amlc.gov.ph (NoReply@amlc.gov.ph)
то:	rlynpineda@yahoo.com;
Date:	Friday, February 10, 2017 4:31 PM

Dear MS. JANE C. REYES,

Your account will be activated after you have verified your email address.

Please click the link below to validate your email address!

http://192.168.6.55:8080/amlc/web/validate-email.htm?code=JCREYES0120170210163112CO-684cbfae819295e515fc80ef65927316

Note: If the link does not work by clicking on it, try to copy and paste the link to your browser. This is a system generated email, please do not reply!

Thank you, AMLC - IMAG

Click on the link to verify the email address of the Compliance Officer

Dear Mr. MARK N. RIVERA,

Your account will be activated after you have verified your email address.

Please click the link below to validate your email address!

 $\label{eq:http://192.168.6.55:8080/amlc/web/validate-email.htm?code=JCREYES0120170210163131A1-b6c9e793a21080e38461201754565ad3}{\label{eq:http://192.168.6.55:8080/amlc/web/validate-email.htm}}$

Note: If the link does not work by clicking on it, try to copy and paste the link to your browser. This is a system generated email, please do not reply!

Thank you, AMLC - IMAG

Click on the link to verify the email address of the Alternate

Note: Email verification will be sent to the email address of the CO, as well as the designated alternate (if any).

8. After the CO and alternate have validated their email addresses, this page will appear, just click "Agree".



Then click on the "Exit" button.



9. To check the status of your Registration, log-in to <u>https://portal.amlc.gov.ph</u>, and click on Registration Status.

🔗 Anti Money Laundering Cou: x +				- 0	X
() 🚱 https://portal.amic.gov.ph/amic/	'n	☆ 自	↓ 1		∍≡
Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit					
Welcome to the Anti-Money Laundering Council Portal! (Ver. 2.8.4)	User Login				
The facility allows Covered Persons (CPs) to accomplish the following:	Institution Code:				
*Online Registration - Allows Compliance Officers to register and attach supporting documents. Submission of hardcopy documents are no longer required.	Username/Email:				
*Upload CTR/STR Files - Encrypted Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) may be conveniently transmitted to the AMLC via this facility.	Password: LOGIN FORGOT PASS	 			E
*View History of Uploaded CTR/STR Files - Access history of uploaded CTR/STR files. Errors are logged, allowing users to identify and make the necessary corrections. Users also have the option to download the validation messages.	Note: CPs with 11-digit Inst. CPs with 18-digit Inst	Code - 1st 6 Code - 1st 9	3 digits 9 digits	_	
*View News Advisories - New and archived AMLC advisories may be accessed from this facility.	Registration Status?	CLICK HERE!	1		
 *Upload Attachments to STRs Digital attachments to Suppicious Transaction Reports (STRs) may be submitted through this facility. The STR should have been uploaded first prior to uploading of attachments. *View History of Uploaded Attachments to STRs Access history and status of uploaded STR attachments. 		1			
		AMLC © 2	010 . All i	rights re	served. 👻

Please enter the reference number of your Registration.

Republic of the Philippines Anti-Money La The Philippines' Finan	undering Council ncial Intelligence Unit
	REGISTRATION STATUS INQUIRY Reference Number: Submit Exit

If you have not received an email from AMLC requesting verification of your account, please check your registration status, it will show if the email address is still **unverified**, if still unverified, please check if the email address is correct and edit accordingly. Then click the "Resend" button.

	REGISTRATION STATUS
	On Queue: For Email Verification!
COVERED PERSON I	INFORMATION
Reference Number: Institution Code: Supervising Agency: Industry Type: Institution Name: Address: City/Municipality: Zip Code:	jcreyes@yahoo.com20180424221915-06c3d21ab4f9fa0645c7a09913fffc81 PAGCO INTEGRATED RESORT ABC CASINO 24TH STREET MANILA AVENUE MANILA 1200
CONTACT DETAILS	
Telephone Number: Fax Number: Authorized Person: Position:	(02)9999999 (02)8888888 JUAN C. DELA CRUZ PRESIDENT
COMPLIANCE OFFIC	CER INFORMATION
Title: Full Name: Position: e-Mail Address: Telephone Number: User Name:	MS. JANE C. REYES CHIEF COMPLIANCE OFFICER jcreyes@yahoo.com Resend (unverified) (02)1234567 jcreyes@yahoo.com
KEY DETAILS	
Key ID: Generation Date: Fingerprint:	04B38546 04-24-2018 957798A09AF2370BCF89DD963BFE4B9704B38546
ALTERNATE 1 INFO	RMATION
Title: Full Name: Position: e-Mail Address: Telephone Number: User Name:	MR. MARK N. RIVERA AML ASSISTANT mnrivera@yahoo.com Resend (unverified) (02)7654321 mnrivera@yahoo.com
KEY DETAILS	
Key ID: Generation Date: Fingerprint:	E537B4C6 04-24-2018 E389094B4C77A36E59870552993618ECE537B4C6

10. Once AMLC has processed your Registration, you will receive an email from AMLC whether Registration has been approved or disapproved. Below is a sample email of an approved Registration.

This is to inform you that your registration has been approved. Below is your Username and temporary Password. Please log-in and change your password as soon as you received this email. Please take note that your user account shall be valid for two (2) years from the date of account approval.

Institution Code: 12345600000

Username: JCREYES@YAHOO.COM

Password: Q2CT1PH9KL

For Compliance Officers and/or alternates with generated public keys, please perform the following: 1. Download the AMLC public key (amlc.asc) on this link www.amlc.gov.ph/2015-12-09-07-34-10 /reporting-tools

2. Save the AMLC public key (amlc.asc) to:

a. For 32 bit machine - C:\Program Files\GNU\GnuPG\

- b. For 64 bit machine C:\Program Files(x86)\GNU\GnuPG\
- 3. Import the AMLC public key (amlc.asc).
- 4. Certify and Sign the AMLC public key (amlc.asc).
- 5. Perform a back up of your public key (your exported asc file).

**For guidance please download the AMLC Reporting Procedure manual at www.amlc.gov.ph and refer to the Transaction Security Protocol chapter for a step-by-step procedure.

This is a system generated email, please do not reply!

Thank you, AMLC - IMAG

Please note that AMLC can only approve your Registration when the Compliance Officer and all the registered alternate/s have verified their email addresses.

11. Once registration has been approved, log-in to <u>https://portal.amlc.gov.ph</u> to change your password. Please log in using the first 6-digits of your institution code, email address and system generated password.

Welcome to the Anti-Money Laundering Council Portal! (Ver. 2.8.4)	User Login	
he facility allows Covered Persons (CPs) to accomplish the following:	Institution Code:	
Online Registration Allows Compliance Officers to register and attach supporting documents. Submission of hardcopy documents are no longer required.	Username/Email: Password:	
Upload CTR/STR Files Encrypted Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) may be conveniently transmitted to the AMLC via this colity.	FO	LOGIN RGOT PASSWORD
View History of Uploaded CTR/STR Files Access history of uploaded CTR/STR files. Errors are logged, allowing users to identify and make the necessary corrections. Users also have the option o dwnload the validation messages.	Note: CPs with 1 CPs with 1	11-digit Inst. Code - 1st 6 digits 18-digit Inst. Code - 1st 9 digits
View News Advisories New and archived AMLC advisories may be accessed from this facility.	Registrati	REGISTER on Status? <u>CLICK HEREI</u>
Upload Attachments to STRs Digital attachments to Suppicious Transaction Reports (STRs) may be submitted through this facility. The STR should have been uploaded first prior to ploading of attachments.		
View History of Uploaded Attachments to STRs Access history and status of uploaded STR attachments.		

Password: Confirm Password:	
	Submit

Once password has been changed, you can now start to access the AMLC portal.

Section 3. TRANSACTION SECURITY PROTOCOL GUIDELINES. –

A. Guidelines. –



- 1. The File Transfer and Reporting Facility using the Hypertext Transfer Protocol over Secure Socket Layer (FTRF v 2.0) shall be used by the Casinos in transmitting their respective reports.
- 2. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a private, secure and graphical method of accessing web page information and/or sending information across a web. It is especially useful for encrypting forms-based information as it passes between clients and servers. HTTPS which is implemented under the File Transfer and Reporting Facility (FTRF v 2.0) will address the efficiency, integrity and security concerns of data collection from the Covered Persons.
- 3. File Transfer and Reporting Facility (FTRF) has the following features:
 - 1. Secure upload provides data encryption, server authentication and message integrity;
 - Self-signed Digital Identification & Certificate allows encrypting and digital signing of messages; and
- 4. The self-signed digital identification shall be implemented for all Casinos. AMLC and the Casinos shall use the Gnu Privacy Guard (GPG) software for their encryption and authentication and the GPG supported algorithm (MD5) for their signing. Installer of the said software shall be provided by AMLC upon registration.
- 5. The Compliance Officer (CO) of the Casinos shall generate his private key as well as public key using GPG which shall be uploaded during the Online Registration.
- 6. The signed public key of the AMLC shall be used by the Casinos to:
 - 1. Encrypt the electronic files (CTR/STR in csv format) to be submitted to AMLC; and
 - 2. Verify the signature of the files they will receive from AMLC.

- 7. The signed private key of the AMLC shall be used by AMLC to:
 - a. Decrypt the encrypted files sent by the Casinos which were encrypted using AMLC's signed public key; and
 - b. Sign the electronic files they will send to the Casinos.
- 8. The signed public key of the COs shall be used by the AMLC to:
 - a. Encrypt the validation messages that AMLC will send to the Casinos; and
 - b. Verify the signature of the files AMLC will receive from the Casinos.
- 9. The signed private key of the COs shall be used by them to:
 - a. Decrypt the AMLC validation messages from AMLC; and
 - b. Sign the electronic files they will send to AMLC.
- 10. COs are required to encrypt and sign the electronic CTR/STR files before transmitting them to AMLC via https (AMLC portal).
- 11. In cases wherein the public key is compromised, superseded or no longer in use, COs should perform the recovery procedure, only if they have successfully performed the back-up procedure of their existing private and public keys, to be able to continue to encrypt file. Otherwise, a new pair of public and private keys shall be generated and to be uploaded via the Online Registration System.
- B. Procedures. -
- 1. Installing the GnuPG for Windows Software (Gpg4win 2.1.0)
 - Download the gpg4win 2.1.0 from <u>www.amlc.gov.ph</u>, under Reporting Tools, then save this to your local drive.
 - Double click **gpg4win-2.1.0.exe**. You will be asked if you want to allow the program to make changes in your computer.
 - Click **Yes**. The Installer Language window will be displayed on the screen.
 - Select *English*, then click **Ok**.





The License Agreement window will be displayed on the screen. Click Next.

🕑 Gpg4win Setup	-				x
	License Agreeme This software is lic Public License (GPL	ent ensed under t .).	he terms of the	e GNU Genera	al
Press Page Down to see	the rest of the agreem	ent.			
G	NU GENERAL PUBLIC LI Version 2, June 1991	CENSE			
Copyright (C) 1989, 19 51 Franklin Street, Fi Everyone is permitted t of this license documen	91 Free Software Found fth Floor, Boston, MA o copy and distribute ve t, but changing it is not	dation, Inc. 02110-1301 U erbatim copies allowed.	ISA		
	Preamble				
The licenses for most s	oftware are designed t	o take away y	our		-
In short: You are allowed as you give the recipient Nullsoft Install System v2.3	t to run this software fo s the same rights you h	or any purpose ave received.	e. You may dist	tribute it as lo	ng
	(< <u>B</u> ack	Next >	Cano	cel

Setup

Click

Gro D	Choose Components Choose which features of Gpg4	win you want to install.
Check the components you install. Click Next to continue	vant to install and uncheck the c	omponents you don't want to
Select components to install:	✓ GnuPG ✓ Kleopatra □ GPA ✓ GpgOL ✓ GpgEX □ Claws-Mail ✓ Gpg4win Compendium	Description Position your mouse over a component to see its description,
Space required: 102.5MB		
Jullsoft Install System v2.37-3		

Select components to install. Check *Kleopatra*, *GpgEX*, and *Gpg4win Compendium*, then uncheck other components. Click **Next**.



Specify destination folder, then, click **Next**.

• For 32 bit machine the default directory is C:\Program Files\GNU\GnuPG.

10	Choose Install Location
Gre U	Choose the folder in which to install Gpg4win.
Setup will install Gpg4w	win in the following folder. To install in a different folder, dick Browse
and select another fold	der. Click Next to continue.
Destination Folder	
Destination Folder	(x86)\GNU\GnuPG Browse
Destination Folder	(x86)\GNU\GnuPG
Destination Folder	(x86)\GNU\GnuPG
Destination Folder C: Program Files () pace required: 101.07 pace available: 237.9	X86)\GNU\GnuPG Browse
Destination Folder	(x86)\GNU\GnuPG IMB 9GB

 For 64 bit machine the default directory is
 C:\Program Files (x86)\GNU\GnuPG.



🕑 Gpg4win Setup		
Gro D	Choose Start Menu Folder Choose a Start Menu folder for the Gpg4wi	n shortcuts.
Select the Start Menu fold can also enter a name to o	er in which you would like to create the program reate a new folder.	m's shortcuts. You
Gpg4win		
Accessories Administrative Tools Games Hummingbird Intel KONICA MINOLTA Lotus Applications Maintenance Microsoft .NET Framewor Microsoft Office NVIDIA Corporation Oracle - OraClient 11g_ho	k SDK v2.0 me1	E
Nullsoft Install System v2,37-	3	I Cancel

Choose Start Menu folder for the Gpg4win shortcuts. Enter **Gpg4win**, then click **Install**.

	🚱 Gpg4win Setup
	Please wait while Gpg4win is being installed.
	Extract: view-refresh.png
Please wait while	Show details
Gpg4win is being installed.	
	Nullsoft Install System v2.37-3
	<pre></pre>

© Gpg4win Setup Installation Complete Setup was completed successfully.	
La Completed Show <u>d</u> etails	Once the setup is completed successfully, click Next .
Nullsoft Install System v2.37-3	

Check Root certificate

or

skip

then

defined

configuration, click **Next**.

GFG U	Define trustable root certificates S/MIME configuration	
Gpg4win needs a lis	st of root certificates which you trust.	
(To use S/MIME cer of X.509 root certif	rtificates for sign and encrypt, you have to define the trustability ficates.)	^
A root certificate (r If you trust the roo	root CA) is used to check the validity of all child certificates. ot certificate therby you trust also all underlying certificates.	
1.1		
To avoid that each also check and auth a system-wide defa	user must search and install the required root certificates, and henticate the trustworthiness of the same, it is useful to install ault of the most important root certificates:	Ŧ
To avoid that each also check and auth a system-wide defa Therewith you can u configuration only if	user must search and install the required root certificates, and henticate the trustworthiness of the same, it is useful to install ault of the most important root certificates: use S/MIME, the configuration is stringently required. Skip this f you don't want to use S/MIME.	Ŧ
To avoid that each also check and auth a system-wide defa Therewith you can u configuration only if	user must search and install the required root certificates, and henticate the trustworthiness of the same, it is useful to install ault of the most important root certificates: use S/MIME, the configuration is stringently required. Skip this f you don't want to use S/MIME. defined or skip configuration	Ŧ



2. Generation of Key Pairs (One time Procedure)



	New Certificate	Ctrl+N		-
	Lookup Certificates on Server	Ctrl+Shift+I	n Lookup Certificates on Server	
- -	Import Certificates	Ctrl+I	My Certificates	
200	Export Certificates	Ctrl+E	cates	sele
200 200	Export Secret Keys	Control E	Until Details Key-ID	Cer
1	Export Certificates to Server	Ctrl+Shift+E		
R	Decrypt/Verify Files			
•	Sign/Encrypt Files			
	Create Checksum Files			
	Verify Checksum Files			
8	Close	Ctrl+W		
~	Quit	Ctrl+Q		_

e, then New ate.

Certificate Creation Wizard will be displayed on the screen. Click Create a personal OpenPGP key pair.

I		Certificate Creation Wizard
(Cho	ose Certificate Format
1	Plea	se choose which type of certificate you want to create.
	÷	<u>C</u> reate a personal OpenPGP key pair OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every
	→	Create <u>a</u> personal X.509 key pair and certification request X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of
		Next Canc <u>e</u> l

Enter Det Please ent certificate	ertificate Creation Wizard ails er your personal details below. If you want more control ove parameters, click on the Advanced Settings button.	er the	Enter Details then click Advance Settings.
Name:	Juan C. Dela Cruz	(required)	
EMail:	juan.delacruz@yahoo.com	(required)	
Comment:	ABC Bank	(optional)	
J	uan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com <u>A</u>dvanced <u>N</u>ext</juan.delacruz@yahoo.com 	> Settings <u>C</u> ancel	

Note:

Name – Name of Compliance Officer Email – Email address of Compliance Officer Comment – Name of the Casino

The		Technical
Deta	ails	window
will	be	displayed
on t	he so	creen.

- From Key Material, select DSA: 2,048 bits (default).
- Check + Elgamal
 :2,048 bits
 (default).
- From Certificate Usage, check
 Signing,
 Encryption and Certification.
- Click Ok.



Enter Det	ertificate Creation Wizard			
Please ent	ans er your personal details below. If you want more parameters, click on the Advanced Settings but	e control over the ton.	From Certificate Creation	the Wizard
Name:	Juan C. Dela Cruz	(required)	window,	click
EMail:	juan.delacruz@yahoo.com	(required)	Next.	
Comment:	ABC Bank	(optional)		
J	uan C. Dela Cruz (ABC Bank) <juan.delacruz@< td=""><td>yahoo.com> Advanced Settings</td><th></th><td></td></juan.delacruz@<>	yahoo.com> Advanced Settings		
	1	lext <u>Cancel</u>		



pinent	ny 🔼
	Enter passphrase
	Passphrase
	Quality:
	<u>OK</u> <u>C</u> ancel

Re-enter

Pinentry window will be displayed on the screen. Enter Passphrase (gpg password of compliance officer), then click Ok.



Please be reminded that once you forget your passphrase, you need to generate a new public key, since AMLC cannot retrieve the said passphrase.

I	Certificate Creation Wizard	
	Creating Key	
	Your key is being created.	
	The process of creating a key requires large amounts of random numbers. To foster this process, you can use the entry field below to enter some gibberish. The text itself won't be used at all, only the inter-character timing. You can also move this window around with your mouse, or start some disk-intensive application.	
	Next Cancel	

Wait until the key pair is successfully created.

	Key Pair Successfully Created
•	Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
	Result
	Certificate created successfully. Fingerprint: 7F2C0A8B90C6E4E83FFDFC4E09D7D50EBC5CC263
	Next Steps
	Make a Backup Of Your Key Pair
	Send Certificate By EMail
	Upload Certificate To Directory Service

Click Finish.
3. Exporting Public Key

	e view Cell	tilicates Tools	Settings	window Heip)	
		i i i i i i i i i i i i i i i i i i i	C	8	<i>i</i>	
Im	port Certificates	Export Certificates	Redisplay	Stop Operation	Lookup Certificates	on Server
F <u>i</u> nd	d:		Export Cer	tilicates	My Cert	tificates
••	My Certificate	es T <u>r</u> usted Ce	rtificates	Other Certificat	es	
	Name	E-Mail	Valid Fro	om Valid U	ntil Details	Key-ID
(Juan C j	uan.delacru 2	2012-02-08		OpenPGP	BC5CC263
•						

From your desktop, double click Kleopatra. The Kleopatra main window will be displayed on the screen. Click the name of compliance the officer, then click Export Certificates.



Note: The default filename of the public key is the key fingerprint.

Please be ready with the exported asc file as you will need this for ONLINE REGISTRATION.

4. Saving AMLC public key

Get a copy of the AMLC public key (amlc.asc) from <u>www.amlc.gov.ph</u> under Reporting Tools then save this to your local drive.

- For 32 bit machine: c:\Program Files\GNU\GnuPG\
- For 64 bit machine: c:\Program Files (x86)\GNU\GnuPG\

5. Importing of AMLC public key

File View Certifi	cates Tools Setting	gs Window Help			deskton dou
	🔄 🤤		<i>i</i>		click Kleopa
Import Certificates E	xport Certificates Redis	play Stop Operation L	ookup Certificates on Serv	er	The Kleopa
Find:			My Certificates	•	main window
My Certificates	Trusted Certificates	<u>O</u> ther Certificates			be displayed
Name	E-Mail Valid	From Valid Until	Details	Key-ID	the screen.
Juan C jua	n.delacru 2012-02	-08	OpenPGP E	C5CC263	
					Click Import
					Certificates.
•		III		•	



Select the directory where you have saved the**AMLC.asc**, then click **Open.**



The Certificate Import Result window will be displayed on the screen. Click Ok.

The introducted	Kleopatra File View Certificates	Tools Settings \	Vindow Help		
oublic key will	Import Certificates Export Ce	ertificates Redisplay	Stop Operation Loc	okup Certificates on Server	
(leopatra –	Find:			AN ertificates	
mported	My Certificates Tru	sted Certificates	Other Certificates	Imported Certificates	6
Certificates tab.	Name E-Ma	ail Valid From	Valid Until	Details	Key-ID
	Anti-Mone amlc@bs	p.go 2010-01-12		OpenPGP 11	.7B9F65
	•		III		4

Certifying AMLC Key 6.

le view Certificates loois	Settings vvir	ndow Help			
🔤 🚉	C	8	<i>i</i> i i i i i i i i i i i i i i i i i i		
Import Certificates Export Certificates	Redisplay Sto	op Operation Lo	okup Certificates on S	erver	
ind:			All Certifica	tes	•
My Certificates T <u>r</u> usted Ce	rtificates <u>O</u> th	ner Certificates	Imported Certifi	cates	
Name E-Mail	Valid From	Valid Until	Details	Key-ID	
Anti-Mone amlc@bsp.go 1	2010-01-12		OpenPGP	117B9F65	
		1			Þ

your op, double (leopatra.

Kleopatra window, Anti-Money dering cil's public







7. Backup Procedure

Make sure to do this procedure to ensure that you will not perform all the steps enumerated above in the event that your public key has been corrupted.

ile	View Certificates Tools	Settings W	/indow Help				Open	
Imp	oort Certificates Export Certificate	s Redisplay S	Stop Operation Lool	kup Certificates on	Server		Kleopat	ra.
<u>i</u> nd:	:			My Certific	ates	-		
3	My Certificates Trusted C	ertificates <u>O</u>	ther Certificates				From M	у
_	Name E-Mail	Valid From	Valid Until	Details	Ke	y-ID	Certifica	ates
J	luan C juan.delacru	2012-02-08		OpenPGP	BC5CC2	63	tab, clic	k the
						•		
	leopatra				_		×	
K File	leopatra) View Certificates Tools Set	tings Window H	m Help				×	
File	leopatra 2) View Certificates Tools Set New Certificate	tings Window F Ctrl+N	rii Help				X	From the
) K File	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server	tings Window H Ctrl+N Ctrl+Shift+I	Help n Lookup Certificates o	n Server			x	From the menu bar
N K	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates	tings Window F Ctrl+N Ctrl+Shift+I Ctrl+Shift+I	Help	n Server	My C	Lertificates	×	From the menu bar click File
Tile	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates	tings Window H Ctrl+N Ctrl+Shift+I Ctrl+I Ctrl+E	Help n Lookup Certificates o cates Valid From	n Server Valid Until	My C	Lertificates Key-ID	×	From the menu bar click File then selec Export
■ K File	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates Export Secret Keys Export Certificates to Server	tings Window F Ctrl+N Ctrl+Shift+I Ctrl+E Ctrl+E Ctrl+E	Help Lookup Certificates o Cates Valid From g 2010-01-12	n Server Valid Until	Details DepenPGP	Certificates Key-ID 117B9F65	×	From the menu bar click File then selec Export Certificat
N K File	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates Export Secret Keys Export Certificates to Server Decryot/Verify Files	tings Window H Ctrl+N Ctrl+Shift+I Ctrl+I Ctrl+E Ctrl+E Ctrl+Shift+E	Help Lookup Certificates o cates Valid From g 2010-01-12 2004-10-11	n Server Valid Until C C	Details DpenPGP DpenPGP	Lertificates Key-ID 117B9F65 4D0BDEE5	×	From the menu bar click File then selec Export Certificate
N K File	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates Export Secret Keys Export Certificates to Server Decrypt/Verify Files Sign/Encrypt Files	tings Window F Ctrl+N Ctrl+Shift+I Ctrl+Shift+I Ctrl+E Ctrl+Shift+E	Help Lookup Certificates o Cates Valid From g 2010-01-12 2004-10-11	n Server Valid Until C C	Details DepenPGP DepenPGP	Certificates Key-ID 117B9F65 4D0BDEE5		From the menu bar click File then selec Export Certificat
File	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates Export Secret Keys Export Certificates to Server Decrypt/Verify Files Sign/Encrypt Files Create Checksum Files Varie Checksum Files	tings Window F Ctrl+N Ctrl+Shift+I Ctrl+I Ctrl+E Ctrl+E Ctrl+Shift+E	Help Lookup Certificates o Cates Valid From g 2010-01-12 Lookup Certificates o	n Server Valid Until C C	Details DeenPGP DeenPGP	Certificates Key-ID 117B9F65 4D0BDEE5		From the menu bar click File then selec Export Certificate
Tile	leopatra View Certificates Tools Set New Certificate Lookup Certificates on Server Import Certificates Export Certificates Export Secret Keys Export Certificates to Server Decrypt/Verify Files Sign/Encrypt Files Create Checksum Files Verify Checksum Files	tings Window H Ctrl+N Ctrl+Shift+I Ctrl+I Ctrl+E Ctrl+Shift+E	Help Lookup Certificates o Cates Valid From g 2010-01-12 1 2004-10-11	n Server Valid Until C C	Details DenPGP DenPGP	Certificates Certificates Key-ID 117B9F65 4D0BDEE5		From the menu bar click File then selec Export Certificate

rganize 🔻 New folder		•== • 🔞
Documents ^ Name	Date modified	Туре
J Music		
E Pictures	No items match your search.	
Computer Local Disk (C;) RLYN (G:) Drive H (\\nasug IMAGAPPS (\\na		
Cls (\\legaspi\CS + 4		,
File name: back up publickey.asc		
Save as type: OpenDGD Certificates (* asc 3	* ana * nan)	-
Save as type: open of certificates (lase	יאנאי נאני	· ·

Select the directory where you want to save the backup of your public key (USB), by default filename is your fingerprint. (You have the option to change the filename) Click Save.

On My Certificates tab, click the name of the key owner (Compliance Officer).

	Ê	C	8		<i>8</i> %		
Import Certificates	Export Certificates	Redisplay	Stop Operation	Lookup	Certificates on S	Server	
Find:					My Certifica	ates	-
My Certifica	tes T <u>r</u> usted Ce	ertificates	Other Certificat	es			×
Name	E-Mail	Valid Fro	om Valid Ur	ntil	Details	Key-ID	
Juan C	juan.delacru	2012-02-08		0	penPGP	BC5CC263	

💼 K	leopatra							x		
File	View Certificates Tools Set	tings Window I	Help							
s:	New Certificate	Ctrl+N		<i>8</i> %						
*	Lookup Certificates on Server	Ctrl+Shift+I	n Lo	okup Certificates o	n Server					
	Import Certificates	Ctrl+I		-			My Certificates	•		
	Export Certificates	Ctrl+E	cates							
	Export Secret Keys			Valid From	Valid Until	Deta	ils Key-ID		From	tha
	Export Certificates to Server	Ctrl+Shift+E	g 2	010-01-12		OpenPG	P 117B9F65		FIOIII	line
	Decrypt/Verify Files Sign/Encrypt Files	•	1 2	004-10-11		OpenPG	P 4DUBUES		click then s	File
	Create Checksum Files Verify Checksum Files								Export Secret	Keys.
8	Close	Ctrl+W	L							-
×	Quit	Ctrl+Q								

Export Secret Certificate	2 ×	
Please select export options for <pre></pre>	JUAN DELA CRUZ	Sel dir wh
Output file:		wa sav bao
<u>A</u> SCII armor		you key clic dis
(<u>O</u> K <u>C</u> ancel	ico

Select the
directory
where you
want to
save the
backup of
your private
key (USB) by
clicking the
diskette



7. Recovery Procedure

This is done if the public key is compromised, only if the Casinos have performed the backup procedure for their private and public keys.

- 110	New Certificate	Ctrl+N		AA					_	pro
<u>eq</u>				Lookup Certificates o	n Server					inst
%	Lookup Certificates on Server	Ctrl+Shift+I	H				Trusted	Certificates		CD
- 49	Import Certificates	Ctrl+I	hat					ooranoatoo		GP
à	Export Certificates	Ctrl+E	cate						<u> </u>	
i g	Export Secret Keys		om	Valid Until	Details	Key	/-ID		_	
3	Export Certificates to Server	Ctrl+Shift+E								On
8	Decrypt/Verify Files		1							Op
	Sign/Encrypt Files		Ŀ							the
	Create Checksum Files		L							the
	Verify Checksum Files									Imr
8	Close	Ctrl+W								Cer
×	Quit	Ctrl+Q								
~	400	our a								
_									_	

the ure in ng the ftware.

stalled, leopatra ck File elect ate.

	Computer > RLYN (G:)	✓ ✓ Search RLYN (G:)	۶
t the	Organize 🔻 New folder	i= • 🔳	?
tory	Recent Places Name	Date modified Type	
re the	back_up_publickey.asc	11/27/2013 9:54 AM ASC File	
up of public .asc) is d then Open.	Image: Documents Documents Image: Discures Discures Image: Discure	11/27/2013 10:34 GPG File	
	File name: back_up_publickey.asc	← Certificates (*.asc *.cer *.cert *. <u></u> <u></u> <u></u> 	. •

	Certificate
Detailed results of importing K:/back_up_certificate.asc:	Import
Total number processed: 1	Result
Imported: 1	window w
	appear the
	click Ok

👩 Kleopatra File **File** Window Help Rew Certificate... Ctrl+N *6*% Lookup Certificates on Server Kookup Certificates on Server... Ctrl+Shift+I 🗔 Import Certificates... 🗲 Trusted Certificates • Ctrl+l cates × Export Certificates... Ctrl+E Key-ID Valid Until Details om Export Secret Keys... Export Certificates to Server... Ctrl+Shift+E Decrypt/Verify Files... Bign/Encrypt Files... Create Checksum Files... Verify Checksum Files... Close Ctrl+W 🔀 Quit Ctrl+Q

To import your secret key, click file then select Import Certificate.

_ 🗆 🗙

ganize 🔻 New f	older	:==	• 🔟 🔞
🗼 Downloads	^ Name	Date modified	Туре
📃 Recent Places	back_up_publickey.asc	11/27/2013 9:54 AM	ASC File
Liburation	back_up_secret_key.gpg	11/27/2013 10:34	GPG File
Pictures Videos Computer Local Disk (C:) RUNN (G:)			
Prive H (\\nasug	✓ <iii< p=""></iii<>		
Fil	e name: back_up_secret_key.gpg	✓ Certificates (*.asc *.	cer *.cert *.c ▼

Select the directory where the backup of your private key (.gpg) is saved then click Open.

	Certificate	Import Result - Kleopatra	
Certificate Import Result window will appear then click Ok.	i	Detailed results of importing G:/back_up_secr Total number processed: 1 mported: 0 Secret certificates processed: 1 Secret certificates unchanged: 1	et_key.gpg:

Repeat Procedures 4-6 of the Transaction Security Protocol.

Section 4. **REPORTING PROCEDURES.** –

A. Covered/Suspicious Transaction Report. -



A.1 Data Elements Chart (Format Code 1.0) – CASINOS



A.2 Electronic Record Format (Format 1.0–Casinos)

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS
H-1	Header Record Indicator	Text	1	Н	H - for Header
H-2	Supervising Agency	Number	1	9	5 –PAGCOR , 6-CEZA, 7-APECO
H-3	Institution Code	Number	11/18	9(11) / (18)	AMLC Library
H-4	Report Date	Number	8	9(8)	yyyymmdd ; not greater than current date; not less than 20011017
H-5	Report Type	Text	3	X(3)	CTR,STR
H-6	Format Code	Number	2	99	1
H-7	Submission Type	Text	1	X(1)	A- add, E- edit/correction, D- delete, T-test

HEADER RECORD

DETAIL RECORD Transaction Data

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS
D-1	Detail Record Indicator	Text	1	D	D - for Detail
D-2	Transaction Date and Time	Number	8	9(8)	yyyymmddhhmmss ; not greater than current date; not less than 20011017
D-3	Transaction Code	Text	6	X(6)	AMLC Transaction Codes
D-4	Transaction Reference No.	Text	20	X(20)	must be unique per transaction date
D-5	Transaction Amount (Php)	Number	20	9(18).99	Greater than 0 w/ or w/o decimal value
D-6	Transaction Amount (FX)	Number	17	9(15).99	Optional
D-7	FX Currency Code	Text	3	X(3)	Optional; mandatory if FX amount <> null
D-8	Nature/Purpose of Transaction	Text	200	X(200)	
D-9	Name of Correspondent Bank	Text	90	X(90)	
D-10	Address				
	Address1		50	X(50)	Room No./Office Name, Bldg./House No., Street, Subd./ Brgy.
	Address2		50	X(50)	District, Town, City
	Address3		30	X(30)	Province, Country code, ZIP
D-11	Country Code of Correspondent Bank	Number	3	9(3)	Country Code (Refer to Systems Code, Annex B.3)

Subject Da	ta						
Detail Record–Party details							
Customer							
D-A-1	Party Type Flag	Text	1	Х	A–Customer		
D-A-2	Customer Reference Number	Text	30	X(30)			
D-A-3	Name	Text					
	Last Name		100	X(100)	Last name of customer		
	First Name		100	X(100)	First name of customer		
	Middle Name		50	X(50)	Middle name of customer		
D-A-4	Address	Text					
					Room No./Office Name,		
	Address1		100	X(100)	Bldg./House No., Street,		
					Subd./ Brgy.		
	Address2		100	X(100)	District, Town, City		
	Address3		100	X(100)	Province, Country , ZIP		
D-A-5	Date of Birth	Number	8	9(8)	date < current date and the difference between current date and birthdate must be less than 150		
D-A-6	Place of Birth	Text	90	X(90)	City, Municipality, Country		
D-A-7	Nationality	Text	40	X(40)			
D-A-8	ID Type	Text	4	X(4)	 ID1 - Passport ID2 - Driver's License ID3 - PRC ID ID4 - NBI Clearance ID5 - Police Clearance ID6 - Postal ID ID7 - Voter's ID ID8 - TIN ID9 - Barangay Certification ID10 - GSIS e-Card/UMID ID11 - SSS ID12 - Senior Citizen Card ID13 - Overseas Workers Welfare Administration (OWWA) ID ID15 - Seaman's Book ID16 - Alien/Immigrant Certification of Registration ID17 - Gov't Office/GOCC ID ID18 - Certification from National Council for the Welfare of Disabled Persons(NCWDP) ID19 - Department of Social Welfare and Development (DSWD) Certification 		

					ID20 – Integrated Bar of the
					Philippines (IBP) ID
					ID21–Company ID
					ID22 – Student's ID
					ID23 – National ID
					ID24 - SEC Certificate of
					ID25 – Business Registration
					Certificate
					ID26– Philhealth ID
					ID27 - Others
D-A-9	Identification No.	Text	30	X(30)	
D-A-10	Telephone No.	Text	15	X(15)	
D-A-11	Nature of Business	Text	35	X(35)	
OTHER PA	RTICIPANT				
D-P-1	Party Type Flag	Text	1	Х	P-Other Participant
D-P-2	Customer Reference Number	Text	30	X(30)	
					Y – if Other Participant is a
D-P-3	Name Flag	Text	1	x	corporation
DIS	Name Flag	TCXC	-	~	N – if Other Participant is an
					individual
D-P-4	Name	Text			
	Last Name		100	X(100)	Last name of other participant
	First Name		100	X(100)	First name of other participant
	Middle Name		50	X(50)	Middle name of other
			50	7(50)	participant
D-P-5	Address	Text			
					Room No./Office Name,
	Address1		100	X(100)	Bldg./House No., Street,
					Subd./ Brgy.
	Address2		100	X(100)	District, Town, City
	Address3		100	X(100)	Province, Country , ZIP
SUBJECT O	F SUSPICION				
D-S-1	Party Type Flag	Text	1	Х	S – Subject of Suspicion
D-S-2	Customer Reference Number	Text	30	X(30)	
D-S-3	Name	Text			
	Last Namo		100	V(100)	Last name of subject of
			100	X(100)	suspicion
	First Name		100	X(100)	First name of subject of
			100	A(100)	suspicion
	Middle Name		50		Middle name of subject of
			50	A(30)	suspicion
D-S-4	Address	Text			
					Room No./Office Name,
	Address1		100	X(100)	Bldg./House No., Street,
					Subd./ Brgy.

	Address2		100	X(100)	District, Town, City
	Address3		100	X(100)	Province, Country , ZIP
D-S-5	Date of Birth	Number	8	9(8)	date < current date and the difference between current date and birthdate must be less than 150
D-S-6	Place of Birth	Text	90	X(90)	City, Municipality, Country
D-S-7	Nationality	Text	40	X(40)	
D-S-8	ID Type	Text	4	X(4)	 ID1 – Passport ID2 – Driver's License ID3 – PRC ID ID4 – NBI Clearance ID5 – Police Clearance ID6 – Postal ID ID7 – Voter's ID ID8 – TIN ID9 – Barangay Certification ID10 – GSIS e-Card/UMID ID11 - SSS ID12 – Senior Citizen Card ID13 – Overseas Workers Welfare Administration (OWWA) ID ID14 – OFW ID ID15 – Seaman's Book ID16 – Alien/Immigrant Certification of Registration ID17 – Gov't Office/GOCC ID ID18 – Certification from National Council for the Welfare of Disabled Persons(NCWDP) ID19 – Department of Social Welfare and Development (DSWD) Certification ID20 – Integrated Bar of the Philippines (IBP) ID ID21–Company ID ID22– Student's ID ID23 – National ID ID24 - SEC Certificate of Registration Certificate ID26 – Philhealth ID ID27 – Others
D-S-9	Identification No.	Text	30	X(30)	
D-S-10	Telephone No.	Text	15	X(15)	
D-S-11	Nature of Business	Text	35	X(35)	

Details of Suspicion

D-D-1	Reason	Memo	800	Reason for Suspicion SI1- There is no underlying legal or trade obligation, purpose or economic justification. SI2- The client is not properly identified.
-------	--------	------	-----	---

		SI3-	The amount involved is not
			commensurate with the
			business or financial capacity
			of the client.
		SI4-	The transaction is structured
			to avoid being reported
		CIE	There is a deviation from the
		313-	liest a deviation nom the
			client's profile/past
			transactions.
		SI6-	The transaction is similar,
			analogous or identical to any
			of the foregoing. (Additional
			reason is required after a
			semicolon i.e. SI6: The client
			is)
		DC1	Kidnanning for ransom
		PC1-	
		PC2-	offenses
		PC3-	Graft and corrupt practices
		PC4-	Plunder
		PC5-	Robbery and Extortion
		PC6-	lueteng and Masiao
			Diracy on the high coos
		PC7-	
		PC8-	Qualified Inett
		PC9-	Swindling
		PC10	- Smuggling
		PC11	Violations under the Electronic Commerce Act of 2000
		PC12	Hijacking: destructive arson:
			and murder including those
			nernetrated by terrorists
			perpetrated by terrorists
			against non-compatant
			persons and similar targets
		PC13	– Terrorism and conspiracy to
			commit terrorism
		PC14	 Financing of Terrorism
		PC15	– Bribery
		PC16	 Frauds and Illegal Exactions
			and Transactions
		PC17	 Malversation of Public Funds
			and Property
		PC18	 Forgeries and Counterfeiting
		PC19	 Violations of Sections 4 to 6
			of the Anti-Trafficking in
			Persons Act of 2003
		PC20	- Violations of Sections 78 to
			79 of the Revised Forestry
			Code of the Phile as
			coue of the Fills, as
		D C C	amended
		PC21	– violations of Sections 86 to
			106 of the Fisheries Code of
			1998

				1	
					PC22 – Violations of Sections 101 to
					107 and 110 of the Philippine
					Mining Act of 1995
					PC23 – Violations of Section 27 (c),
					(e), (f), (g) and (i) of the
					Wildlife Resources
					Conservation and Protection
					Act
					PC24 – Violation of Section 7h of the
					National Cavos and Cavo
					Descurrees Management
					Resources Management
					Protection Act
					PC25 – Violation of the Anti-
					Carnapping Act of 2002
					PC26 – Violations of Sections 1,3 and
					5 of the Decree Codifying the
					Laws on Illegal/Unlawful
					Possession Manufacture
					Dealing in, Acquisition or
					Disposition of Firearms,
					Ammunition or Explosives
					PC27 – Violation of Anti-Fencing Law
					PC28 – Violation of Section 6 of the
					Migrant Workers and
					Overseas Filipinos Act of
					1995
					PC29- Violation of Intellectual
					Property Code
					PC30 – Violation of Section 4 of the
					Anti-Photo and Video
					Voveurism Act of 2009
					PC31 – Violation of Section 4 of the
					Anti Child Dornography Act of
					2009
					PC52 - VIOIATIONS OF K.A. NO. 7610,
					Special Protection of Children
					Against Abuse, Exploitation
					and Discrimination
					PC33- Fraudulent practices and other
					violations under the
					Securities Regulation Code of
					2000
					PC34- Felonies or offenses of a
					similar nature that are
					punishable under the penal
					laws of other countries.
					Narrative of events leading to
D-D-2	Narrative	Memo	4000		Suchician
					Suspicion

Trailer Record

FIELD					
NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS
T-1	Trailer Record Indicator	Text	1	Т	T - for Trailer
T-2	Php Amount Total	Number	20	9(18).99	Total Transaction Amount

	Records Total of batch to be				
T-3	sent	Number	10	9(10)	Total number of CTR/STRs

B. Transaction Security Process and Transferring of Files. -



B.1 Encrypting of Files (done after CP has created a CSV file – Format1.0)



- From your desktop, double click
 Kleopatra. The Kleopatra main window will be displayed on the screen.
- Click File, then click Sign/Encrypt Files...

Select the csv file you want to sign and encrypt, then click **Open.**

Sample e	SV 🖡 SIR	▼ + Search SIR	ې
Organize 👻 🛛 New folde	r		H • 🚺 🔞
📃 Recent Places 🔺	Name	Date modified	Туре
No. 11	1234562007042601.csv	7/7/2010 8:15 AM	CSV File
Computer Local Disk (C:) New Volume (D:) drive h (\\192.168 MAGAPPS (\\na CIs (\\legaspi\CS	٢	11	



	For whom do you want to encrypt? Please select for whom you want the files to be Find:	encrypted. Do not forget to pick one	of your own certificates.
	Name	E-Mai	Valid From Valid U
alaat Anti	Juan C. Dela Cruz (ABC Bank)	juan.delacruz@	yahoo.com 2012-02-08
elect Anti-	Anti-Money Laundering Council (AMLC Inst	tutional Key Pair) amlc@bsp.gov.ph	2010-01-12
by, then click	Name E-Mail Valid From	n Valid Until Details	Fingerprint Key-ID

ind:		All Certi	ificates		lick Novt
	Name	E-Mail	Valid From	Valid U	
Juan Anti-M	C. Dela Cruz (ABC Bank) oney Laundering Council (AMLC Institutional Key Pair)	juan.delacruz@yahoo.co amlc@bsp.gov.ph	o m 2012-02-08 2010-01-12	m be	essage v e display n the scr
	III Add A	emove		, Cl	lick Cont
	Name	E-Mail Valid F	rom Valid Until	Detai	
Anti-M	oney Laundering Council (AMLC Institutional Key Pair)	amlc@bsp.gov.ph 2010-01	-12	OpenP	



Please enter the passphrase to unlock the secret key for "Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.co 2048-bit DSA key, ID BC5CC263, created 2012-02-08.</juan.delacruz@yahoo.co 	the OpenPGP certificate: om>"	Enter passphrase of the Compliance Officer, then click Ok .
	K <u>C</u> ancel	

	Sign/Encrypt Files	
	Results	
	Status and progress of the crypto operations is shown here.	
	OpenPGP: All operations completed.	
	1234562007042601.csv → 1234562007042601.csv.gpg: Signing and encryption succeeded.	
Click Finish.		
	✓ Keep open after operation completed	
	<u>Einish</u> <u>Cancel</u>	

B.2 Transferring of Files (File Transfer Reporting Facility version 2.0)

B.2.1 Log-in Page

Log-on to https://portal.amlc.gov.ph

(- 四 × 价 ☆ ^磁 🥲
Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit	Entrus - Vertra
Description Descriptin Descriptin Descriptin Descriptin Descriptin	User Login Institution Code: Username/Email: Password: LOCIN EORCOT PASSWORD Note: CPs with 11-digit Inst. Code - 1at 6 digits CPs with 11-digit Inst. Code - 1at 9 digits REGISTER Registration Status? OLICK HERE!

Enter the 1 st 6-digits of the Inst. Code for CPs	User Login		
with 11-digit Inst. Code			
	Institution Code:		
	Username/Email:		
Enter the 1st 9-digits of the Inst. Code for	Password:		
CPs with 18-digit Inst. Code	LOGIN		
	FORGOT PASSWORD		
Enter the Username or Registered email			
address	Note: CPs with 11-digit Inst. Code - 1st 6 digits		
	REGISTER		
	Registration Status? CLICK HERE!		
MAIN	PAGE		
(Producti	on Mode)		
Welcome GUEST ACC	COUNT (ABC BANK)!		
	2		
	X		
Advi	sory		
(5)	Sa Successful		
<u> </u>	login will		
CTR/STR File Upload CTR/STR File	e Upload History Logout show the		
Electronic Docume	ents Upload Facility CP User		
	Main Page		
KYC Docs Upload Electronic Re	turns Upload Electronic Returns Template		
Upload the Elect Docs first faci	ronic SIR & KYC ore using this lity.		
and the second s			

There are nine (9) options or links available in CP User Main Page:

a. **Advisory**, if the icon is clicked, it will automatically display latest advisory/announcement of AMLC.

b. CTR/STR File Upload provides access for the registered CP user to upload the electronic CTRs and STRs.

۲

c.

d.

e.

f.

g.

h.

i.

CTR/STR File Upload History gives the option for the registered CP user to inquire and view the files uploaded; only files uploaded by the particular CP can be viewed.



Logout will log the CP user out of the system and go back to CP User Login Page.



KYC Docs Upload provides access for the registered CP user to upload KYC Documents for STRs.



Electronic Returns Upload provides access for the registered CP user to upload E-Returns for Freeze Orders



Electronic Returns Template provides a template facility (excel file) for Electronic Returns.



STR Attachment Upload gives the option for the registered CP user to upload a STR attachment, provided that the STR has been uploaded and processed



STR Attachment History gives the option for the registered CP user to check the status of the STR attachment that has been uploaded.

B.2.2 CTR/STR File Upload

When the registered CP's Institution Code, user name and its corresponding password are entered correctly, the CP user should be able to use the FTRF to upload the electronic reports.



CTR/STR FILE UPLOAD	
Instructions: Click browse to select the encrypted CTR/STR file to be uploaded and click the upload button to upload the selected file.	Click Browse button to locate
CTR/STR File Upload CI Code: Thru: Diskette T File: Choose File No file chosen Upload Back to Menu	the file to be uploaded.

Note: Only files with [.csv.gpg] or [.csv.enc] or [.csv.pgp] as extension at the end of the filename will be accepted for uploading through the FTRF. The filename should follow the file naming convention 123456yyyymmddss of 123456789yyymmdd where:

123456/123456789	 1st six digits/1st 9 digits of the institution code
yyyymmdd	 report date (date the report is sent to AMLC)
SS	 Sequence number (from 01-99) representing no. of files
	transmitted for the day

After locating the file, click UPLOAD to upload the selected file or click BACK TO MENU to cancel the upload and return to the User Main Page.

After the Upload button is clicked and upon every successful upload, the "Upload Confirmation Receipt" is displayed.

The Upload Confirmation Receipt has the following information:

- Confirmation Receipt: Date and time of receipt + Username + FileName •
- File Name: Name of the file that was uploaded •
- File Size: size of the file that was uploaded
- Date and Time: Uploaded by: Receipt date and time of the file at AMLC Secretariat
- Name of the CP user who uploaded the file • Uploaded by:

Confirmation Receipt	2010-10-26-131454-PNBADC-0003302010102601.csv.gpg	
File Name	0003302010102601.csv.gpg	
File Size	1486	
Date and Time	Oct 26, 2010 1:14:54 PM	
Uploaded By	ANGELICA DELA CRUZ	
		× 1
e	🔒 🧐 Local intra	net
• If there are still file for	uploading, click	net
e If there are still file for If there are no more fil	uploading, click	net "

Note: The Upload Confirmation Receipt does not guarantee that all CTRs/STRs in the CSV file/s have been uploaded. To check the status of the submission, files should be viewed in the File Upload History Page.

B.2.3 File Upload History

A registered CP User can search/view anytime the files that have been uploaded for the registered CP he is representing. Status of each file uploaded is indicated in the search result.



		CTR/STR FILE UPLO	AD HISTORY
	Query Criteria: From date: (mm-dd-yyyy) Clear	date: 09-11-2017 E Search (mm-dd-yyyy) oday	To view specific past date or date
	Calendar - Go — — X about:blank ugust ▼ 2017 ▼ ≤ [≤] [Print] [≥] un Mon Tue Wed 1 2 3 4 2 8 9 10 11	Page size: Page size: Page size: No uploaded On Uploaded by Remarks Submission Type Tran. Count Good Trans. Bad Trans. Uploaded Via Validati No uploaded reports on these dates. Save Report to File Print Request for Validati	(calendar icon) to specify START DATE and END DATE.
122	3 14 15 16 17 18 19 0 21 22 23 24 25 26 Z 28 29 30 31 1 2		• Click > SEARCH to start the search.

• When the search is completed, the query result is displayed.

Page 64 of 96

Query Cri Promidate:	(mm dd yyyy) (taar Taa	ute: (15-15-2014 (mm:dd-yyyy) fay	ст	R/S	TR FILE U	IPLOAD H	ISTORY					
Total (1) - He	drash											nga sipai 10 V (iji
Select	Confirmation Receipt	File Name	File Type	File Size	Uploaded On	Uploaded by	Remarks	Tran. Count	Good Trans.	Bad Trans.	Uploaded Via	Validation Message
	2014-11-11-123456-8P5GKT- 00005502014111168-CTV-geg	0000502014102768.CEV.gag	CIEV	1553	2014-11-11 12-34-96-0	BPSORY	06F1 33K3P1 98C1 00UP1 00F1 0CF	1		1	PORTAL V2.0	
Page 1 of 1 Annualis Lapped (7 - 5 Done Ave Star - 5 Done Ave Star - 5 Done Ave Dol - 5 Done Ave (7 - 5 Connection (7 - 5 Connection C - 5 Connection	n den skipped des te error in Header date de Distriktion, Turmaction, Cormany, Ci te Header in Falsed latt. Natur	unity code and etc.)							Term Repo	enarria (r	the Report to	Valdelina Wanager

Check the result of the file uploaded by comparing the number of transaction count with the number of good transactions.

- a. If the transaction count is equal to the number of good transactions, the CP can save a copy of the confirmation receipt by clicking on the "SAVE REPORT TO FILE" button, or the "PRINT" button to have a printed copy for filing.
- b. If the transaction count is not equal to the number of good transactions, the CP should select the report file with Bad Transactions and click on the "Download Validation Message" button. The validation message of the selected uploaded file will be sent via email. Check the validation message for the details of the error/s and make the appropriate correction.

To search another date or date range, click> **CLEAR** button before entering the new search dates.

B.2.4 How to Log-out

	Advisory		
S.	9		
CTR/STR File Upload	CTR/STR File Upload Histor	z Logout	
Electron	ic Documents Upload	l Facility	
- A		×I	
KYC Docs Upload	Electronic Returns Upload	Electronic Returns Template	
Uploa Do	d the Electronic STR cs first before using t facility.	& KYC this	
STR Attach	ment Upload STR Attachm	nent History	

From the User Main Page, click Logout link



- If CP User closes the browser, a notification message below will be displayed on the screen.
- Click Ok to logout or click Cancel to stay on the current page.

Nicroso	ft Internet Explorer 🛛 🕹
	Are you sure you want to navigate away from this page?
-	You will be logged out from the AMLC Portal!
	Press OK to continue, or Cancel to stay on the current page.
	OK Cancel

B.3 Uploading of KYC Documents for Suspicious Transaction Reports

B.3.1 Mandatory Uploading of KYC Documents

Uploading of KYC Documents is mandatory if the Reason of Suspicion falls under any of the following:

PC1	-	Kidnapping for Ransom
PC2	-	Drug Trafficking
PC12	-	Hijacking; destructive arson; and murder, including those perpetrated by terrorists against non-combatant persons and similar targets
PC13	_	Terrorism and conspiracy to commit terrorism
PC14	-	Financing of Terrorism

Uploading of KYC documents should be performed prior to the upload of the STR, otherwise the STR will be rejected for processing due to non-submission of KYC documents.

The customer reference number (CRN) will be mandatory for the Account Holder Party or Subject of Suspicion Party, whichever is applicable for the above mentioned predicate crimes.

Uploading of KYC Documents for a CRN of a subject STR will only be done once, if a subsequent STR is filed on the same CRN, CPs need not re-upload the corresponding KYC Documents.

Mandatory update of submitted KYC Documents is required every three (3) years, however this is optional if no STR will be filed under the same CRN. In cases where the CP has no updated KYC documents, reason for which should be indicated in the **Remarks** portion of the KYC Docs Update window.

Below is the Acceptable KYC Documents:

Account Opening Forms are the following:

- Signature Cards
- Customer Information File/Sheet

Scanned copy of the following for ID Documents presented:

- Government IDs
- Articles of Incorporation/General Information Sheet for Corporation/Articles of Partnership
- Authorized Signatory's ID for Corporate accounts
- DTI Certificate for Sole Proprietor
- Digital Photo, if available

Procedures for Uploading of KYC Documents

Log-on to https://portal.amlc.gov.ph

Anti Money Laundering Cour × +				- 0
D 🚱 https://portal.amlc.gov.ph/amlc/	🛱 🦉 🔍 Sea	urch	☆自♣	r
Republic of the Philippines Anti-Money Laundering Count The Philippines' Financial Intelligence Unit	cil t			
Welcome to the Anti-Money Laundering (Council Portal! (Ver. 2.8.4)	User Login		
*Online Registration - Allows Compliance Officers to register and attach supporting documents. Submission of ba	ardropy documents are no longer required.	Username/Email:		
"Upload CTR/STR Files - Encrypted Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (S Facility.	iTRs) may be conveniently transmitted to the AMLC via this	Password:	LOGIN DT PASSWORD	
*View History of Uploaded CTR/STR Files - Access history of uploaded CTR/STR files. Errors are logged, allowing users to identify an to download the validation messages.	id make the necessary corrections. Users also have the option	Note: CPs with 11-di CPs with 18-di	git Inst. Code - 1st 6 digits igit Inst. Code - 1st 9 digits EGISTER	_
*View News Advisories - New and archived AMLC advisories may be accessed from this facility.		Registration S	Status? CLICK HERE!	
*Upload Attachments to STRs - Oigital attachments to Suspicious Transaction Reports (STRs) may be submitted through uploading of attachments.	this facility. The STR should have been uploaded first prior to			
*View History of Uploaded Attachments to STRs - Access history and status of uploaded STR attachments.				
			AMLC © 2010 . A	ll rights re
	User Login			
	Institution Code:			
	Username/Email:			

Institution Code:	
Username/Email:	
Password:	
	OGIN
FORGO	T PASSWORD
Note: CPs with 11-di CPs with 18-di	git Inst. Code - 1st 6 digits git Inst. Code - 1st 9 digits
Registration S	tatus? <u>CLICK HERE!</u>

A successful log-in will show the Covered Person go to the Upload window.

Advisory
CTR/STR File Upload History Logout
Electronic Documents Upload Facility
KYC Docs Upload Electronic Returns Upload Electronic Returns Template Upload the Electronic STR & KYC Docs first before using this
STR Attachment Upload STR Attachment History

In the initial KYC Docs Upload window, three options will be available: Choose Add/New STR (No STRs filed), if the KYC Docs to be uploaded corresponds to an STR not previously uploaded; Add/New STR (Existing STRs), if the KYC Docs to be uploaded is for previously uploaded STRs with no KYC docs on file; and Update, for updating previously filed KYC Docs.

Ittp://localhost:000/amic/web/uploadKycDoc	s.htm	- 日 × 分 ☆ 遼 🧐
Republic of the Philippines Anti-Money Lo The Philippines' Fina	nundering Council	Entrust
-	KYC DOCUMENTS UPLOAD FACILITY	
c	Instructions:	
	KYC Documents Henu Add/New (No STRs filed) Add/New (Existing STRs) Update	
Go to Main Page		

Click Add/New (No STRs filed) button to enable the KYC Docs Upload Facility.

Instructions:		
Click Add/New for first	t time uploading of KYC documents or Click Update to modify previously uploaded KYC do	cuments.
	KYC Documents Henu	
	Add/New (No STRs filed)	
	Add/New (Existing STRs)	
	Hadata	

Enter the Customer Reference Number and attach the corresponding KYC Documents, attach the KYC documents then Click the Save Button.

Instructions:				
Click BROWSE butto	n to select the documents to be uploaded and	click the UPLOAD button to	submit the selected files.	
	Upload KYC Documents (No STRs filed)	-		*Enter the Account Holder's Customer Poference Number (CPN)
	Customer Reference Number: *		Paura	Attach scanned copies of t Account Opening Forms
	ID's Presented: * Digital Picture/Photo:		Browse	Attach scanned copies of of IDs presented by the Account Holder
	Save	Back to Menu		Attach a digital photo of

*All fields with asterisk are mandatory

*Customer Reference Number (CRN) is a unique number assigned to a customer of a CP; please make sure that the CRN indicated in the KYC Docs upload window will be the same CRN inputted in the STR where the KYC Docs will be attached.

*After the Save button is clicked and upon every successful upload, the "KYC Upload Confirmation Receipt" is displayed.

	KYC UPLOAD Confirmation Receipt
Confirmation Receipt	2017-10-02-143654-39272
Digital Picture/Photo	aspen.jpg
Account Opening Forms	Holidays2010.pdf
ID's Presented	Holidays2011.pdf
Date and Time	Oct 2, 2017 2:36:54 PM
Uploaded By	GUEST USER

Click Add/New (Existing STRs) to enable Upload KYC Documents (Existing STRs).

Instruction	51		
Click Add/New fo	first time uploading of KYC	documents or Click Update to modify previously uploaded KYC docum	nents.
	KYC Documents Her	14.	
		Add/New (No STRs filed)	
		Add/New (Existing STRs)	
		Undate	- 1

Fill up the mandatory fields and attach KYC documents, then click the Upload button.

	KYC DOCUMENT	S UPLOAD FAC	ILITY		
nstructions:					
up the form below ected files. TE: It is assumed	and click the BROWSE button to select the d that you have already uploaded the Ele	documents to be uploaded and clie	ck the UPLOAD butto ed that it was proc	n to su essed	bmit the successfully.
	Upload KYC Documents (Existing STRs))			
	Institution Code: * Transaction Date: *	(11-digits or 18 (YYYYMMDD)	8-digits)		Enter the Institution Code, Transaction Date and Transaction Reference number of the STR where
	Reference Number: *				the KYC Docs will be attached
	Description:		 →[Cu	stomer Reference Number, if avail
	Account Opening Forms: *		Browse	Att	ach scanned copies of the Acco Opening Forms
	ID's Presented: * Digital Picture/Photo:		Browse	Att	ach scanned copies of IDs pres by the Account Holder
	Upload (OL	D) Back to Menu		٨	ttach a digital photo of the

*All fields with asterisk are mandatory

* After the Upload button is clicked and upon every successful upload, the "KYC Upload Confirmation Receipt" is displayed.

KYC UPLOAD Confirmation Receipt

Confirmation Receipt	2017-10-02-143654-39272
Digital Picture/Photo	aspen.jpg
Account Opening Forms	Holidays2010.pdf
ID's Presented	Holidays2011.pdf
Date and Time	Oct 2, 2017 2:36:54 PM
Uploaded By	GUEST USER

ad History

Click **Update** to update a previously uploaded KYC Documents.

Instruction	ns:	
Click Add/New	for first time uploading of KYC documents or Click Update to modify previously uploaded KYC documents.	
	KYC Documents Henu	
	Add/New (No STRs filed)	
	Add/New (Existing STRs)	
	Update	

To update type in the CRN with a previously filed KYC Documents, then click the Find button.

KYC DOCUMENTS UPLOAD FACILITY

indicate the O	stomer reference number to be updated.	
	Upload KYC Documents (No STRs filed)	Enter the CRN
	Customer Reference Number: *	to be updated, and Click Find
	Find Back to Menu	
KYC Docs Update window will appear

,	(YC DOCUMEN	TS UPLOAD FAC	ILITY	
Instructions:				
Click the Upload New button to u remarks field and Click the Updat	pload new documents under th te button to save the reason.	e same Customer Reference Numbe	r otherwise enter the reas	on on the
KYC Doct	iment Update			
	Customer Reference Number:	ABCDEF		
	Last Update:	12-13-2017		If there is no KYC Docs
	Kemarks			to upload, please type
	Update	Upload New Back to Menu		Remarks portion, then
		-		Click Update
	If there are KYC Upload New. Thi KYC Docs	Docs to upload, Click s will direct you to the Upload Window		

After the Update/Upload button is clicked and upon every successful update, the "KYC Update Confirmation Receipt" is displayed.

	KYC UPDATE Confirmation Receipt
Confirmation Receipt	2017-10-02-144118-39272
Last Update	2017-09-29
Remarks	Account Closed
Date and Time	Oct 2, 2017 2:41:16 PM
Uploaded By	GUEST USER

B.4 STR Attachment Upload

Please note, that a successfully processed and uploaded STR is required before a Covered Person can upload an STR attachment.

Enter the 1st 6-digits of the Inst. Code for CPs with 11-digit Inst. Code

Enter the 1st 9-digits of the Inst. Code for CPs with 18-digit Inst. Code

Enter the Username or Registered email address

stitution Code:	
sername/Email:	
assword:	
	LOGIN
E	ORGOT PASSWORD
Note: CPs with CPs with	11-digit Inst. Code - 1st 6 digits 18-digit Inst. Code - 1st 9 digits
	REGISTER
Registra	tion Status? CLICK HERE!



Enter the 11 or 18 - digit Inst. Code of the uploaded STR (Please note that the Inst. Code should be the same as the uploaded STR up to the branch level)

Enter the Transaction Date and Transaction Reference No. of the STR where the file will be attached.

Enter a brief description of the file to be attached.

Locate the file to be attached, then Click the Upload Button.

STR ATTACHMENT UPLOAD

Instructions:

Fill-up the form below and click browse to select the attachment to be uploaded and click the upload button to upload the selected file. NOTE:It is assumed that you have already uploaded the Electronic STR and have confirmed that it was processed successfully.

STR Attachment Upload	
Institution Code:	(11-digits or 18-digits)
Transaction Date:	(YYYYMMDD)
Reference Number:	
Description:	
File:	Choose File No file chosen
	Upload Back to Menu



Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit

STR ATTACHMENT UPLOAD Confirmation Receipt

Confirmation Receipt	2017-08-31-153634-BPIGRY-00005000000-20170605-FF000ICHJACOB001
Institution Code	00005000000
Transaction Date	20170605
Reference Number	FF000ICHJACOB001
Description	STR Attachment
File Name	ECTRSTRSQL.TXT
File Size	2173
Date and Time	Aug 31, 2017 3:36:34 PM
Uploaded By	GRACE DELOS REYES-YABUT

This confirms that the file has been received by the Anti-Money Laundering Council and will be queued for processing. Please check the results of processing in the <u>STR Attachment Upload History</u>.

Go to STR Attachment Upload History



Back to STR Attachment Upload Page

After the Upload button is clicked and upon every successful upload, the "STR Attachment Upload Confirmation Receipt" is displayed.

B.5 STR Attachment History

A registered CP User can search/view anytime the STR attachment/s uploaded for the registered CP he is representing. Status of each attachment is indicated in the search result.



- To view specific past date or date range, click (calendar icon) to specify START DATE and END DATE.
- Click >**SEARCH** to start the search.
- When the search is completed, the query result is displayed.

Republic of the Philippines Anti-Money Laur The Philippines' Financi	ndering al Intellige	Council ence Unit						
Query Criteria: 08-31-2017 From date: (mm-dd-yyyy) Clear To date: Today	STR AT	FACHMENT	UPLOAD H	ISTORY				
Total (1) - [refresh]	CI Code	Transaction Date	Reference Number	File Name	File	Unloaded On	Page Uploaded	Processed
2017-08-31-153634-BPIGRY-00005000000-20170605- FF000ICHJACOB001	00005000000	2017-06-05 00:00:00.0	FF000ICHJACOB001	ECTRSTRSQL.TXT	Size 2173	2017-08-31 15:36:34.0	BPIGRY	Not yet processed
FF0001CHJACOB001 Page 1 of 1	000000000000000000000000000000000000000	00:00:00.0	Providence	CINGINGQUIXI	21/3	15:36:34.0	DFIGRT	processed

Check the result of the STR Attachment, Status should show "Processed" otherwise, re-upload the attachment.

B.6 Uploading of Electronic Returns (E-Return) for Freeze Order

Rule 10, E.4 paragraph 2 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as amended states that:

"The covered person shall also submit to the AMLC, through the internet, an electronic detailed return in a format to be prescribed by the latter."

For uniformity of E-Returns Format, CP user should first download the Electronic Return Template. This template is an excel worksheet where CPs must encode their E-Returns.

To download the template:

Log-on to https://portal.amlc.gov.ph

🔊 Anti Money Laundering Cour 🗙 🔪 🕂				Ŀ		×
1 1 kttps://portal.amlc.gov.ph/amlc/	🖾 🤇 C Sea	ırch	☆ 自	+ 1	1	:
Republic of the Philippines Anti-Money Laundering Council The Philippines' Financial Intelligence Unit						
Welcome to the Anti-Money Laundering Council Portal	!! (Ver. 2.8.4)	User Login				
*Online Registration - Allows Compliance Officers to register and attach supporting documents. Submission of hardcopy documents are no	longer required.	Username/Email:]		
*Upload CTR/STR Files - Encrypted Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) may be conveniently facility.	y transmitted to the AMLC via this	FORGO	LOGIN	_		
*View History of Uploaded CTR/STR Files - Access history of uploaded CTR/STR Files. Errors are logged, allowing users to identify and make the necessary con to download the validation messages.	rections. Users also have the option	Note: CPs with 11-dig CPs with 18-dig	jit Inst. Code - 1st git Inst. Code - 1st	6 digits 9 digits	-	
*View News Advisories - New and archived AMLC advisories may be accessed from this facility.		Registration S	tatus? CLICK HER	1		
*Upload Attachments to STRs - Digital attachments to Suspicious Transaction Reports (STRs) may be submitted through this facility. The STR shou uploading of attachments.	Id have been uploaded first prior to					
*View History of Uploaded Attachments to STRs - Access history and status of uploaded STR attachments.						

Enter the 1st 6-digits of the Inst. Code for CPs with 11-digit Inst. Code or the 1st 9-digits of the Inst. Code for CPs with 18-digit Inst. Code

Enter the Username or Registered email address

Enter password

User Login	
Institution Code:	
Username/Email:	
Password:	
	LOGIN
E	ORGOT PASSWORD
Note: CPs with CPs with	n 11-digit Inst. Code - 1st 6 digits 18-digit Inst. Code - 1st 9 digits REGISTER
Registra	tion Status? CLICK HERE!



A successful log-in will show the Covered Persons' User Main Page. Click on Electronic Returns Template,

The excel file contains two sheets, 1st sheet is for the main account and the 2nd sheet is for the related account/s.

1st Sheet is for the Main Account which is the subject of the Freeze Order

E	∃ 5 - ⊲	ਟੈਂ∗ ∓				Electronic	Return Template - E	xcel			困	-		×
Fi	ile Home	Insert	Page Layout	Formulas	Data Revie	ew View 🖓	Tell me what you v	vant to do				Sign ir	n A Sh	are
Pas	te 💉 B	ibri IU·▼	• 11 • A [*] ⊡ • ☆ • ↓		≫ - E	General S Number	€00 000 Formattin	al Format as g = Table = St Styles	Cell yles • Cells	x ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	nd & Manu lect • Classific Data Prot	ual ation tection		*
E33	2 *	+ ×	$\sqrt{-f_X}$											~
	А	В	с	D	E	F	G	н	I	J	к	L	М	
1											-			
2	Account Name	Account Number	Case/ Docket No.	Type/ Nature of Account	Branch	Status of Account (Active or Close)	Date& Time of Receipt of Freeze Order	Amount Frozen	Date & Time of Freeze	Other Relevant Information				
3														_
4														-
6														
7														_
8														-
10														
	()	RETURN FO	OR MAIN ACCO	DUNT DETAI	LED E-RETURN	FOR RELATED	(+)	: •						
						1	~			m n	m		1 10	00/

2nd Sheet is for Related/Materially-linked account which contains two (2) tables:

Table 1 is for materially-linked accounts as defined under Rule 3-Definition of Terms, R.1-5 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as Amended.

	8	o- ⊘	7					Electronic F	Return Template - E	cel				
	File	Home Inse	rt Page Laj	yout For	mulas Di	ata Revi	iew View	♀ Tell me						
Pa	aste pboard	Calibri	- 11 - - ⊡ - ♪ Font		= = = 4		' Wrap Text Merge & Center	Genera • 💽 •	al ••••••••••••••••••••••••••••••••••••	Conditional Formatting ▼	Format as Table - St	Cell yles •	nsert • Delete • Format • Cells	Sort & Filter • S
Q	12	×	$\checkmark f_x$											
1	A	В	С	D	E	F	G	н	1	J	К	L	М	1
	Tab	le 1 should i	include ma	aterially l	inked ac	counts a	s defined ur	nder Rul	e 3-Definition	n of Terms	, R.1-5 o	f the 20:	L6 Revised	
1	_		Im	plementi	ng Rules	and Reg	ulations of	Republi	c Act No. 916	0, as ame	nded			
2						MATER		ED ACCO	UNTS					
4	Accou Name the Freez Orde	nt in Number in the Freeze Order	Case/ Docket No.	Related Account Name	Related Account Number	Type/Nat ure of Account	Branch	Status of Account(Active or Close)	Date& Time of Receipt of Freeze Order	Amount Frozen	Date &Time of Freeze	REASON For Freezing As Related Account	Other Relevant Information	
5														
6														
8														
9														
10														
12														
13														
	$+$ \rightarrow	RETURN	FOR MAIN A	CCOUNT	DETAILED	DE-RETURN	N FOR RELATED) +)	:	•			
Re	ady													

Table 2 should include related accounts wherein Account Holder (Subject of Freeze Order) is either the Sender or Recipient of funds to/from another account holder.

E	<u>ج</u>	· @ · -	:					Electroni	c Return Template - E	xcel					Æ	- = >
F	le Ho	ome Inser	t Page L	ayout For	mulas [Data Rev	view View									Sign in 🔑 Shar
Pas	te	Calibri B I U	• 11 • ⊞ • ∠ Font				₩ Wrap Text Merge & Cente ht	Gene r + 🍄 ·	eral ▼ • % •	Conditional Formatting ▼	Format as Table + S Styles	Cell Ins	ert Delete Form Cells	at ∑ • A. ↓ • Z Sor € • Filt Ed	▼ t & Find & er ▼ Select ▼ iting	Manual Classification Data Protecti
134		• • · · ×	√ <i>f</i> s													
	A	B	с	D	E	F	G	H	1	J	К	L	M	N	0	P
14 15	Table 2	snould in	iciuae re	атео ассо	unts Wh	erein Ac	count Holde	acc	ount holder	oraer) is e	eitner th	e sende	r or kecipiei	nt of funds	to/from	another
16							E-RETURN	I - TRAN	ISFER OF FUNE)S						
17		MAIN A	CCOUNT						Relat	ed Accou	nt					
18	Account Name in the Freeze Order	Account Number in the Freeze Order	Case/ Docket No.	**Sender/ Recipient	Related/ Sender Account Name	Related/ Sender Account Number	Type/Nature of Account	Branch	Status of Account (Active or Close)	Date& Time of Receipt of Freeze Order	Amount Frozen	Date &Time of Freeze	REASON For Transaction Description	Freezing As REASON For Freezing As Related	Amount	Other Relevant Information
20																
21 22 23 24																
25 26 27 28 29	**Sender	r/Recipient	pertains to	the particp	ation of th	e Account	Name in the F	reeze On	der, if Name in th Recipient	e Freeze Or	der is the	Sender of	funds, type Se	nder, if a re	cipient of	funds, type
	C 🗼	RETURN	FOR MAIN	ACCOUNT	DETAILE	D E-RETUR	N FOR RELATE	D (Ð		4					Þ

Once the E-Return Worksheet/s has been accomplished, CP user may again log-in to the AMLC Portal and click on Electronic Returns Upload.



In the Electronic Returns Upload Facility, select between CA-GR AMLC Case and AMLC Resolution then click Proceed.

ELECTRONIC RETURNS UPLOAD FACILITY

Instructions:		
Select whether CA-Gi	R AMLC Case or AMLC Resolution on the list below.	
	Upload Electronic Returns	
	Select Document Type: * CA-GR AMLC CASE AMLC RESOLUTION Proceed	

If AMLC Resolution is selected, enter the AMLC Resolution Number, its corresponding year then click Browse to attach the E-Return file.

ELECTRONIC RETURNS UPLOAD FACILITY								
Instructions:								
Click the BROWSE bu	Itton to select the excel file containing the electronic returns and click the UPLOAD button to submit the selected file.							
	Upload Electronic Returns							
	Base Number: *							
	Electronic Returns: *							
	Upload Back to Menu							

If CA-GR AMLC Case is selected, enter the Case Number then click Browse to attach the E-Return file.

ELE	CTRONIC RETURNS UPLOAD FACILITY
Instructions:	
Upload E	Select Document Type: * CA-GR AMLC CASE Case Number: * Electronic Returns: * Browse Upload Back to Menu

C. General Guidelines. -



1. REPORTING FORMAT. –

- A. The electronic CTR/STR file is a comma separated variable file or **CSV** (see Attachment A) where each column/field/variable is separated by a comma. Text/Data fields must **not contain commas, single and double quotes**. A comma is used to separate the different fields of the record. The CSV file may be created by extracting all the required data (those above PHP 5,000,000.00) from the CP's database and building records following the format provided by AMLC or inputting the information in Excel and saving it using CSV as its file type. **Header column names or columnar headings should not be included in the file**. This file is structured to have several header records for CPs with branches and several detail records for the various transactions under each header record. At the end of the file is a trailer record containing the total number of transactions and the total Php amount of all the detail records. (See Attachment A)
- B. A single report format (Format 1.0) applicable to all covered persons shall be adopted for both CTRs/STRs in which the following **MANDATORY** fields shall be strictly filled up.

- 1. All fields in the HEADER RECORD.
- 2. In the DETAIL RECORD TRANSACTION DATA
 - a. TRANSACTION DATE AND TIME (D-2), TRANSACTION CODE (D-3), REFERENCE NO. (D-4), and PESO AMOUNT (D-5).
 - b. FX CODE if the FX AMOUNT has a value.
 - c. For wire transactions, Correspondent Bank details are mandatory.
- 3. For DETAIL RECORD SUBJECT DATA
 - a. For Name Fields for foreign nationals with one (1) name only, the following should be observed: 1. there should be five (5) dots (.....) either in first name or last name and 2. Nationality will be mandatory.
 - b. For ID Type 27 Others the ID no. should be preceded by the ID Type. (Please make sure that the ID type indicated does not fall in any one of the ID types before using ID 27.).
 - c. For Customer Party (CTRs only) all fields are mandatory.
 - d. For Subject of Suspicion (STRs only) all fields are mandatory.
 - i. The REASON and NARRATIVE fields.
 - ii. If the value in the reason field is "SI6", the description of the suspicious activity should always be specified separated by a semicolon.
 - e. For Other Participant (Used for Junket Operators) optional; If other participant is present, all fields are mandatory.
- C. The CTR/STR report file has three (3) parts identified by the Record Indicator located at the first field of every record with values H, D, or T:
 - 1. The Header Record identifies the Covered Person (CP), up to branch level, where the transaction occurred. A file may have several header records, if the reporting CP has several transactions from different branches to report;
 - There is one Detail Record for every transaction to report. Since the file may contain transactions from several branches, each group of Detail Records from one (1) branch is preceded by a Header Record; and
 - 3. Trailer Record (T) is the last record of the file and contains the total peso amount of the transactions and the total number of transactions in the file.

- D. The CTR/STR may be submitted in four (4) types.
 - 1. The CTR/STR with submission type value "A" refers to a new CTR/STR to be submitted to AMLC.
 - 2. The CTR/STR with submission type "E" edits or amends the previously submitted, uploaded and successfully processed CTR/STR with ERRONEOUS VALUE.

Note: The Institution code, Transaction date and reference number of the corrected transaction must be the same as the original transaction.

3. The CTR/STR with submission type "D" is a request to delete the previously submitted, uploaded and successfully processed CTR/STR. This shall be followed by an email request stating the reason for deletion. Email to be sent at <u>imag@amlc.gov.ph</u>

Note: The deleted transaction must be exactly the same as the original transaction previously submitted to AMLC.

- 4. The submission type "T" is used by CPs under test mode. Once they are comfortable with the reporting of covered and suspicious transactions, they should shift to submission type "A".
- E. The list of valid entries for the TRANSACTION TYPE, FX CURRENCY CODE and COUNTRY CODE fields are provided in pages B-1 to B-43.
- F. Definition of Field Names

HEADER RECORD

- H-1. Header Record Indicator This is the first field of the electronic record and will contain "H" to indicate that it is the beginning of the electronic file being sent by the CP to AMLC.
- H-2. Supervising Agency This field represents the supervising agency (whether PAGCOR/APECO/CEZA) of the reporting covered person.
- H-3. Institution Code This refers to the 11-digit code or 18-digit code of the reporting CP as assigned by the AMLC.
- H-4. Report Date Date of report in year, month, day format (YYYYMMDD). It should not be greater than the current date and not less than 20011017.

- H-5. Report Type Identifies whether report is CTR or STR.
- H-6. Format Code This identifies the format of the record.
- H-7. Submission Type Indicates whether the report being submitted is new, correction of previously submitted report and for deletion.

DETAIL RECORD

- D-1. Detail Record Indicator Contains "D" indicating start of detail record for each and every transaction belonging to the same date and transaction group defined in the header record.
- D-2. Transaction Date and Time Date and Time when transaction occurred in year, month, and day format (YYYYMMDDHHMMSS). Date should not be greater than the current date but not less than 20011017.
- D-3. Transaction Code Refers to the type of transaction based on AMLC's table of codes.
- D-4. Transaction Reference No. Refers to the unique reference number assigned by the reporting covered person to its individual transaction per transaction date.
- D-5. Transaction Amount (Php) Philippine Peso amount involved in the transaction or its equivalent if transaction is in foreign currency. Amount should be greater than 0.
- D-6. Transaction Amount (FX) If applicable, amount in original foreign currency involved in the transaction.
- D-7. FX Currency Code Indicates the currency of the FX transaction following AMLC's currency codes. Mandatory if FX Amount is not null.
- D-8. Nature/purpose of Transaction Explains the nature or purpose of transaction or the risk being insured.
- D-9. Correspondent Bank Where applicable, indicates the correspondent bank or remittance partner, i.e., remitter's bank in case of inward remittance transaction or the beneficiary's bank for outward remittance.
- D-10. Address of Correspondent Bank Gives the detailed address of the correspondent bank or remittance partner specifying the Room

No./Office Name, building/house no., street, District, Town, City, Country, and ZIP code.

- D-11. Country Code of Correspondent Bank Indicates the country of the correspondent bank following BSP country codes.
- D-A-1. Party Type Flag Indicates that the person is a customer (A)
- D-A-2. Customer Reference Number Refers to the CP's reference number of their client. This will serve as reference for the static data to be submitted by the reporting institution.
- D-A-3. Name of Customer Refers to the customer specifying the last name, first name, middle name of the individual person or the registered name of the corporation or partnership.
- D-A-4. Address of Customer Gives the detailed address of the account holder specifying the Room No./Office Name, building/house no., street, Barangay, District, Town, City, Province, Country, and ZIP code.
- D-A-5. Birthdate of Customer Date of birth of the customer. For individual accounts, the difference between the current date and the birthdate must be less than 150 and should also be less than the current date.
- D-A-6. Place of Birth Birth place of the customer (City, Municipality, Country).
- D-A-7. Nationality Nationality of the customer.
- D-A-8. ID Type Type of ID presented by the customer (SSS, GSIS, Company, etc.).
- D-A-9. Identification No. Identification No. of the customer.
- D-A-10. Telephone No. Contact number of the customer.
- D-A-11. Nature of Business Specifies the occupation of the customer or nature of the business of the corporation or partnership.
- D-P-1. Party Type Flag Indicates that the person is the Other Participant (P).
- D-P-2. Customer Reference Number Refers to the CP's reference number of their client. This will serve as reference for the static data to be submitted by the reporting institution.

- D-P-3. Name Flag "N" if Other Participant is an individual, "Y" if Other Participant is a corporation.
- D-P-4. Name of Other Participant Identifies the other party/person/entity involved in the transaction other than the beneficiary, counterparty, etc., specifying the last name, first name, middle name of the individual person or the registered name of the corporation or partnership. This is usually used for the Junket Operator.
- D-P-5. Address of Other Participant Gives the detailed address of the other party/person/entity involved in the transaction other than the beneficiary, counterparty, etc., specifying the Room No./Office Name, building/house no., street, Barangay, District, Town, City, Province, Country, and ZIP code.
- D-S-1. Party Type Flag Indicates that the person/corporation is the Subject of Suspicion (S).
- D-S-2. Customer Reference Number Refers to the CP's reference number of their client. This will serve as reference for the static data to be submitted by the reporting institution.
- D-S-3. Name of Subject of Suspicion Identifies the subject of suspicion, specifying the last name, first name, middle name of the individual person or the registered name of the corporation or partnership.
- D-S-4. Address of Subject of Suspicion Gives the detailed address of the subject of suspicion, specifying the Room No./Office Name, building/house no., street, Barangay, District, Town, City, Province, Country, and ZIP code.
- D-S-5. Birthdate of Subject of Suspicion Date of birth of the subject of suspicion. For individual accounts, the difference between the current date and the birthdate must be less than 150 and should also be less than the current date.
- D-S-6. Place of Birth of Subject of Suspicion Birth place of the subject of suspicion (City, Municipality, Country).
- D-S-7. Nationality of Subject of Suspicion Nationality of the subject.
- D-S-8. ID Type of Subject of Suspicion Type of ID presented by the subject (SSS, GSIS, Company, etc.).

- D-S-9. Identification No. of Subject of Suspicion Identification No. of the subject.
- D-S-10. Telephone No. of Subject of Suspicion Contact number of the subject.
- D-S-11. Nature of Business of Subject of Suspicion Specifies the occupation of the subject or nature of the business of the corporation or partnership.
- D-D-1. Reason For STRs, reason field refers to the coded reason for suspicion categorized by suspicious indicator (SI) or predicate crime (PC).
- D-D-2. Narrative Narrates the events leading to the suspicion including other information which might be of help or importance to the report, i.e., where the possible violation took place, related litigations, relation to other transactions, description of supporting documents, etc.

TRAILER RECORD

- T-1. Trailer Record Indicator Contains "T" indicating start of trailer record of every file.
- T-2. Total CTR Amount refers to the total/sum of all peso transaction amounts in the file.
- T-3. Records Total refers to the number of transactions included in the file.

Party Flag

- The party flag value "A" is for the customer of the reporting institution.
- For transactions involving parties other than the customer, beneficiary and counterparty, the party flag "P" for other party shall be used.
- The party flag "S" is for the subject of suspicion.
- G. The parties do not follow a particular order in the CSV file.
- H. The parties in the detail record are not mandatory for all transactions. Attached as Annex C, is the summary of the required parties per transaction. Failure to provide the mandatory parties shall cause the rejection of the file.
- I. For multiple valued name field, such as &/or account holders' names, multiple beneficiaries etc., each name shall be preceded by their corresponding party flags.

Example: For Joint Accounts: If Name Flag = N A,1234,DELA CRUZ,JUAN,REYES,123 ABC STREET,MAKATI CITY,MAKATI PHILIPPINES 2000,19700101,MANILA PHILS.,FILIPINO,ID1,XX1234567,7210202,REAL ESTATE, A,5678,DELA CRUZ,MARIA,ALCANTARA,123 ABC STREET,MAKATI CITY,MAKATI PHILIPPINES 2000,19720203,MANILA PHILS.,FILIPINO,ID1,XX7654321,7210202,REAL ESTATE,

- J. The address is divided into address 1 (Room No. /Office Name, building/house no., street, barangay), address 2 (District, Town, City) and address 3 (Province, Country Code, Zip Code).
- K. For STRs.
 - 1. Uploading of KYC Documents for STRs is mandatory, if an STR filed has no corresponding upload of KYC Documents, such STR will be rejected. (Complete guidelines are discussed in Section 4.B.3)
 - 2. In cases where in the perpetrator is not identified, CPs shall use the term **"Unknown"** in the Subject of Suspicion Name.
 - 3. The reporting institution shall choose the applicable Reason for Suspicion as enumerated in Section 2.A.2 [Electronic Record Format (Format 1.0–Casinos)]. For reasons other than the specified, the institution shall use the "SI6" followed by a semi-colon and the reason for suspicion.

Note: Please make sure that the reason for suspicion indicated in SI6 does not fall in any one of the Suspicious Indicators or Predicate Crimes before using SI6.

Example:

xxx,SI6;suspected boiler room operations, the client was named in one foreign news article xxx

- 4. The transaction code "ZSTR" shall be used if the subject is not a customer of the reporting institution or is a customer but has no monetary transaction with the covered person at the time the suspicious activity is determined.
- 5. In filing an STR, the following questions should be answered:¹

¹ Presentation materials on Intelligence Analysis & Intelligence Reports: A Workshop for FIUs held on 11 July 2008.

- WHO are the individuals/entities involved
 - People real, false IC
 - Business or companies, shell companies, legitimate businesses
 - Non profit organization/ charities
- WHAT is the activity of concern
 - Financing of terrorism
 - Drug Trafficking
 - People smuggling
- WHEN is the activity taking place
 - One-off transaction
 - o Daily
 - o Weekly
 - Monthly
 - Patterns within these time frames how many times, number of entities involved
- WHERE is the activity taking place
 - Consider all levels
 - Countries
 - o Cities
 - o Towns
 - \circ Are these patterns in location or use of same address?
- WHY is the activity taking place
 - Providing finance for terrorist activity
 - Moving proceeds of drug activity or other illegal activity
 - Purchase of Drugs or other illegal commodity etc.
- HOW is the activity taking place
 - Movement of funds, wire transfers, traditional banks, underground banks, cash couriers
 - o Quantity
 - o Currency used
 - Other commodities diamonds, precious gems, stored value cards, traveler's checks.

- 6. The narrative should contain all the details and events leading to the suspicion including other information which might be of help or importance to the report, i.e. where the possible violation took place, related litigations, relation to other transactions, description of supporting documents, etc.
 - a. Additional documents may be attached to the STR through the AMLC Portal. An STR attachment may be any of the recognized file types (.xls,.doc, .docx, .pdf, .bmp, .jpeg, .jpg , .tiff, .tif).

A facility in the AMLC portal allows the submission of this attachment. To upload an attachment, please make sure that the STR has been uploaded in the AMLC portal before uploading attachments. Please make sure you enter the complete eleven (11) or eighteen (18) digit institution code for the uploaded STRs; if the institution code used is that of the branch please ensure that you input this in the institution code field, then enter the transaction date and transaction reference number of the STR where the file will be attached.

- L. Key fields the key fields consist of the institution code, transaction date and transaction reference number. Together, they should be unique at all times. This means that the transaction reference number should be distinct per transaction date per institution.
- M. All amount values must **not** contain commas or special characters except the decimal point to indicate centavos, i.e., P550,120.50 should be encoded as 550120.50.
- N. Validity of each field values in terms of length and data type must be observed.
- O. The number of commas must be less than one from the required total number of field values

field1,field2,field3,field4 Total Fields = 4 Total Commas = 3

Note: field3 should always be followed by a comma whether or not field4 has data

CRN,Lastname,Firstname,Middlename or CRN,Lastname,Firstname,

P. CTR/STR reports should reflect **where the transaction occurred**, i.e. Head Office or branch. This is identified by the institution code in the Header record which must be 11 or 18 digits (up to branch level). There may be several detail records less than one (1) header record to report several transactions of one branch, and there may be several header records in one (1) file to report transactions of several branches.

For Covered Persons with Different Branches, the CTR/STR Format Structure should be as follows:

- H Header Record of Head Office
- **D** 1st Detail Record of Head Office
- **D** 2nd Detail Record of Head Office
- D Last Detail Record of Head Office
- H Header Record of Branch1
- **D** 1st Detail Record of Branch1
- D Last Detail Record of Branch1
- H Header Record of Branch2
- **D** 1st Detail Record of Branch2
- **D** 2nd Detail Record of Branch2
- D Last Detail Record of Branch2
- H Header Record of Branch n
- **D** 1st Detail Record of Branch n
- **D** 2nd Detail Record of Branch n
- D Last Detail Record of Branch n
- T Trailer Record
- Q. File Name convention for CPs with 11-digit institution code-999999yyymmddss.csv where 999999 = first 6 digits of institution code, yyyymmdd = reporting date (year, month, day the report is sent to AMLC), ss = sequence number from 01-99 representing number of files transmitted for the day (batch number or number of transmission). Default sequence no. is 01.

2. Additional Guideline in CT/ST Reporting. -

- A. The amount indicated in the CTRs or STRs shall include all taxes, or other fees incidental to the execution of the transaction.
- B. The AMLC supports the use of "multi-legged transactions" (series of transactions initiated by one (1) action within a covered person). Only the main transaction is required to be reported as CTR and the transactions inherent to the main transaction need not be reported.

E.g. Purchase of Manager's Check wherein amount will be paid by debiting the account of the client, instead of reporting two (2) CTRs for this, which is the debiting of the account and the actual purchase of MC; transaction code to be reported under Format 1.0 will be Purchase of MC via debit to account wherein the accountholder's account details (client who purchased the MC) will be reported.

- C. The Customer Reference Number (CRN) is mandatory for the Customer Party or Subject of Suspicion Party, whichever is applicable for Suspicious Transaction Reports, especially if the reason of Suspicion will fall in any of the following predicate crimes: Kidnapping for Ransom; Drug Trafficking; Hijacking; destructive arson; and murder, including those perpetrated by terrorists against non-combatant persons and similar targets; Terrorism and conspiracy to commit terrorism; and Financing of Terrorism. CRN will be used in the uploading of KYC documents.
- D. Deferred reporting shall be applicable to covered transactions only. The responsibility of CPs to report suspicious transactions, where applicable, remains. Should there be further adjustments/modifications in the application thereof; the foregoing policy shall be prospective.
- E. Digital certificate shall be implemented to ensure integrity, efficiency and security of the report files. The Gnu Privacy Guard (GPG) shall be provided to all the CPs to be used for encrypting and digital signing.
- F. To ensure that only authorized officials will be allowed to send reports to AMLC electronically, there shall be a registration and continuous data updating of business units, and their authorized compliance officers.
- G. Functional trainings for authorized persons are usually conducted on the last Wednesday of the month or upon announcement by the AMLCS.

- H. Rejected transaction due to invalid codes (transaction, currency and country) should be sent again using submission type A. Please take note that the reference number of the original transaction should be used for the resent transaction.
- I. The AMLC Web Services is a facility for CPs to transmit CTR/STRs automatically. To avail of the service, CPs should send an email to the Secretariat (imag@amlc.gov.ph) requesting enrolment to the facility. Thereafter, an email shall be sent by the Secretariat with the attached Registration Form and Web Services specifications.
- J. For COs handling multiple CPs under the same company umbrella, a single User Account may be arranged to be able to log-on and submit CTRs/STRs of the different subsidiaries/affiliates. To apply for this arrangement, an email request specifying the list of subsidiaries/affiliates to be grouped should be sent.
- K. The advisory icon in the AMLC portal which contains advisories, resolutions and guidelines shall be the main process of communication with the CPs. The "New Advisory" icon will flash whenever a new advisory is published, and will continue to do so until such time the user opens or reads the advisory.
- L. Electronic returns for Freeze orders shall be uploaded in the AMLC portal, guidelines please refer to Section 4.B.6 (Uploading of Electronic Returns (E-Return) for Freeze Order.
- M. Updates on the UNSC Designated list (include both the Taliban 1988 Sanctions List and the Al-Qaida Sanctions List) shall be posted in both the AMLC website and AMLC portal for reference and guidance.

Section 5. ANNEXES. –

The attached Annexes shall form part and parcel of this ARI:

- A. Annex A Sample CSV File (Format 1.0)
- B. Annex B System Codes
- C. Annex C Examples of Alerts and Red Flag Indicators

5

D. Annex D – Typologies of Money Laundering for Casinos

FOR THE AMLC:

MEL GEORGIE B. RACELA Executive Director

21 February 2018

SAMPLE CSV File (Format 1.0)

Sample Plotting of a CSV file (Format 1.0), using Microsoft Excel

			FIELD								
			NO.	FII	ELD NAME	TYPE	LENGTH	FORMAT	VALU	JE/REMARKS	
			H-1	Header F	Record Indicator	Text	1	Н	H - for Hea	der	
Ē	_		H-2	Supervis	ing Agency	Number	1	9	5 – PAGCO	R, 6 -CEZA, 7 -A	APECO
								9(11) /			
			H-3	Institutio	on Code	Number	11/18	(18)	AMLC Libra	ry	
									yyyymmdd	; not greate	r than
									current da	ite; not less	than
			H-4	Report D	ate	Number	8	9(8)	20011017		
			H-5	Report T	уре	Text	3	X(3)	CTR,STR		
			H-6	Format C	Code	Number	2	99	1		
									A- add, E- e	dit/correctio	n, D -
			H-7	Submissi	on Type	Text	1	X(1)	delete, T -te	est	
						L	1				
			А	В	С	D	E	F	G	Н	
		1	H	5	12345600000	20180103	3 CTR	1	Α		
		2		↑							
L		3									

Header Record

Note: Header Record consists of seven (7) fields; these 7 fields will be inputted from Columns A-G

	FIELD NO.	FIELD NA	AME		TYPE		LENGTH	FORMAT		VALU	JE/REM/	ARKS		
	D-1	Detail Record Indic	ator		Text		1	D	D - f	or Detail				
	D-2	Transaction Date a	ind Time		Numbe	r	8	9(8)	yyyy than 2001	mmddh current 11017	hmmss; date; r	not greater ot less than		
	D-3	Transaction Code	.C Transa	action Codes										
	D-4	Transaction Refere	ence No.		Text		20	X(20)	mus date	must be unique per transaction date				
	D-5	Transaction Amou	ınt (Php)		Numbe	r	20	9(18).99	Grea value	iter than e	0 w/ or	w/o decimal		
	D-6	Transaction Amou	ınt (FX)		Numbe	r	17	9(18).99	Opti	onal				
	D-7	FX Currency Code			Text		3	X(3)	Opti amo	onal; ma unt <> n	ndatory ull	if FX		
	D-8 to D-11													
	D-11	Country Code of Co Bank	ent	Numb	er	3	9(3)	Opti Syste	onal;Cou ems Cod	intry Coo e, Chapt	de (Refer to er 8.3)			
				7					Column	M, Row	2			
A	В	C	0	E	F	G	Н	I J	К	L	M			
	5	12345600000 53345 ACTCU	20180103 REE01	VCIR	▼ 1	▼ A					•			
3	LUIUUII31		NLI UI	5000001										

DETAIL RECORD TRANSACTION DATA (ROW 2, COLUMNS A-M)

Note: Detail Record Transaction Data will occupy Columns A-M

 	Party Type Flag	Text	1	Х	A - Customer
D-A-2	Customer Reference Number	Text	30	X(30)	
					N – if acct. holder is an individual
D-A-4	Name	Text			
 	Last Name		100	X(100)	Last name of account hol
	First Name		100	X(100)	First name of account ho
 	Middle Name		50	X(50)	Middle name of account
D-A-5	Address	Text			
_	Address1		100	X(100)	Room No./Office Name, Bldg./House No., Street, S Brgy.
 _	Address2		100	X(100)	District, Town, City
-	Address3		100	X(100)	Province, Country , ZIP
D-A-6	Birthdate/Registration Date	Number	8	9(8)	
D-A-7	Place of Birth/Registration	Text	90	X(90)	City, Municipality, Counti
D-A-8	Nationality	Text	40	X(40)	
D-A-9	ID Type	Text	4	X(4)	ID1 – Passport
D-A-10	Identification No.	Text	30	X(30)	
D-A-11	Telephone No.	Text	15	X(15)	
– D-A-12	Nature of Business	Text	35	X(35)	

SUBJECT DATA (Customer)

Note: Subject Data will immediately follow the details of the transaction data, D-A-1 (Customer Party Flag) should be inputted at Column N, same row as that of the transaction data.

TRAILER RECORD

		FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMA	۹T	VALUE/REMA	RKS	
		T-1	Trailer Record Indicator	Text	1	Т		T - for Trailer		
_		- T-2	Php Amount Total	Number	20	9(18).9	99	Total Transaction	Amount	
			Records Total of batch to be	e						
		T-3	sent	Number	10	9(10)	1	Total number of C	TR/STRs	
		A	В	С	D	E	F	G		
	1	1 H 5		12345600000	20180103	CTR	1	Α	_	
	2	D	20180115153345	ACTCH	REF01	5000001				
	3	Т	500001	1						
		<u> </u>		\bigwedge						

Note: Trailer Record will occupy the last row of the file to be uploaded, there are only three (3) fields, which will only be inputted from Columns A-C.

Below is a complete CSV file (Format 1), which consists of a Header Record, Detail Record (Transaction Data and Subject Data) and a Trailer Record.

4	A	В	с	D	E	F	G	н	1.1.1	J.	K	L	м	N	0	P	Q	R	s	т	U	V	W	x	Y	z	AA	AB	
1	н	5	12345600000	20180103	CTR	1	A																						
2	D	20180115153345	ACTCH	REF01	5000001									Α	CREF00001	REYES	JOSE	SANTOS	ADD1	ADD2	ADD3	19800912	MANILA	CHINESE	ID1	EE98238	9178234567	GAMBLER	
3	т	5000001	1																										

Sample using Notepad:

CASINOS

CASH TO CHIPS TRANSACTION (CTR)

H,5,12345600000,20180103,CTR,1,A → HEADER RECORD D,20180115153345,ACTCH,REF01,5000001,,,,,,,,A CREF00001,REYES,JOSE,SANTOS,ADD1, ADD2,ADD3,19800912,MANILA,CHINESE,ID1,EE98238,9178234567,GAMBLER,P,JUNKET001, N,JUNKETLAST,JUNKETFIRST,JUNKETMIDDLE,123 ABC STREET,MAKATI CITY,MAKATI PHILIPPINES 2000 T,5000001,1 → TRAILER RECORD PARTY FLAG

FOREIGH CURRENCY TO CHIPS TRANSACTION (STR)

H,5,12345600000,20180103,STR,1(A) → SUBMISSION TYPE D,20180115231535,AFCCH,REF02,1000000,20000,USD,TO PLAY SLOT,CHASE MORGAN,ADD1,ADD2,ADD3,USA,S,CREF56789,DELA CRUZ,JUAN,REYES,123 ABC STREET,MAKATLCITY,MAKATLPHILIPPINES 2000,19450203,MANILA PHILS.,FILIPINO,ID1,XX123456,4251754,REAL ESTATE, PC1 CLIENT WAS ALLEGEDLY INVOLVED IN A KIDNAPPING FOR RANSOM ACTIVITY ON 1 JANUARY 2018 XXX. T,1000000,1 NATIONALITY, ID TYPE, ID NO.

SYSTEM CODES

B.1 Transaction Codes for Casinos

GROUP	REVISED CODE	TRANSACTION TITLE	TRANSACTION DEFINITION
А	ACTCH	Cash to Chips	The purchase of chips using Cash
А	ACCCH	Purchase of Chips – Credit Card	The purchase of chips using Credit Cards.
А	ATITOP	Ticket-in-ticket-out (TITO) Ticket Purchase	Players purchase TITO tickets from the teller's cage to be used in the slot machine.
А	AFCCH	Foreign Currency to Chips	Exchange of Foreign Currency to tokens or peso bills to used in the slot machines with the option to redeem foreign currency at the same rate it originally used.
А	AFCCH	Foreign Currency to Tokens/Bills	Exchange of Foreign Currency to chips with the option to redeem foreign currency at the same rate it originally used.
A	AIRCH	Purchase of Chips via telegraphic transfer/wire	Players remit funds to the Treasury Fund Capital accounts of casino branches maintained with Land Bank of the Philippines. Chips are released after confirmation of the credit of funds.
А	ADDCH	Purchase of Chips via Demand Draft	Player deposits demand drafts issued by foreign banks to Land Bank of the Philippines. Chips are released once demand drafts are cleared.
А	ACHTC	Chips to Cash	The payment in cash in exchange for the players' chips holdings
А	ATITOR	Ticket-in-ticket-out (TITO) Ticket Redemption	Payment of TITO tickets presented for redemption to the teller's cage.
А	APAYW	Payment of winnings via telegraphic transfer/wire	Players' winning will be sent via wire to any bank in the country, subject to bank requirements and issuance of Certificate of Winnings.
А	АРАҮК	Payment of winnings via Demand Draft/Manager's Check	Players' winning shall be released via issuance of Demand Draft/Manager's Check, subject to bank requirements and issuance of Certificate of Winnings.
A	ATFC	Payment of winnings via TFC	Players' winning shall be released via issuance of Treasury Fund Capital Check (TFC) drawn against the branch's TFC account with Land Bank of the Philippines duly supported with a Certificate of Winnings from the Gaming Division, Slot Machine Division or Bingo Section.
А	АССКС	Chip check (cash)	Issuance of chip check in exchange of players' cash. Chip checks are negotiable only at PAGCOR casinos.
A	АССКСН	Chip check (Chips)	Issuance of chip check in exchange of players' chips. Chip checks are negotiable only at PAGCOR casinos.
A	ACCKE	Chip Check Encashment	Encashment of Chip Checks in casinos

А	AFTCH	Fund transfer to chips	Transfer of players' personal funds deposited to the Branch Treasury, wherein withdrawal of chips will be
			done in another branch.
А	ACHSE	Safekeeping	Players deposit playing chips for safekeeping with the
		sarenceping	Casino Treasury Division.
^		Capital Infusion Cash	Infusion of funds by a shareholder of the reporting
A	ACAPC	Capital Infusion - Cash	covered Person via cash
			Infusion of funds by a shareholder of the reporting
А	АСАРК	Capital Infusion - Check	covered person via check
			Infusion of funds by a shareholder of the reporting
A	ACAPD	Capital Infusion - Debit	covered person via debit to account
			Infusion of funds by a shareholder of the reporting
A	ACAPW	Capital Infusion - Wire	covered person via wire
			STR filed on the basis of suspicious trigger (ex. subject
			of news report, qualified theft, etc.) even if the subject
z	ZSTR	STR transactions	has no monetary transaction with the covered
	_		institution at the time the suspicious activity was
			determined
			uetermineu.

GROUP LEGEND: A - Casinos

B.2 Currency Codes

Description	Code
AFGHANISTAN AFGHANI	AFN
ALBANIAN LEK	ALL
ALGERIAN DINAR	DZD
ANDORRAN PESETA	ADP
ANGOLAN KWANZA	AOA
ARGENTINE PESO	ARS
ARMENIAN DRAM	AMD
ARUBAN GUILDER	AWG
AUSTRALIAN DOLLAR	AUD
AUSTRIAN SCHILLINGS	ATS
AZERBAIJANIAN MANAT	AZM
BAHAMIAN DOLLAR	BSD
BAHRAINI DINAR	BHD
BANGLADESHI TAKA	BDT
BARBADOS DOLLAR	BBD
BELARUSSIAN RUBLE	BYR
BELGIAN FRANC	BEF
BELIZE DOLLAR	BZD
BERMUDIAN DOLLAR	BMD
BHUTAN NGULTRUM	BTN
BOLIVIAN BOLIVIANO	BOB
BOTSWANAPULA	BWP
BRAZILIAN REAL	BRL
BRUNEI DOLLAR	BND
BULGARIAN LEV	BGL
BULGARIAN LEV	BGN
BURUNDI FRANC	BIF
CANADIAN DOLLAR	CAD
CAPE VERDE ESCUDO	CVE
CAYMAN ISLANDS DOLLAR	KYD
CFA FRANC BCEAO	XOF
CFA FRANC BEAC	XAF
CFP FRANC	XPF
CHILEAN PESO	CLP
CHINESE RENMINBI	RMB
COLOMBIAN PESO	СОР
COMORO FRANC	KMF
CONVERTIBLE MARKS	BAM
COSTA RICAN COLON	CRC
CROATIAN KUNA	HRK
CUBAN PESO	CUP
CYPRUS POUND	СҮР

CZECH KORUNA	CZK
DANISH KRONE	DKK
DEUTSCHE MARK	DEM
DJIBOUTI FRANC	DJF
DOBRA	STD
DOMINICAN PESO	DOP
EAST CARRIBEAN DOLLAR	XCD
EGYPTIAN POUND	EGP
EL SALVADORCOLON	SVC
ERITREA NAKFA	ERN
ESTONIAN KROON	EEK
ETHIOPIAN BIRR	ETB
EURO CURRENCY	EUR
EURO CURRENCY UNIT	ECU
FALKLAND ISLANDS POUND	FKP
FIJI DOLLAR	FJD
FINLAND MARKKA	FIM
FRANC CONGOLAIS	CDF
FRENCH FRANC	FRF
GAMBIAN DALASI	GMD
GEORGIAN LARI	GEL
GHANAIAN CEDI	GHC
GIBRALTAR POUND	GIP
GREECE DRACHMA	GRD
GUATEMALAN QUETZAL	GTQ
GUINEA FRANC	GNF
GUINEA-BISSAU PESO	GWP
GUYANA DOLLAR	GYD
HAITIAN GOURDE	HTG
HONDURAN LEMPIRA	HNL
HONGKONG DOLLAR	HKD
HUNGARIAN FORINT	HUF
ICELAND KRONA	ISK
INDIAN RUPEE	INR
INDONESIAN RUPIAH	IDR
IRANIAN RIAL	IRR
IRAQI DINAR	IQD
IRISH	ILE
IRISH POUND (PUNT)	IEP
ITALIAN LIRA	ITL
JAMAICAN DOLLAR	JMD
JAPANESE YEN	JPY
JORDANIAN DINAR	JOD
KAMPUCHEAN RIEL	KHR
KAZAKHSTAN TENGE	KZT
KENYAN SHILLING	KES

KUWAITI DINAR	KWD
KYRGYZSTANIAN SOM	KGS
LAO KIP	LAK
LATVIAN LATS	LVL
LEBANESE POUND	LBP
LEONE	SLL
LIBERIAN DOLLAR	LRD
LITHUANIAN LITAS	LTL
LUXEMBOURG FRANC	LUF
LYBIAN DINAR	LYD
MACAU PATACA	MOP
MACEDONIAN DENAR	MKD
MALAGASY FRANC	MGF
MALAWI KWACHA	MWK
MALAYSIAN RINGGIT	MYR
MALDIVE RUFIYAA	MVR
MALTESE LIRA	MTL
MAURITANIAN OUGUIYA	MRO
MAURITIUS RUPEE	MUR
MEXICAN PESO	MXN
MEXICAN UNIDAD DE INVERSION (UDI)	MXV
MOLDOVAN LEU	MDL
MONGOLIAN TUGRIK (TUGRUG)	MNT
MOROCCAN DIRHAM	MAD
MOZAMBIQUE METICAL	MZM
MVDOL	BOV
MYANMAR KYAT	MMK
NAMIBIA DOLLAR	NAD
NAMIBIAN DOLLAR	NAM
NEPALESE RUPEE	NPR
NETHERLAND GUILDER	NLG
NETHERLANDS ANTILLAN GUILDER	ANG
NEW ISRAELI SHEQEL	ILS
NEW TAIWAN DOLLAR	TWD
NEW ZEALAND DOLLAR	NZD
NICARAGUAN CORDOBA ORO	NIO
NIGERIAN NAIRA	NGN
NORTH KOREAN WON	KPW
NORWEGIAN KRONE	NOK
PAKISTAN RUPEE	PKR
PANAMANIAN BALBOA	PAB
PAPUA NEW GUINEA KINA	PGK
PARAGUAY GUARANI	PYG
PERUVIAN NUEVO SOL	PEN
PESO URUGUAYO	UYU
PHILIPPINE PESO	PHP

POLISH SLOTY	PLN
PORTUGUESE ESCUDO	PTE
POUND STERLING	GBP
QATARI RIAL	QAR
RIAL OMANI	OMR
ROMANIAN LEU	ROL
RUSSIAN RUBLE	RUR
RUSSIAN RUBLE	RUB
RWANDA FRANC	RWF
SAINT HELENA POUND	SHP
SAMOAN TALA	WST
SAUDI RIAL	SAR
SERBIAN DINAR	CSD
SEYCHELLES RUPEE	SCR
SINGAPORE DOLLAR	SGD
SLOVAK KORUNA	SKK
SLOVENIAN TOLAR	SIT
SOLOMON ISLANDS DOLLAR	SBD
SOMALI SHILLING	SOS
SOUTH AFRICAN RAND	ZAR
SOUTH KOREAN WON	KRW
SPANISH PESETA	ESP
SRI LANKA RUPEE	LKR
SUDANESE DINAR	SDD
SUDANESE POUND	SDG
SURINAME GUILDER	SRG
SWAZILAND LILANGENI	SZL
SWEDISH KRONA	SEK
SWISS FRANC	CHF
SYRIAN POUND	SYP
TAJIKISTANI SOMONI	TJS
TANZANIAN SHILLING	TZS
THAILAND BAHT	ТНВ
TONGAN PA'ANGA	ТОР
TRINIDAD & TOBAGO DOLLAR	TTD
TUNISIAN DINAR	TND
TURKISH LIRA	TKL
TURKMENISTAN MANAT	ТММ
U.S. DOLLAR	USD
UAE DIRHAM	AED
UGANDA SHILLING	UGX
UKRAINE HRYVNIA	UAH
UNIDADES DE FOMENTO	CLF
UZBEKISTAN SUM	UZS
VANUATU VATU	VUV
VENEZUELAN BOLIVAR	VEB

VIETNAMESE DONG	VND
YEMENI RIAL	YER
YENI TURK LIRAS (YTL)	TRY
YUAN RENMINBI	CNY
ZAMBIAN KWACHA	ZMK
B.3 Country Codes

Description	Code
ABU DHABI - U.A.E.	248
AFGHANISTAN	102
AFRICA N.E.S.	997
ALBANIA	081
ALGERIA	103
AMERICANPACIFICISLAND	021
AMERICAN SAMOA	034
AMERICANVIRGINISLANDS	027
ANDORRA	104
ANGOLA	105
ARGENTINA	106
ARMENIA	270
ARUBA	030
AUSTRALIA	107
AUSTRIA	051
AZERBAIJANIREPUBLIC	271
AZORES	036
BAHAMAS COMM OF	108
BAHRAIN	109
BANGLADESH	247
BARBADOS	110
BELARUSREPUBLIC OF	280
BELGIUM	052
BELIZE	118
BENIN	139
BERMUDA	113
BHUTAN	114
BOLIVIA	115
BOSNIA	277
BOTSWANA	112
BRAZIL	116
BRITISH ARAB STATES	121
BRITISH IND. OCEAN T.	119
BRITISH OCEANIA N.E.	120
BRITISHVIRGINISLAND	029
BRITISH WEST INDIES	122
BRUNEI	123
BULGARIA	082
BURKINA FASO	239
BURMA/MYANMAR	124
BURUNDI	125
CAMEROUN UNITED REP	127

CANADA	022
CANARYISLANDS	039
CAPE VERDEISLANDS	040
CAROLINE ISLANDS	041
CAYMANISLANDS	028
CENTRAL AFRICAN REP.	128
CHAD	130
CHANNELISLANDS	031
CHILE	131
CHINA	083
CHRISTMASISLANDS	042
COLUMBIA	133
COMORES ARCHIPELAGO	043
CONGO REP OF	134
COOKISLANDS	260
COSTA RICA	136
CROATIA	094
CUBA	137
CURACAO	032
CYPRUS	138
CZECHOSLOVAKIA	084
CZECH REPUBLIC	288
DENMARK	053
DJIBOUTI (REP OF)	261
DOMINICAN REPUBLIC	140
DUBAI - U.A.E.	249
ECUADOR	141
EGYPT	238
EL SALVADOR	142
ESTONIA	096
ΕΤΗΙΟΡΙΑ	143
EUROPE N.E.S.	998
FAEROE ISLANDS	145
FALKLANDISLAND& DEP	144
FIJI	146
FINLAND	147
FRANCE	054
FRENCH GUINA	148
FRENCH OCEANIA N.E.S.	149
FRENCH SOMALILAND	150
FRENCH WEST AFRICA	151
FRENCH WEST INDIES	152
GABON	153
GAMBIA THE	154
GERMANY DEM REP OF	085
GERMANY FEDERAL REP	055

GHANA	155
GIBRALTAR	156
GREECE	056
GREENLAND	157
GUADALOUPE	158
GUAM (MARIANASISLAND)	023
GUATEMALA	159
GUINEA	160
GUINE-BISSAU REP OF	206
GUYANA	117
HAITI	161
HONDURAS	162
HONGKONG	163
HUNGARY	086
ICELAND	057
INDIA	164
INDONESIA	165
IRAN	166
IRAQ	167
IRELAND REP OF	058
IRIAN (WEST/BARAT)	168
ISLE OF MAN	046
ISRAEL	169
ITALY	059
IVORY COAST	170
JAMAICA	171
JAPAN	060
JORDAN	172
KAMPUCHEA	126
KAZAKHSTAN	089
KENYA	173
KIRGHIZIAREPUBLIC OF	273
KIRIBATIREPUBLIC	262
KOREAREPUBLIC OF	221
KUWAIT	174
LAOS	175
LATVIA	284
LEBANON	176
LEEWARD & WINDWARD	035
LESOTHO	111
LIBERIA	177
LIBYA	178
LIECHTENSTEIN	061
LITHUANIA	097
LUXEMBOURG	062
MACAO	983

MACAU	047
MACEDONIAREPUBLIC OF	268
MADAGASCAR DEM REP	179
MADEIRA	048
MALAWI REP OF	180
MALAYSIA	245
MALDIVEISLANDS	049
MALIREPUBLIC OF	181
MALTA	182
MARSHALL ISLANDS	050
MARTINIQUE	183
MAURITANIA	184
MAURITIUS	185
MEXICO	186
MOLDOVAREPUBLIC OF	282
MONACO	033
MONGOLIA	087
MONTENEGRO	285
MOROCCO	187
MOZAMBIQUE	188
NAMIBIA	266
NAURU	189
NEPAL	190
NETHERLANDS	063
NETHERLANDS ANTILLES	191
NEW CALEDONIA	192
NEW ZEALAND	194
NICARAGUA	195
NIGER	196
NIGERIA REP OF	197
NORFOLK ISLAND	263
NORTH KOREA	088
NORWAY	064
OCENIA N.E.S.	990
OMAN SULTANATE OF	246
OTHER COUNTRIES	999
PAKISTAN	199
PALAUREPUBLIC OF	269
PALESTINIANTERRITORIES	301
PANAMA	200
PANAMA CANAL ZONE	024
PAPUA NEW GUINEA	201
PARAGUAY	202
PERU	203
PHILIPPINES	204
POLAND	090

PORTUGAL	065
PORTUGUESE AFRICA	244
PORTUGUESE ASIA	205
PORTUGUESE TIMOR DEP	207
PUERTO RICO	025
QATAR	208
REPUBLIC OF SERBIA	287
REUNION ISLAND	209
RODRIGUEZISLAND	045
ROMANIA	091
RUSSIAN FEDERATION	281
RWANDA	210
RYUKYU ISLANDS	198
SABAH	211
SAIPAN	098
SAO TOME & PRINCIPE	283
SARAWAK	212
SAUDI ARABIA	213
SENEGAL	214
SEYCHELLES	215
SIERRA LEONE	216
SINGAPORE	217
SLOVAK REPUBLIC	286
SLOVENIA	278
SOCIETYISLANDS	038
SOLOMON ISLANDS	264
SOMALIREPUBLIC	218
SOUTH AFRICA REP OF	219
SOUTH WEST AFRICA TE	220
SOUTHERN RHODESIA	223
SPAIN	066
SPANISH AFRICA (ORO/M	224
SRI LANKA	129
ST. HELENA & DEP	225
STPIERRE ET MIGUELON	226
SUDAN DEP REP OF	227
SURINAM	228
SWAZILAND	229
SWEDEN	067
SWITZERLAND	068
SYRIA	251
ТАНІТІ	252
TAIWAN	132
TAJIKISTANREPUBLIC OF	275
TANZANIA	230
THAILAND	231

TOGO	232
TONGA	233
TRIESTE	236
TRINIDAD & TOBAGO	234
TUNISIA	235
TURKEY	069
TURKMENISTANREPUBLIC OF	276
TURKS & CAICOSISLAND	044
U.S.S.R.	092
UGANDA	237
UKRAINE	267
UNITED KINGDOM	070
UNITED STATES	026
URUGUAY	240
UZBEKISTAN	095
VANUATU	193
VENEZUELA	241
VIET-NAM SOC REP OF	222
WEST INDIES N.E.S.	991
WESTERN SAMOA	265
YEMENARABREPUBLIC	242
YEMEN PEOPLE'S DEM	101
YUGOSLAVIA	093
ZAIREREPUBLIC	135
ZAMBIA	243
ZIMBABWE	037

EXAMPLES OF ALERTS AND RED FLAG INDICATORS

1. There is no underlying legal or trade obligation, purpose or economic justification

- Offsetting bets
- Acquaintances betting against each other in even-money games and appearing that they are intentionally losing to one of the parties.
- Customer requesting for fund transfer to charity that is unfamiliar to the casino or appears to have links to countries that have lack AML/CFT controls.
- Buying casino chips and cashing them in, without gambling, by way of a casino cheque, bank draft of money transfer.
- Putting money into slot machines and claiming the accumulated credits as a jackpot win.
- Customers asking to combine winnings and his and her own cash not played in the casino into casino cheques
- Customers frequently inserting substantial amounts of banknotes in gaming machines that have high payout percentages and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Frequent even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat, or craps).
- Customer's intention to win is absent or secondary.
- Two or more customers frequently wagering against one another on evenmoney games.
- Customer in possession of large amounts of coinage or bills.
- Customer befriending/attempting to befriend casino employees.
- Purchasing and cashing out casino chips with little or no gaming activity.
- Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque.
- Multiple cheques being requested or drawn on account.
- Chip cash out is same/similar to chip purchase.
- Requests for credit transfers to other casinos.
- Use of multiple names to conduct similar activity.
- Use of third parties to purchase casino chips.
- Customer purchases chips and leaves casino shortly after.
- CPV, TITO, ticket or voucher dated prior to date of redemption.
- Large chip purchases.
- Frequent purchase of casino gift certificates.
- Detection of chips brought into the casino.
- Deliberation on losing a bet to other party(ies) on
 - peers to peers games; or
 - opposite bets with similar odds in banker hosted games

- Exchange of cash/ casino currencies without commensurate gambling activities
- Structuring transactions to stay below reporting threshold
- Chip walk
- Customer conducting small changing of chips or deposit or withdrawal of funds without gambling.
- Customer requesting for multiple payments of winnings and capital to the same account of a third party.
- Frequent access to safety box without commensurate gambling activities
- A patron provides a wire transfer, cashier's check or other form of payment and such instrument reflects that the transaction is being made for a purpose other than related to gaming
- Fund transfer to a customer or from a customer that is through multiple financial institutions or jurisdictions in an attempt to disguise their origin.
- Transfer of funds between customers through means such as hand to hand, wire transfer, safety box deposit, front money, or online casino accounts etc
- Inserting funds into gaming machines and immediately claiming those funds as credits.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.

2. The client is not properly identified

- Client refused to provide details/ provide fake details
- Proxy betting
- Bettor employed by other parties to place bets
- Client receives money/ casino currencies from 3rd parties through means such as hand to hand, wire transfer, safety box deposit, front money, or online casino accounts etc
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.

3. The amount involved is not commensurate with the business or financial capacity of the client

- Unexplained income inconsistent with financial situation/customer profile.
- Client's gaming/ cage activity dramatically increases with no known substantiation for the source of those funds
- Client's gaming/ cage activity or wagers incommensurate to the profile originally established by the covered person
- Customers with unclear source of wealth/ funds betting in large amount
- A negotiable instrument or wire transfer is presented for the benefit of multiple patrons, or multiple patrons engage in play on a single patron account
- A patron presents funds which the casino has a basis for suspecting to be the proceeds of illegal activity;

- A patron presents funds in any form that derive from a high risk jurisdiction
- 4. Taking into account all known circumstances, it may be perceived that the client's transaction is "structured" in order to avoid being the subject of reporting requirements under the law
 - Structuring transactions to stay below reporting threshold
 - A patron requests information about how to avoid AMLC reporting requirements
 - A patron refuses to provide information for the completion of a CTR, or identifying information more broadly
 - Multiple players requesting for payments to the same beneficiary (except for customers of junket operators)
 - Structuring the purchase of chips below the mandatory cash transaction reporting threshold.
 - Regularly depositing or transacting similar amounts of cash, which are below a country's reporting disclosure limit.
 - The use of third parties to undertake transactions using single or multiple accounts.
 - Using cheques from multiple financial institutions or branches of a financial institution to "buy in" while the amount of each cheque is below the reporting threshold.
 - Utilizing shift changes to systematically "cash in" chips or other value instruments to avoid threshold reporting.
 - Regularly switching gaming tables, gaming rooms, junkets or casinos within a chain when the wagering amounts are approaching the reporting threshold.
 - Requesting the division of winnings or prize money, which exceeds the reporting threshold, to be broken down into cash and chips below the reporting threshold in order to exchange it at the cashier's desk.
 - High volume of transactions within a short period.
 - Multiple chip cash outs on the same day.
 - Structuring of chip/cheque transactions.

5. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person

- Dramatic or rapid increase in size and frequency of transactions for a regular card holder.
- Noticeable spending/betting pattern changes.
- Dramatic or rapid increase in size and frequency of transactions for regular account holder.
- Client's gaming activity dramatically increases with no known substantiation for the source of those funds
- Client's gaming activity or wagers incommensurate to the profile originally established by the covered person

- Cage perform wire transfer/ remittance to customer(s) or a different beneficiary without apparent reason/ supporting gaming activity records
- Client request for winner cheques without commensurate gaming activities/ winnings
- 6. The transaction is in any way related to an unlawful activity or offense under this Act that is about to be, is being or has been committed; or
 - Use of fraudulent identity/ credit cards/ payment cards to perform any form of cage transactions
 - Withdraw money using fraudulent credit cards/ payment cards in the casino
 - Use of counterfeit casino currencies
 - Booking of fictitious gaming activities/ transactions by junkets (e.g. for the purpose of bypassing table limit/ facilitation of cross border transfer etc)
 - Client(s) who perform the transactions are found to be known or related associates of criminal/ wanted persons
 - Funds involved in the transaction/ activity originates from casino cheat/ scam or another other offenses as described under the AMLA

7. Any transaction that is similar or analogous to any of the foregoing.

- Supposed winnings do not correspond with recorded winnings.
- Use of credit cards to purchase casino chips.

TYPOLOGIES OF MONEY LAUNDERING IN CASINOS

Typology 1: Use of Junkets

A Syndicate Member in Country A wants to send (beneficiary) drug proceeds to Syndicate Head in Country B. With the help of a junket promoter, Syndicate Member caused the transfer of said proceeds to a casino in country A. The junket operator then informed an underground remitter in Country B about the amount and beneficiary of the funds. The remitter would then arrange payment of the fund to the beneficiary. When the beneficiary arrives at the casino in Country B, he immediately obtains the amount transferred by the Syndicate Member in County A through gambling. Both the casino and the remitter would perform reconciliation for net settlement, and thus, basically no transfer of monies between two sides was required.

Typology 2: Use of Junkets

A casino in Las Vegas, operated a marketing team ("junket") catering to Korean customers. The junket representative lent gambling money to Koreans in the form of cards (coupons), not cash, so that the corresponding loan would be spent only for gambling at the Las Vegas Casino. Representatives of this junket visited Korea to collect debts or make the customer's relatives in Korea do so on their behalf. The collected money was paid to trading companies in Korea for the goods that these companies sold to importing companies in the United States. The importing companies paid the amount to the Las Vegas Casino.

Typology 3: Hedging

- a) A customer routinely bets both sides of the same line and thus the amount of overall loss to the customer is minimal (known as hedging).
- b) A pair of bettors frequently cover between them both sides of an even bet, such as: (1) betting both "red and black" or "odd and even" on roulette; (2) betting both with and against the bank in baccarat/mini-baccarat; or (3) betting the "pass line" or "come line" and the "don't pass line" or "don't come line" in craps; and, the aggregate amount of both bettors' total wagering is in excess of USD5,000.00.

Typology 4: Use of Junkets

Mr. A contacted junket operator AA in Jurisdiction X to facilitate a junket game for him and his friends at Casino 1 and Casino 2.

Junket operator AA, through an officer in Bank B, caused the opening of four (4) bank accounts in Bank B. The accounts would be used as a depository account to receive money from Mr. A for his casino gaming activity.

A total of USD81 million was wired to the four (4) accounts opened in bank B by Junket operator AA. Junket AA instructed the bank officer of Bank B to transfer USD65.8 million to another fictitious account, and to transfer USD15.2 million to the bank account of remittance agent C. Thereafter, junket operator AA and bank officer B instructed remittance agent C to perform the following: (a) Transfer Php1 billion to the account of junket operator AA; (b) Deliver cash to junket operator AA; and (c) Transfer funds to the account of Casino 1.

Junket operator AA facilitated the gaming activity of Mr. A and his friends at the VIP gaming program of Casino 1 and junket program of Casino 2. Mr. A and his friends requested Casino 1 to transfer most of their gaming funds to an account with another junket operator, BB, also located inside Casino 1.

Mr. A and company played in Casino 2 briefly, then played for several days in the VIP program of Casino 1 and junket operator BB. In the course of their gaming activities, they withdrew a substantial amount of winnings.

When Casino 1 found out that the money being played by Mr. A and his friends were proceeds of a bank hacking incident in jurisdiction Z, its officers immediately stopped the gaming activities and seized all chips and money in the gaming tables, gaming accounts and those that were found inside their hotel rooms.

Investigation by the Financial Intelligence Unit (FIU) into the casino transactions of Mr. A and his friends revealed that some of them do not have previous gaming activities, while the gaming transactions of others substantially deviated from their gaming profiles. The large transactions, deviation from transaction profiles, and unusual gaming patterns displayed by Mr. A's group would have been reportable as Suspicious Transactions under the anti-money laundering laws of Jurisdiction X. However, casinos are not required to file said reports there because casinos were not covered by the country's anti-money laundering/counter-financing of terrorism (AML/CFT) regime. Thus, the FIU in jurisdiction X and the law enforcement agencies there were unable to conduct a timely investigation.

Cases of money laundering were filed against junket operator AA, officers of bank B, and officers of remittance agent C.

Typology 5: Casino to bank transactions

A law enforcement investigation identified a professional money laundering syndicate operating between Australia, Jurisdiction X and Jurisdiction Y.

The investigation revealed that the offender flew to Australia from Jurisdiction X, and two (2) days upon arrival, played at a casino. There she received USD473,000.00 in cash stashed in a backpack from an associate (suspect A), at the casino car park, then deposited it into her casino account. After unsuccessfully attempting to transfer a portion of the funds from her casino account to the bank account of another associate (Ms. X), the offender withdrew USD227,000.00 in cash. Then she attempted to deposit the cash with the intention of transferring it to Ms. X, who worked for an Australian money remittance business based in a different state. The offender was unable to provide satisfactory information when questioned by bank staff as to the origins of the cash and purpose of the transaction. The

results of the law enforcement investigation led to the offender's arrest at the bank as she was attempting to deposit the cash.

The offender was charged with one count of dealing with more than AUD100,000.00 based on a reasonable suspicion that the funds represented the proceeds of crime; she was sentenced to sixteen (16) months' imprisonment.

Typology 6: Use of gambling coupons

Person M, a well-known entrepreneur, is the suspect of money laundering and dealing with the proceeds of crime. Person M sells coupons used for gambling in District "T" supplied by person P, who lives in district "B". Person M has two (2) accounts used to carry out the gambling transactions, account "1", used for placement, transfer and receipt of proceeds from gambling, and account "2", used to place profits from the sale of gambling coupons supplied by person P. The profit represented up to 17% of all coupon transactions.

Typology 7: Use of licensed casinos

Mr. X, an employee of a point of sale business for two (2) casinos (FDJ and PMU), located in the greater Paris region, and run by Mr. Y. Tracfin (France FIU) was alerted to an unusually large number of cheques and wire transfers of winnings credited to the bank accounts of these two casinos. Over a fifteen (15)-month period, Mr. X deposited more than 4,000 separate winnings totaling about €1.5million (USD1.69 million). Mr. Y deposited nearly 700 separate winnings for more than €200,000.00 (USD225,600.00). The winning tickets, nearly all of them sports and horseracing betting products, were validated in Mr. Y's outlet, whose turnover in gaming products increased exponentially over the same period. However, the origin of the money bet by Messrs. X and Y was not clear. Upon investigation it was determined that although payments by cheque, wire transfer or credit card were registered with their bank accounts, they did not sufficiently account for the recurrence and the extremely high amount of the winnings. Mr. X and Y must have been injecting additional money into gaming, whose origin was unknown and therefore raised red flags. Finally, Mr. X, whose official sources of income were quite modest, lived a quite comfortable lifestyle and also acquired real estate.

Typology 8: Use of Casino Gaming Account

AUSTRAC (Australian FIU) disseminated an intelligence assessment report to law enforcement agencies regarding the financial activities of a suspect attempting to launder the proceeds of crime raised through drug related activity. The suspect used bank and casino accounts to launder the funds.

The suspect was the subject of five (5) suspicious matter reports (SMRs) submitted to AUSTRAC. Over a four (4)-day period the suspect made five (5) structured cash deposits of between AUD8,000.00 and AUD9,000.00 into his personal bank account. The structured cash deposits totaled AUD41,500.00. Bank staff reported in the SMRs that the deposited cash smelled of mothballs. After the deposits, the suspect undertook a domestic electronic transfer to move AUD40,000.00 from his bank account into an account with an Australian casino. The suspect deposited another AUD40,000.00 cash directly into the casino account.

An additional SMR submitted by the bank reported that the suspect received a deposit via domestic electronic transfer of AUD131,000.00 from the casino. Following this deposit into his bank account, the suspect withdrew AUD9,000.00 in cash.

The casino submitted an SMR. indicating that the suspect was known by two (2) aliases and that he would become aggressive when casino staff requested identification as part of the casino's normal identification procedures for customers cashing out gaming chips. The casino also reported that the suspect was known to cash out chips in amounts under the AUD10,000.00 cash reporting threshold, presumably to avoid the requirement to present identification to staff.

The suspect was arrested at a domestic Australian airport after a drug detector dog reacted to his suitcase. The suitcase contained ten (10) vacuum-sealed plastic bags containing a total of 4.5 kilograms of cannabis. The suspect was charged with attempting to traffic a controlled drug, contrary to sections 11.1 and 302.4 of the Criminal Code Act 1995 and was sentenced to two-and-half years' imprisonment.

Typology 9: Significantly large wire transfer to a casino gaming account

AUSTRAC contributed to a joint international investigation sparked by the suspicious behavior of a prominent Asian businessman. The investigation exposed a multi-million-dollar global fraud committed by an Asian finance manager, who was known as a habitual gambler and international casino 'high roller'.

Authorities in Asia suspected that the suspect had defrauded a number of international banks. AUSTRAC received an international request for information from counterparts in Asia, seeking assistance with their enquiries with regard to the financial activity of the target while he was in Australia.

AUSTRAC data identified that the suspect had conducted significant international funds transfers to Australian casinos, had visited Australia to gamble at the casinos, and had left Australia with substantial amounts of money, presumed to be the proceeds of his gambling. This information proved the initial suspicions of AUSTRAC's Asian counterparts that the suspect had transferred funds to casinos in Australia.

The suspect was arrested and subsequently admitted to Asian authorities that he had embezzled approximately AUD78 million (USD72,003,360.00) from four (4) international banks by forging signatures of his company's executives and opening accounts in the name of his employer.

Over a four (4)-year period the suspect transferred approximately AUD190 million (USD175 million) into an Australian casino account via international funds transfer instructions (IFTIs). In addition, the suspect had visited a number of casinos in London, Macau and Malaysia, in some instances placing bets worth up to AUD400,000.00 (USD369,248.00).

Asian authorities requested further assistance from Australian law enforcement to trace additional proceeds of the suspect's fraud. In conjunction with AUSTRAC, Australian law

enforcement discovered an additional AUD30 million (USD28 million) in accounts with various Australian casinos, held in the name of the suspect. Of this amount, AUD7 million (USD6.5 million) was restrained by Australian law enforcement under the Proceeds of Crime Act 2002, and a portion of this was repatriated back to the investigating authorities in Asia.

The suspect pleaded guilty in Asia to six (6) counts of forgery and eight (8) counts of cheating and was subsequently sentenced to forty-two (42) years' imprisonment.

Typology 10: Cashing out without record of chips purchase

Suspect A was arrested by law enforcement upon arrival in Australia, where he was found to be in possession of card skimming technology. This included computer disks, a laptop, a card encoder, an ATM feeder 'face unit' and thirty-one (31) blank ATM cards. The suspect was an international student residing in Australia.

Upon his arrest, law enforcement commenced an investigation into his activity and discovered a card skimming syndicate operating in Australia which laundered the proceeds of its crimes through casinos. Analysis of AUSTRAC financial transaction data associated with suspect A identified three additional members of the syndicate and their activities.

Members of the syndicate regularly visited casinos. Over a five (5)-month period, AUSTRAC received threshold transaction reports (TTRs) indicating that suspect A had cashed in more than AUD180,000.00 (USD166,612.00) worth of gaming chips at an Australian casino. However, transaction records showed that the suspect had not previously purchased a corresponding amount of gaming chips at the casino. This suggested that the suspect may have purchased the chips directly from another player before cashing them out, while claiming they were actually his 'winnings'.

AUSTRAC information was also used to identify the irregular gaming activity of suspect B. Information on AUSTRAC's database indicated that, over a twelve (12)-month period, suspect B had purchased AUD50,000.00 (USD46,156.00) worth of gaming chips at a casino. However, records indicated that the suspect had cashed out more than AUD610,000.00 (USD563,103.00) worth of gaming chips at the casino. Suspect B also made regular cash deposits and withdrawals, often in amounts over the reporting threshold of AUD10,000.00 (USD9,231.00), into bank accounts in Australia in the days following the casino transactions.

A suspect transaction report (SUSTR) was submitted by an Australian casino, noting that: (a) suspect B presented AUD28,000.00 (USD25,847.00) worth of casino chips to a cashier to be cashed out, before handing the cash proceeds to another person, believed to be suspect A; and (b) The value of gaming chips cashed out by suspect B did not correspond with the suspect's observed game play at the casino due to the high volumes of winnings compared to funds withdrawn for gambling purposes, nor did it correspond with the expected financial activity of a young university student.

A second SUSTR was also submitted by an Australian financial institution detailing suspicious transactions conducted by suspect B. Over a (3) three-month period suspect B deposited more than AUD155,000.00 (USD143,084.00) in cash into an account, indicating to bank staff

that these funds were casino winnings. The majority of these funds were then withdrawn in cash at the bank and via ATMs at the casino.

Suspect A was charged under section 480.6 of the Criminal Code Act 1995 for the importation of a thing to dishonestly obtain or deal in personal information.

Typology 11: Use of casino accounts, third party placement, infiltration of junket management

CYK, a Hong Kong tycoon and owner of British soccer club in Birmingham (UK), was convicted of laundering HKD93 million through, inter alia, junket operators and casinos in Macau.

The prosecution charged that since 2001 various parties made deposits to their accounts, many for no apparent reason. Some were made by securities firms and a Macau casino company, while others were made by unknown parties. Some 437 deposits totaling more than HKD97 million were made in cash.

Throughout the trial, CYK said he accumulated hundreds of millions of dollars through stock trading, business ventures in main land China, winnings from gambling and even hair dressing. The Court showed that CYK moved funds for Neptune VIP Club, a junket operator in Macau. One of Neptune's owners, CCT, is alleged to be the head of a powerful Hong Kong Triad gang. According to the evidence at trial, more than HKD18 million was washed by Mr. Yeung for Mr. Cheung.

Typology 12: Use of third parties, triggering transaction reports to legitimize suspicious transactions

A number of persons purchased chips with illicit cash in amounts below the CTR threshold, but then passed the chips to one individual who cashed out, receiving a casino cheque and triggering the filing or a CTRC that gave the appearance of further authenticating the transaction.

Over a twelve (12)-month period, one individual was named in casino CTRCs reporting USD1.1 million paid out, but was not named in a single CTRC for cash taken in.

Typology 13: Use of third parties to move illicit funds

John in Macau could not perform a large remittance to China due to its foreign exchange control. Susan in China wished to gamble in this casino of Macau, but had difficulty in bringing in the cash. Junket and remitter (aka "M") performed matchmaking and reconciliation/ settlement to solve the demand.

John paid M's Macau account the desired remittance amount. Susan paid M's China account the desired gaming funds amount. As Susan arrives in Macau, M provide gaming capital to Susan via Macau account using the funds from John. M also pays John's beneficiary in China via China account using the funds from Susan. M would perform reconciliation for net settlement (insofar John and Susan has paid their ends in advance), and basically no transfer of monies between two sides was required.

Typology 14: Use of third parties and false identities to structure gambling transactions

A Person of Interest (POI) of a drug trafficking organization, utilizing both the money he was paid for his services and the large sums of money put into his possession to be laundered, recruit third parties at the casino to purchase, or cash in, chips for him, paying them a nominal fee to do so. He then gambles. After gambling, he would cash some of these third-party purchased chips back out again, claiming they were his gambling winnings.

According to the CTRs a USD 313,000.00 discrepancy was found to exist between chip purchases and cash out. Twenty-four of the CTRCs recording his activities revealed the use of aliases and multiple social security numbers. On numerous other CTRCs he had refused to provide a social security number.

Typology 15: Use of debit cards to conduct money laundering transactions

An existing member of a casino introduced a number of people over a period of time. Suspicious was raised as the new members were completing debit card transactions to the maximum limit and receiving gaming plaques in exchange, which in turn were passed to the existing member.

Most of the new members never returned to the casino after the initial visit. The nationalities of the new members varied widely, but all are believed to have recently arrived from foreign jurisdictions. The transactions varied from GBP1,000.00 to 7,000.00.

Typology 16: Proxy betting

Gamblers in China obtain credit lines from Macau junket operators, who are repaid using funds derived from unlawful activities by the players ("beneficial owners") inside China. The gaming credit stays outside China, away from scrutiny by the Chinese government and its currency controls – and where it can be cashed out in Macau as gambling proceeds.

To launder funds, these gamblers use Macau's junket operators as fronts, especially for highrollers, to bet on their behalf. Hired hands of these junket operators often use wireless headsets to receive instructions from the "beneficial owners" in China. Some proxy players hide their phones inside their elaborate coiffure.

While Macanese law prohibited phone betting in 2001, there was no enforcement as long as operators reported the bets and the identities of the gamblers to the regulator. Proxy betting, therefore, represents high risks for money laundering.