

A world map with a blue background and various countries colored in different shades of yellow, orange, and green. The map is centered on the Atlantic Ocean. The title text is overlaid on the map.

Cross-Border Investment Fraud

2015 Strategic Analysis Report

A study of cross-border investment fraud involving the Philippines as a destination of proceeds from crime and money laundering activities.

Table of Contents

EXECUTIVE SUMMARY	2
I. BACKGROUND OF THE STUDY	4
II. METHODOLOGY	5
II.1. ASSESSMENT METHODOLOGY – TRIGGERED BY SEARCH REQUESTS	5
II.2. ASSESSMENT METHODOLOGY - TRIGGERED BY SUSPICIOUS TRANSACTION REPORTS.....	7
III. DATA AND STATISTICS	9
III. 1. DATA AND STATISTICS EXTRACTED FROM THE CTRs RELATED TO SEARCH REQUESTS	9
III. 2. DATA AND STATISTICS EXTRACTED FROM SUSPICIOUS TRANSACTION REPORTS	17
IV. TYPOLOGIES AND INDICATORS	25
TYPOLOGIES.....	25
INDICATORS AND SUSPICIOUS TRIGGERS	30
V. CONCLUSION	31
ANNEXES	A-1
Annex 1. Actual Currency Value of Remittance PHP Value per Area of Domestic Beneficiary (in reference to Table 3)	A-1
Annex 2: Actual Currency Value of Yearly PHP Value of Remittance per Area of Domestic Beneficiary (in reference to Table 5)	A-2
Annex 3: Actual Currency Value of Yearly PHP Value of Remittances from Presumed Victims per Country of Origin (in reference to Table 7).....	A-4
Annex 4: Actual Currency Value of Yearly PHP Value of Remittances from Possible Associates per Country of Origin” (in reference to Table 8)	A-6

EXECUTIVE SUMMARY

The study on cross-border investment fraud involving the Philippine jurisdiction as destination of the proceeds thereof showed that around PHP4.656 billion was remitted to the Philippines over a 5-year period covering the years 2010 to 2014. The assessment involved reviewing covered transaction reports (CTRs) relating to remittances of identified and suspected fraudsters and their cohorts who/which were subjects of requests for information from other financial intelligence units (FIUs), various domestic and international law enforcement agencies, and the suspicious transaction reports (STRs) which were captured within the parameters used to search the AMLC database on cross-border investment fraud.

A total of 1,718 CTRs on inward remittances with an aggregate amount of PHP4.433 billion, and 178 STRs estimated at PHP222.934 million all relating to cross-border investment fraud proceeds were included in the study. Based on these data, the top five domestic beneficiary locations as shown in the addresses of the perpetrators and their cohorts were identified. The CTR analysis showed that a bulk of the remittances went to the areas of Makati, Pasig, Quezon City, and Butuan, which received PHP3.98 billion or 89.92% of the total remittances through 1,424 remittance transactions or 82.89% of the total volume. On the other hand, PHP178 million or 79.86% of the total estimated proceeds of fraud reported as STRs were siphoned to the areas of Paranaque, Makati, Cavite, Iloilo and Muntinlupa; while in terms of volume, the areas of Paranaque, Makati, Cainta, Taguig and Naga got 113 or 63.48% of the total STRs.

Based on the study, remittances of cross-border investment related funds to accounts in our jurisdiction were made by 1) presumed victims, usually individuals who remit funds as directed by the perpetrators, or 2) possible associates of the perpetrators, in most instances, entities, remitting funds (to the Philippines) received from victims in other jurisdictions. Open source information or Anti-Money Laundering Council Secretariat (AMLCS) assessments indicate that the latter are part of a network of boiler room operators. These would constitute money laundering in the placement and layering stages¹.

¹ RA 9160, as amended by RA 9194, RA 10167 and RA 10365 defines *money laundering* as an act committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity: (a) transacts said monetary instrument or property; (b) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property; (c) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property; (d) attempts or conspires to commit money laundering offenses referred to in paragraphs (a), (b) or (c); (e) aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (a), (b) or (c) above; and (f) performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraphs (a), (b) or (c) above. Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required under the AMLA, as amended, to be reported to the Anti-Money Laundering Council (AMLC), fails to do so.

Money laundering process is comprised of three (3) stages:

- placement or the physical disposal of the criminal proceeds
- layering or the separation of the criminal proceeds from their source by creating layers of financial transactions to disguise the audit trail

Of the PHP4.433 billion peso value of remittances reported as covered transactions, PHP1.958 billion was remitted by presumed victims (placement stage)², while PHP2.474 billion was remitted by possible associates (layering stage)³. The victims are mostly from UK, USA, Malaysia, Australia, and Singapore; while the possible associates remitted funds largely from Singapore, Germany, USA, Indonesia and Hong Kong – constituting the top five jurisdictions.

The schemes of cross-border investment fraud as defined in the study are boiler room, recovery room, and advance fee frauds. The people behind these operations who cold-call potential investors or victims are very deceiving. They present themselves as investment advisors, brokers, lawyers, or accountants with offers of remarkable returns on investments or require outright payment for fees (taxes, liquidation, clearing, or service fees) to be able to recover previous investments.

This study has shown that among the relevant indicators and suspicious triggers of laundering of cross-border investment fraud proceeds are:

1. Accounts are opened with banks for individuals or entities which have just been registered with SEC or DTI. There may be a common signatory for the accounts opened and are usually active for a period of one year. Potential boiler room companies operate within a limited period to avoid detection. Thereafter, a new company with similar nature of business will emerge.
2. Transactions in the domestic account are mostly inward remittances which are immediately withdrawn in cash or by check issuances to different individuals, or wire transferred to another account in the Philippines or overseas, leaving the account with minimal balance.
3. Multiple companies linked by common addresses and common signatories. These companies maintain accounts at different banks to conceal their business activities.
4. Recipients of remittances are individuals or companies having common counterparties or remitters.

The extent of cross-border investment fraud involving our jurisdiction would show that the country is being used as a laundering site for fraudulently acquired funds.

• integration or the provision of apparent legitimacy to the criminal proceeds

Any transaction involving such criminal proceeds or attempt to transact the same during the placement, layering or integration stage shall constitute the crime money laundering.

² *Presumed victims* are remitters usually characterized as individuals not identified with investment fraud scams or whose profile fit that of a victim and send remittances to individuals or entities in this jurisdiction once or over a period of time. Remittances from counterparties/remitters tagged as victims are considered money laundering at the *placement stage*.

³ *Possible fraudsters/associates* are remitters, usually entities or individuals overseas who are suspected to be part of a network of boiler room operators. Remittances from counterparties tagged as suspected fraudsters are presumed to be sending funds to their associates in the Philippines; this can be perceived as *layering stage* of money laundering.

I. BACKGROUND OF THE STUDY

This study will show the extent of cross border investment fraud involving *boiler room operations*, *recovery room*, and *advance fee fraud* in this jurisdiction, particularly, as recipient of fraudulently acquired funds from overseas victims or associates of the perpetrators. The several requests for information on suspected participants in the country from various local and international government agencies, as well as Suspicious Transaction Reports (STRs) in relation to cross-border investment fraud, presented a need to conduct an in-depth study of its impact specifically from an anti-money laundering perspective. The study covers a five-year period starting 2010 until 2014.

The schemes of cross-border investment fraud in this study shall be defined as follows:

- “Boiler Room” is commonly taken from the context of high pressure sales tactics to sell stocks or products to clients who are cold-called, or called randomly, most likely picked out from a telephone directory. It typically refers to a room where salesmen work using unfair, dishonest sales tactics, sometimes selling penny stock, private placements, or committing outright stock fraud.⁴
- “Recovery Room Fraud” refers to a scheme wherein victims of boiler room or other investment scams are contacted by fraudsters offering help in recovering the money they have lost. Further, they will give an assurance that the victim’s original investment is genuine with an offer to buy back or sell the victim’s shares for a good price.⁵
- “Advance fee fraud” is a scheme wherein investors are required to pay fees in advance supposedly as liquidation or service fees, taxes and the like in order to claim proceeds of their investment.⁶

Both *recovery room* and *advance fee frauds* may be considered secondary scams to boiler room since victims of the latter are generally targeted by the same group that operates the *boiler room scam*.

The very nature of cross-border investment fraud initiated by *boiler room operation*, followed through by *recovery room* and *advance fee fraud*, makes it difficult to eliminate. The people behind these operations, who cold-call potential investors or victims, would normally present themselves as investment advisors, brokers, lawyers, or accountants, among others. Furthermore, they would sometimes claim to have overseas

⁴ Boiler room definition from the following websites:

<<http://www.investopedia.com/terms/b/boilerroom.asp>>
<<http://www.investopedia.com/ask/answers/04/080604.asp>>
<[https://en.wikipedia.org/wiki/Boiler_room_\(business\)](https://en.wikipedia.org/wiki/Boiler_room_(business))>

⁵ Recovery room fraud definition from UK Financial Services Authority website

<http://www.fsa.gov.uk/consumerinformation/scamsandwindles/investment_scams/recovery_room>

⁶ Advance fee fraud characteristics gathered from the U.S. Securities and Exchange Commission website

<<https://www.sec.gov/answers/advancefeefraud.htm>>

branches rendering a sense of legitimacy and prominence. They are also very compelling with offers of remarkable returns on investments. They mostly target wealthy professionals, business people, and the elderly with pensions, who desire to earn good returns. They would also target prior victims with a promise of investment recovery, while typically discounting the risks associated with the offer.

II. METHODOLOGY

Strategic descriptive analysis applies various techniques, usually quantitative, to summarize, extract patterns, and produce high-level information on detailed data, reports, etc. For this study, the AMLCS used this type of descriptive research in determining the impact of cross border investment fraud and the money laundering scheme involved in the Philippines.

The study covers those subjects identified in the requests for information and STRs received by the AMLCS for the period 2010 – 2014. The Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) culled from the AMLC database on these subjects, considered as first level or main subjects, were evaluated and included in this study. The data will be presented in two parts: first will be the CTRs involving international inward remittances (“international remittances”) of investment fraud participants as indicated in the requests for information from international counterparts of the AMLC, domestic law enforcement agencies (LEAs) and international LEAs pursuant to Mutual Legal Assistance Treaty (MLAT); and second, the STRs submitted by domestic covered persons which were captured using the cross-border investment fraud parameters to search the database.

II.1. ASSESSMENT METHODOLOGY – TRIGGERED BY SEARCH REQUESTS

For the period 2010 – 2014, a total of thirty-five (35) requests for information on cross-border investment fraud involving boiler room, recovery room and advance fee fraud from various local and foreign government agencies/requestors were assessed. These requests contained a substantial number of confirmed and suspected scammers, their associates and presumed victims. AMLCS hypothesized that all transactions involving these subjects, which are of similar nature to the ones used to defraud victims, are likely fraudulent and therefore included in this study.

Covered transaction reports (CTRs) on these individuals and entities were assessed and filtered to zero in on international remittances. CTRs were further filtered to limit the fields to those data relevant to the study specifically:

- **Names of overseas senders and domestic beneficiaries** – collated from the “Name” and “Other Name” fields of the CTRs. The senders were further grouped into two categories, either as (1) presumed victims or (2) perpetrators or their associates. Categorization of senders/counterparties was determined based on their participation as described in the requests for information sent to the AMLC or findings of the analysts. However, for purposes of this study, victims, perpetrators or their associates will not be identified as emphasis was given on the locations and amounts involved.
- **Location of presumed victims and deemed associates of suspected scammers** – these were gathered from the “Other Address” field of the CTRs that contain the counterparty or sender’s address. In the absence of such data, the country indicated in the “Correspondent Bank Address” field was used considering that it is the only known location where the funds came from before entering our jurisdiction.
- **Location of domestic beneficiaries (suspected scammers or their associates)** – these were gathered from the “Address” and “Other Address” fields of the CTRs
- **Transaction period** – covers the years the transactions being assessed were transacted; the actual transaction dates were converted to transaction year for purposes of this study
- **Transaction Amount** – there were six currencies used by the perpetrators as indicated in the assessed CTRs, namely: Philippine Peso (PHP), US Dollars (USD), Euro (EUR), Great Britain Pound (GBP), Swiss Franc (CHF), and Japanese Yen (JPY). (The figures in their actual currencies are presented as annexes to this report.) The PHP currency was used in the main report to facilitate comparison; transaction amounts in other currencies were converted to PHP based on the average conversion rate for 2010 – 2014 as shown in table 1 below.

Table 1: Average Conversion Rate of PHP

YEARLY AVERAGE COVERSION ⁷ RATE TO PHP FOR THE PERIOD 2010 – 2014					
YEAR	USD	EUR	GBP	CHF	JPY
2010	45.0865970	59.8248650	69.6739790	43.2940640	0.5141510
2011	43.2842400	60.2656800	69.4334320	48.9587940	0.5423360
2012	42.2029970	54.2463140	66.8508460	45.0009820	0.5295310
2013	42.4421620	56.4201830	66.4468130	45.8261750	0.4352560
2014	44.3992420	59.0052500	73.1410940	48.5706370	0.4205000
AVERAGE RATE USED	43.4830476	57.9524584	69.1092328	46.3301304	0.4883548

⁷ Conversion rates based on <<http://www.usforex.com/forex-tools/historical-rate-tools/yearly-average-rates>>

Filtered CTRs regarding international remittance with omitted or erroneous data, i.e., without sender address and correspondent bank details, were not included in the study.

If the remittance was reported both as a covered transaction and suspicious transaction and the STR was captured using the parameters formulated to search the database for purposes of this study then only the figures in the STR were used; otherwise, CTR figures were used.

The study also considered particular details in the various requests for information such as the nature of fraud, requesting party, and the year when the request was sent. These were used in the typologies and indicators of cross border investment fraud and the laundering of the proceeds thereof.

II.2. ASSESSMENT METHODOLOGY - TRIGGERED BY SUSPICIOUS TRANSACTION REPORTS

For purposes of this study, only cross-border investment fraud STRs on suspected *boiler room operations*, *advance fee fraud* and *recovery scams* were considered. AMLC queried electronically filed STRs with predicate crimes “Swindling” and “Violation of Securities Regulation Act of 2000” for the period 2010 to 2014, and STRs filed for specific suspicious circumstances defined under Section 3-b1 of the AMLA such as:

- (1) *There is no underlying legal or trade obligation, purpose, or economic justification;*
- (2) *The client is not properly identified;*
- (3) *The amount involved is not commensurate with the business or financial capacity of the client; and*
- (4) *There is a deviation from the client’s profile/past transactions.*

To drill down into *boiler room*, *recovery room* and *advance fee fraud* STRs, AMLC queried the cross-border investment fraud STRs by year from 2010 – 2014 containing the terms boiler room, recovery room and advance fee fraud in the *Narrative* and *Reason for Suspicion* portion of the report.

However, there were STRs found to possess the criteria on cross-border investment fraud but their narratives did not provide details of crime or money laundering activity. Such STRs were classified as *Suspected Boiler room/Advance fee fraud*.

Additional parameters in the beneficiary's and counterparty/remitter's addresses, correspondent bank and country code fields were also utilized to capture cross-border transactions. The counterparties were also categorized either as victim or fraudster

depending on their participation as narrated in the STR. This process yielded one hundred seventy-eight (178) STRs which were further evaluated in order to capture other information not specified in the data fields of the STRs such as beneficiary and counterparty. The narrative fields of the STRs were also looked into for further information on the remitter and beneficiary.

Other key information from the STRs that were used in the study:

- **Names and locations of suspected associates or beneficiaries of the proceeds of cross-border fraud** - The accountholder/subject of the STR and beneficiary data fields are initially presumed as associates unless indicated otherwise in the “Reason for Suspicion” and “Narrative” fields.
- **Names and locations of the presumed victims or fraudsters** – These pieces of information are captured from the “Counterparty and Other Participant” data fields or from the “Reason for Suspicion” or “Narrative” data fields.
- **Amount of proceeds** – The amount of the proceeds is taken from the transaction amount field and in the narrative field, if any, of the STRs.

However, twenty (20) STRs reflected no estimates on the value of proceeds and used PHP1.00 as transaction amount. These STRs with transaction amount of PHP1.00 were not included in the analysis of the amount of proceeds. For consistency, the peso-equivalent of the currency amount is used.

III. DATA AND STATISTICS

Following are the analyses and statistics of the CTRs and STRs covered in this study.

III. 1. DATA AND STATISTICS EXTRACTED FROM THE CTRs RELATED TO SEARCH REQUESTS

The volume of domestic and international requests for information on cross-border investment fraud from 2010 to 2014 is shown in Table 2.

Table 2: Volume of Search Requests

VOLUME OF ESW/MLAT/LEA REQUEST For the Period 2010 - 2014	
DOMESTIC	
AGENCIES	VOLUME
PCTC - INTERPOL MANILA - NCBS ⁸	6
SEC ⁹	5
NBI ¹⁰ - MANILA	3
PNP - CIDG - ATCD ¹¹	2
BSP - FCAG ¹²	1
Total Domestic Requests	17
INTERNATIONAL	
AGENCIES/REQUESTOR	VOLUME
UNITED KINGDOM - FIU ¹³	4
SINGAPORE - INTERPOL	2
USA – thru MLAT ¹⁴	2
BANK NEGARA MALAYSIA	1
JAFIC (JAPAN) – FIU	1
MOKAS (CYPRUS) – FIU	1
MALAYSIA - PERSONAL E-MAIL FROM VICTIM	1
SWITZERLAND – thru MLAT	1
BELGIUM – FIU (CTIF-CFI)	1
US - FINCEN via ESW ¹⁵	1
WIESBADEN (GERMANY) - INTERPOL	1
MAURITIUS – FIU via ESW	1
MACAO – FIU (GIF)	1
Total International Requests	18
Grand total Domestic & International	35

Certain requests from domestic agencies, i.e., PCTC-Interpol Manila-NCBS and SEC, were mostly on behalf of their foreign counterparts.

⁸ Philippine Center on Transnational Crime (PCTC) – International Police (INTERPOL) Manila – National Central Bureau Secretariat (NCBS)

⁹ Securities and Exchange Commission (SEC)

¹⁰ National Bureau of Investigation (NBI) – Manila

¹¹ Philippine National Police (PNP) – Criminal Investigation and Detection Group (CIDG) – Anti-Transnational Crime Division (ATCD)

¹² Bangko Sentral ng Pilipinas (BSP) – Financial Consumer Affairs Group (FCAG)

¹³ Financial Intelligence Unit (FIU)

¹⁴ Mutual Legal Assistance Treaty (MLAT)

¹⁵ Electronic Secure Website (ESW)

In the evaluation of the various search requests for information covered by this study, we were able to identify sixty-eight (68) domestic beneficiaries, four hundred ninety-nine (499) foreign individual victims, and fifty-two (52) possible foreign associates of domestic beneficiaries.

CTR Analysis

Exported database output on the subjects, associates and victims of investment fraud yielded a total of 1,718 CTRs that involved remittances. These remittances amounted to PHP4.43 billion from 2010 to 2014 which went to specific areas in the country. Table 3 shows the total remittances in terms of volume and PHP value over a five-year period (2010 – 2014).

Table 3: Remittance PHP Value and Volume per Location of Domestic Beneficiary

CITY / PROVINCE	REMITTANCE PHP VALUE	PERCENTAGE	REMITTANCE VOLUME	PERCENTAGE
MAKATI	1,159,540,412.09	26.15%	365	21.25%
PASIG	1,064,982,363.78	24.02%	410	23.86%
QUEZON CITY	745,010,581.46	16.80%	99	5.76%
CEBU	721,863,685.12	16.28%	380	22.12%
BUTUAN	295,593,928.90	6.67%	170	9.90%
PARAÑAQUE	121,033,817.64	2.73%	72	4.19%
BAGUIO	113,991,399.78	2.57%	63	3.67%
MUNTINLUPA	89,170,255.00	2.01%	69	4.02%
ANGELES	52,920,855.48	1.19%	36	2.10%
PANGASINAN	28,931,995.13	0.65%	17	0.99%
RIZAL	22,022,288.19	0.50%	22	1.28%
MANILA	8,680,789.95	0.20%	4	0.23%
LAGUNA	6,824,096.87	0.15%	8	0.47%
CAVITE	2,332,813.15	0.05%	2	0.12%
PASAY	839,572.50	0.02%	1	0.06%
Grand Total	4,433,738,855.03	100.00%	1,718	100.00%

The table above shows that majority of the remittances went to the areas of Makati, Pasig, Quezon City, Cebu, and Butuan, which got PHP3.98 billion or 89.92% of the total remittances in terms of PHP value; and 1,424 remittance transactions or 82.89% in terms of volume. This may indicate the location of the perpetrators or their cohorts.

The succeeding tables and graphs show the total remittances presented annually for each beneficiary location. Table 4 and graph 1 show the volume; while table 5 and graph 2 show the PHP value of these remittances.

Table 4: Yearly Volume of Remittances per Area of Domestic Beneficiary

CITY / PROVINCE	2010	2011	2012	2013	2014	TOTAL VOLUME
PASIG	56	32		8	314	410
CEBU	15	43	258	39	25	380
MAKATI	104	30	128	52	51	365
BUTUAN	32	28	49	44	17	170
QUEZON CITY			46	53		99
PARAÑAQUE		1	43	28		72
MUNTINLUPA			6	17	46	69
BAGUIO		43	20			63
ANGELES	11	22		2	1	36
RIZAL				1	21	22
PANGASINAN				10	7	17
LAGUNA		2	1	5		8
MANILA		2			2	4
CAVITE					2	2
PASAY				1		1
Grand Total	218	203	551	260	486	1,718

**Highlighted above are the top 3 locations per year in terms of volume of remittances*

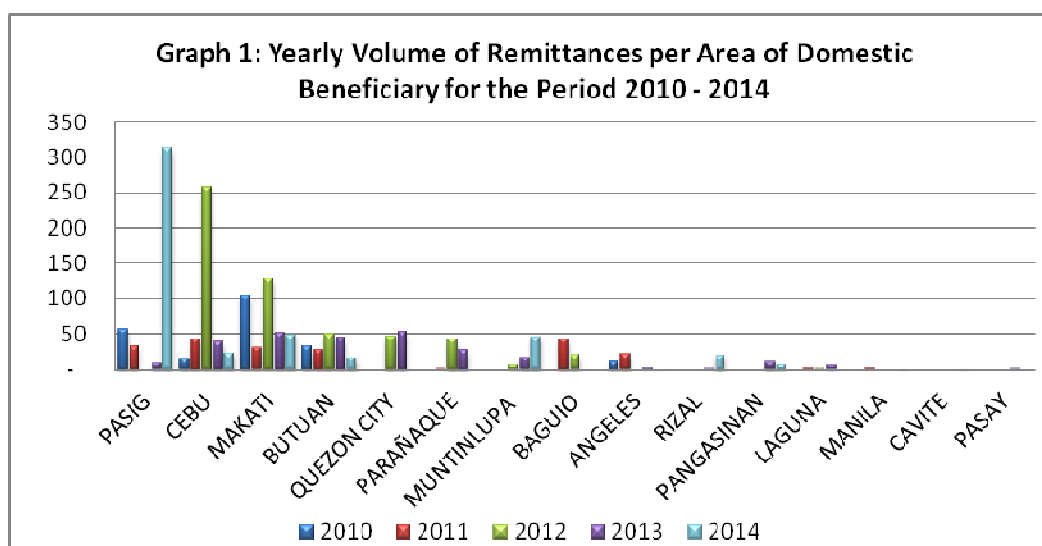


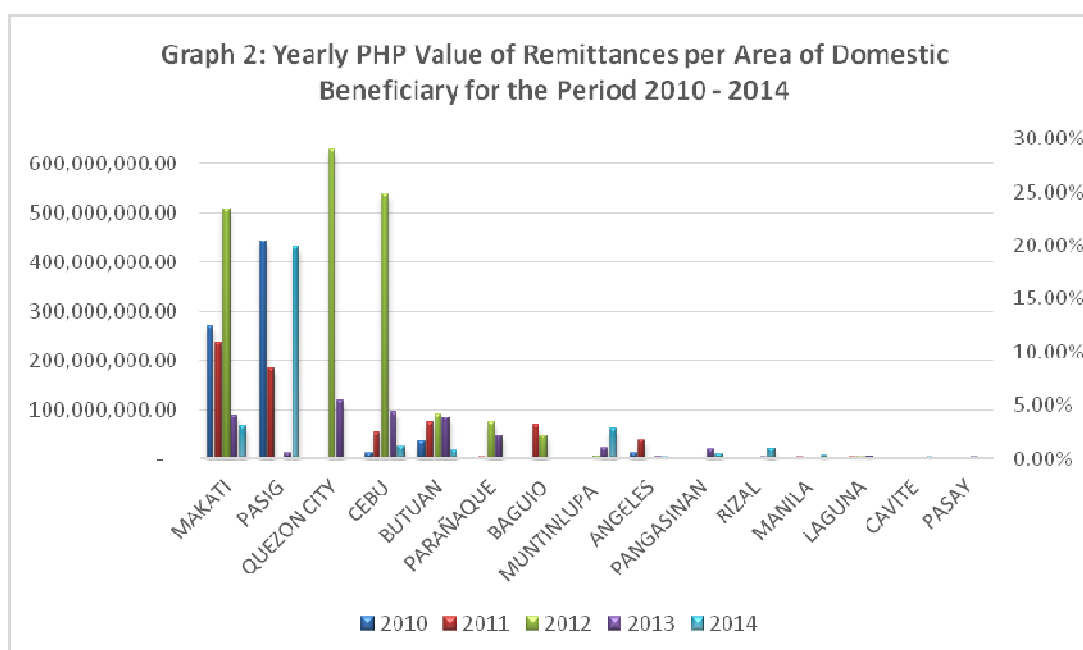
Table 4 and graph 1 above show five cities with the highest volume of remittances for 2010 to 2014 – Pasig, Cebu, Makati, Butuan and Quezon City. On a yearly basis, the top three areas with the highest volume of remittance were among the said five cities. Pasig ranked 2nd in 2010 and 2011, and 1st in 2014; Cebu ranked 1st both in 2011 and 2012; Makati ranked 1st in 2010, 3rd in 2011, and 2nd in 2012 to 2014; Butuan consistently ranked 3rd in 2010 to 2013; Quezon City ranked 1st in 2013; only two areas namely, Baguio which ranked 1st along with Cebu in 2011, and Muntinlupa which ranked 3rd in

2014, were not among the top five cities in the overall ranking. It was noted that Makati, Cebu and Butuan were consistent recipients of remittances from 2010 – 2014.

Table 5: Yearly PHP Value of Remittances per Area of Domestic Beneficiary

CITY / PROVINCE	2010	2011	2012	2013	2014	TOTAL PHP VALUE
MAKATI	267,821,529.48	233,493,628.33	505,347,916.12	87,036,139.00	65,841,199.15	1,159,540,412.09
PASIG	441,038,118.38	182,147,726.46		12,682,075.64	429,114,443.29	1,064,982,363.78
QUEZON CITY			628,354,090.03	116,656,491.42		745,010,581.46
CEBU	12,190,116.27	53,214,268.84	537,864,186.92	94,157,196.82	24,437,916.28	721,863,685.12
BUTUAN	33,969,330.74	73,002,097.14	89,595,734.68	82,938,459.65	16,088,306.70	295,593,928.90
PARAÑAQUE		1,303,926.15	74,001,553.25	45,728,338.25		121,033,817.64
BAGUIO		67,267,017.54	46,724,382.24			113,991,399.78
MUNTINLUPA			6,045,983.28	22,033,985.99	61,090,285.73	89,170,255.00
ANGELES	12,066,110.88	35,783,286.95		3,329,942.64	1,741,515.02	52,920,855.48
PANGASINAN				19,917,899.40	9,014,095.73	28,931,995.13
RIZAL				1,621,102.37	20,401,185.82	22,022,288.19
MANILA		1,715,928.02			6,964,861.93	8,680,789.95
LAGUNA		2,398,449.68	520,709.50	3,904,937.69		6,824,096.87
CAVITE					2,332,813.15	2,332,813.15
PASAY				839,572.50		839,572.50
ANNUAL TOTALS	767,085,205.75	650,326,329.11	1,888,454,556.02	490,846,141.37	637,026,622.78	4,433,738,855.03

*Highlighted above are the top 3 locations per year in terms of value of remittances



The remittances in terms of PHP value as shown in table 5 and graph 2 likewise showed that most of the five cities with the highest value of remittances were also the annual top 3 beneficiary areas. Makati ranked 2nd in 2010 and 2014, 1st in 2011, and 3rd in 2012 and 2013; Pasig ranked 1st in 2010 and 2014, and 2nd in 2011; Quezon City ranked 1st both in 2012 and 2013; Butuan ranked 3rd both in 2010 and 2011; Cebu ranked 2nd in 2012 and 2013; while Muntinlupa, which ranked 3rd in 2014, was not included in the overall top 5 ranking.

There were sixty-eight (68) domestic beneficiaries (individuals / entities) identified. They were grouped according to the city or province indicated in their addresses. Table 6 shows the areas of concentration of identified and presumed fraudsters and their associates.

Table 6: Number of Domestic Beneficiaries and their Respective Location

CITY / PROVINCE	DOMESTIC BENEFICIARIES	PERCENTAGE
CEBU	15	22.06%
MAKATI	14	20.59%
BUTUAN	11	16.18%
QUEZON CITY	7	10.29%
BAGUIO	3	4.41%
MUNTINLUPA	3	4.41%
PASIG	3	4.41%
ANGELES	2	2.94%
LAGUNA	2	2.94%
MANILA	2	2.94%
PARAÑAQUE	2	2.94%
CAVITE	1	1.47%
PANGASINAN	1	1.47%
PASAY	1	1.47%
RIZAL	1	1.47%
Grand Total	68	100.00%

82.35% of the total beneficiaries or fifty-six (56) beneficiaries are located in the top five (5) cities - Cebu, Makati, Butuan, and Quezon City are the top four (4), while Baguio, Muntinlupa and Pasig were tied on the 5th spot. This could indicate the preferred locations of the perpetrators or their cohorts.

Patterns seem to indicate that the senders or counterparties of the remittances are the victims (usually individual remitters) and possible associates (usually entities) of domestic beneficiaries. Classification of the remitters as victims or associates would indicate the stages of money laundering.

AMLC hypothesized that the remittances of those identified as presumed victims constitute the placement stage. This means that the fraudulently acquired funds solicited from victims were remitted directly to the scammers or their associates located in this jurisdiction.

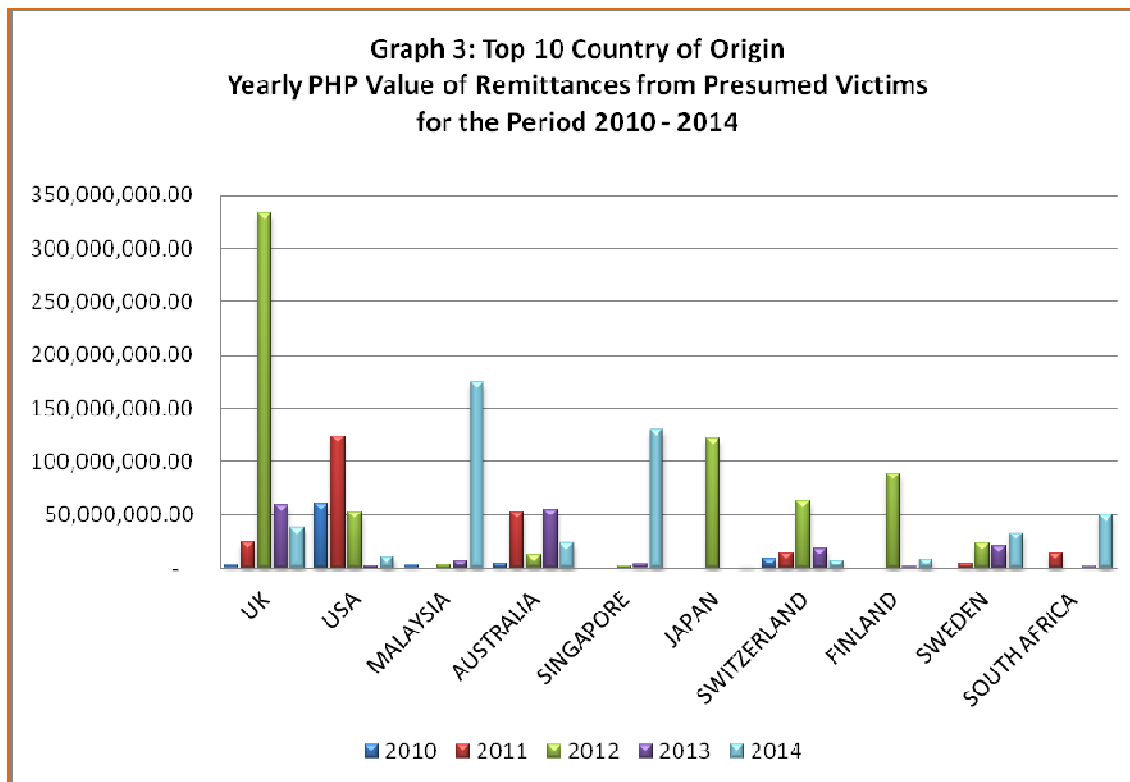
Table 7 shows the total annual remittances of presumed victims per country of origin; this is graphically depicted in Graph 3.

Table 7: Yearly PHP Value of Remittances from Presumed Victims per Country of Origin

COUNTRY	2010	2011	2012	2013	2014	Grand Total
UK	2,273,772.04	24,402,104.08	333,025,748.27	59,343,308.90	38,697,254.98	457,742,188.26
USA	60,592,880.66	123,429,114.80	52,464,762.42	2,149,050.50	9,922,433.27	248,558,241.65
MALAYSIA	2,867,177.37		2,922,258.37	6,513,640.95	174,116,549.39	186,419,626.08
AUSTRALIA	4,259,599.34	52,608,368.23	11,480,963.86	54,687,054.01	23,480,180.68	146,516,166.12
SINGAPORE			2,223,070.81	3,531,171.33	129,769,427.31	135,523,669.45
JAPAN			121,330,303.32		3,005,665.22	124,335,968.54
SWITZERLAND	8,770,530.70	13,759,684.70	63,103,561.33	18,511,770.43	6,574,528.09	110,720,075.26
FINLAND			88,610,471.87	1,380,782.44	8,667,566.76	98,658,821.06
SWEDEN		4,354,202.37	23,238,069.20	21,033,656.44	32,400,347.74	81,026,275.74
SOUTH AFRICA		14,101,053.15		1,715,380.00	50,426,169.74	66,242,602.89
NEW ZEALAND			14,293,730.76	8,006,763.98	27,596,676.55	49,897,171.29
HONG KONG			44,318,768.73	1,645,725.95	3,833,468.09	49,797,962.76
AUSTRIA		1,302,034.64	41,696,763.13	709,730.30		43,708,528.07
BELGIUM			35,583,895.87	1,107,034.91		36,690,930.78
NORWAY			16,419,191.82	777,932.16	3,587,351.43	20,784,475.40
IRELAND		688,876.27	14,907,398.00		934,668.11	16,530,942.38
SAUDI ARABIA			12,166,130.58			12,166,130.58
NETHERLANDS				4,237,713.46	6,728,028.47	10,965,741.92
INDONESIA				1,621,102.37	8,200,954.96	9,822,057.33
CANADA			7,318,462.59		1,562,324.16	8,880,786.75
KUWAIT					7,458,074.48	7,458,074.48
ITALY					7,146,838.48	7,146,838.48
GERMANY			3,047,506.55		3,448,372.74	6,495,879.29
DENMARK			6,354,769.12			6,354,769.12
SPAIN					5,409,251.99	5,409,251.99
RUSSIA					3,342,541.87	3,342,541.87
UAE				3,217,093.28		3,217,093.28
ISRAEL				1,039,331.80	1,549,083.57	2,588,415.37
SLOVENIA				526,767.84	593,926.25	1,120,694.09
KENYA			650,723.81			650,723.81
Grand Total	78,763,960.11	234,645,438.22	895,156,550.40	191,755,011.04	558,451,684.31	1,958,772,644.09

*Highlighted above are the top 3 countries per year

As can be gleaned from the table above, there has been a relentless increase in remittances from presumed victims of cross-border investment fraud from 2010 – 2012 which spiked to PHP895.15 million in 2012 from PHP234.64 million in 2011; dropped to PHP191,755,011.04 in 2013 and rose again in 2014 to P558.45 million. The several alerts and warnings posted on investment fraud did not seem to hamper the activities of the scammers. It is possible that these scammers are also continuously re-inventing the manner of approaching previous and prospective victims in order to perpetuate the scam.



The graph above illustrates that for the period 2010 to 2013 majority of victims were from European countries, the USA and Australia; the only Asian country was Japan, which ranked 2nd in 2012. However, in 2014 a significant increase in remittances from presumed victims shifted to Asia particularly Malaysia and Singapore, and the region of South Africa. This may indicate future trend in so far as jurisdiction of victims is concerned.

AMLC hypothesized that remittances from possible associates is the *layering stage* of cross-border investment fraud. This means that the victims initially remitted the payment for the pseudo investment to an entity in the source country which then transferred the funds to our jurisdiction via international remittance.

Table 8 shows the total annual remittances of possible associates per country of origin with graphical presentation shown in graph 4.

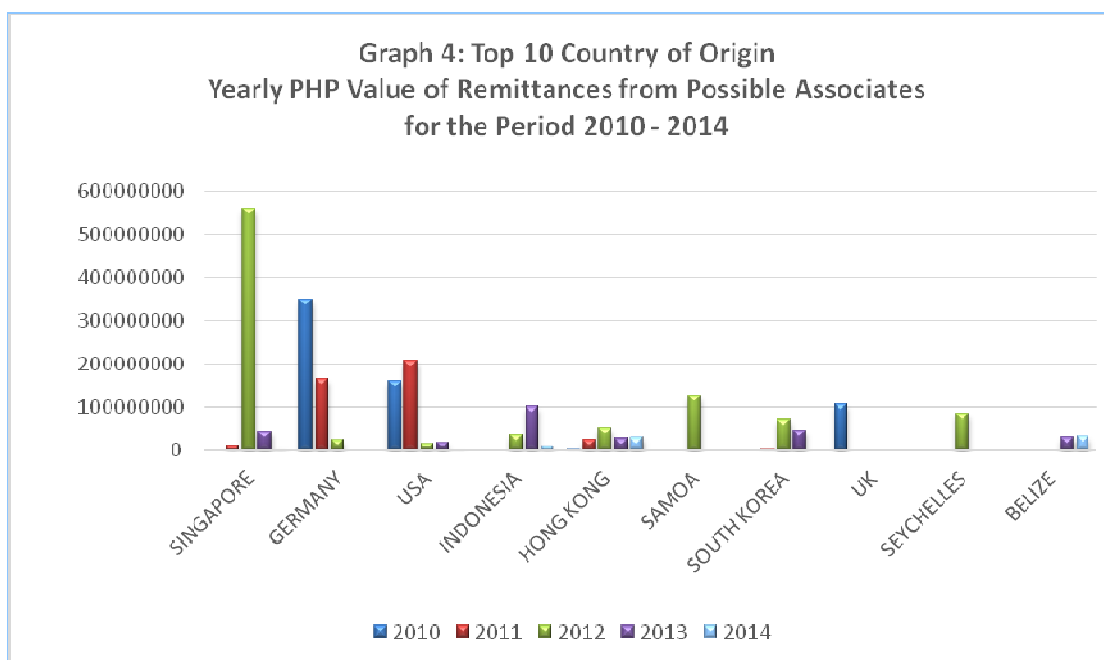
Table 8: Yearly PHP Value of Remittances from Possible Associates per Country of Origin

COUNTRY	2010	2011	2012	2013	2014	Grand Total
SINGAPORE		10,024,459.17	559,692,539.85	42,609,517.45	5,333,046.81	617,659,563.28
GERMANY	348,270,081.57	163,599,571.00	22,769,293.15			534,638,945.73
USA	159,797,055.67	205,980,784.92	13,922,431.75	17,558,361.13	2,460,662.18	399,719,295.65
INDONESIA			35,366,925.17	100,016,803.60	8,956,882.52	144,340,611.28
HONG KONG	1,292,046.58	23,913,936.86	51,673,644.90	26,581,679.23	29,069,036.35	132,530,343.90
SAMOA			124,921,044.37			124,921,044.37
SOUTH KOREA		1,303,926.15	69,731,923.23	45,728,338.25		116,764,187.63
UK	107,686,142.61					107,686,142.61
SEYCHELLES			82,949,520.55			82,949,520.55
BELIZE				28,878,812.97	29,698,203.17	58,577,016.14
JAPAN	45,460,459.98	8,299,589.83				53,760,049.80
FRANCE	6,389,607.73	2,558,622.96		29,855,143.49	2,389,958.75	41,193,332.93
SWITZERLAND			11,127,438.85	7,862,474.22	667,148.70	19,657,061.77
HOLLAND			12,699,962.52			12,699,962.52
MACAU	10,859,021.48					10,859,021.48
SPAIN	8,048,712.11					8,048,712.11
MALAYSIA	518,117.91		7,142,138.05			7,660,255.96
AUSTRALIA			1,301,143.23			1,301,143.23
Grand Total	688,321,245.64	415,680,890.89	993,298,005.62	299,091,130.33	78,574,938.47	2,474,966,210.95

**Highlighted above are the top 3 countries per year*

As above table illustrates, remittances from possible associates in the year 2010 was a high of PHP688.32 million. This dropped to PHP415.68 million but doubled in 2012 at PHP993.29 million. The years 2013 and 2014 showed a significant continuing decline in the remittances from possible associates.

The total remittances from perpetrators or associates amounting to PHP2.474 billion are significantly higher than the total remittances from victims (PHP1.958 billion). However, a yearly analysis showed a massive increase of remittances from presumed victims as supported by the 2014 figures indicated in table 7 - yearly remittances from presumed victims (PHP558.45 million) as against the 2014 figures of PHP78.57 million from perpetrators or associates. A future trend may suggest that the scammers are exploiting the Philippine jurisdiction more as a direct beneficiary location of funds from presumed victims. There is also a high probability that the ultimate beneficiaries including foreign nationals are domiciled in our jurisdiction.



The above graph illustrates that in 2010 and 2011 Germany and the USA are consistently in the top spots of intermediary locations of funds prior to entering the Philippine jurisdiction; the UK landed in the 3rd spot in 2010 and Hong Kong also in the 3rd spot in 2011. Conversely, the period 2012 to 2014 exhibited a sporadic trend with various Asian countries, particularly Singapore, Indonesia, Hong Kong, and South Korea, belonging to the top 3 sources of funds from possible associates. Other nations, i.e. Seychelles – located in Africa, Samoa – part of Polynesia, and Belize – located in the Caribbean Coast of Northern Central America, were also in the top 3 intermediary locations of funds from 2012 to 2014.

III.2. DATA AND STATISTICS EXTRACTED FROM SUSPICIOUS TRANSACTION REPORTS

Table 9 depicts that from 2010 – 2014, AMLC received 178 cross-border investment fraud STRs relating to forty-five (45) accountholders, thirty-six (36) beneficiaries and thirty (30) counterparties/remitters.

For the period 2010 to 2014, 70.79% of the STRs on cross-border investment fraud or one hundred twenty-six (126) STRs were filed under the predicate crime SWINDLING. There were only thirteen (13) STRs under Suspected Boiler room/Advance fee fraud category, however, the amount involved appeared to be significant accounting for 14.72% of the total estimated amount in peso value. Table 9 shows the volume and value of cross-border related STRs per predicate crime.

Table 9. Suspicious Transaction Reports per Predicate Crime and Suspicious Circumstance

<i>Cross-Border Investment Fraud-Related STRs, 2010-2014</i>			
Predicate Crime/ Suspicious Circumstance	Predicate Crime Sub-Classification	Volume of STRs	Estimated Amount Involved, in Peso value
FRAUDULENT PRACTICES AND OTHER VIOLATIONS UNDER THE SECURITIES REGULATIONS CODE OF 2000	Boiler room	33	18,186,086.96
SWINDLING	Advance fee fraud	72	85,432,612.60
	Boiler room	23	59,613,464.77
	Recovery room/ Advance fee fraud	18	7,265,688.52
	Suspected boiler room/advance fee fraud	13	32,822,900.00
THE AMOUNT INVOLVED IS NOT COMMENSURATE WITH THE BUSINESS OR FINANCIAL CAPACITY OF THE CLIENT	Advance fee fraud	1	135,856.76
	Boiler room	15	6,728,884.49
THERE IS NO UNDERLYING LEGAL OR TRADE OBLIGATION, PURPOSE OR ECONOMIC JUSTIFICATION	Advance fee fraud	1	3,984,098.86
	Boiler room	2	8,764,700.14
Total		178	222,934,293.10

Table 10 below shows that the highest volume of cross-border investment fraud STRs were filed in 2011 and 2014 with 33.71% and 34.27%, respectively, of the total cross border investment fraud STRs from 2010 – 2014. The STR trend also indicates *boiler room operation* as one of the main tactics/schemes being exploited by criminals.

Table 10. Number of Cross-Border Investment Fraud–Related STRs from 2010-2014

Type of Fraud	2010	2011	2012	2013	2014	Volume of STRs
Advance fee fraud		44	2		28	74
Boiler room	1	16	7	29	20	73
Recovery room/Advance fee fraud				18		18
Suspected boiler room/advance fee fraud					13	13
Total STRs	1	60	9	47	61	178
% of Total STRs	0.56%	33.71%	5.06%	26.40%	34.27%	

Graph 5 below depicts that the value of cross border investment fraud proceeds, mostly from the advance fee fraud scheme peaked in 2014, a sharp increase of 884% from the 2013 value of PHP15.29 million.

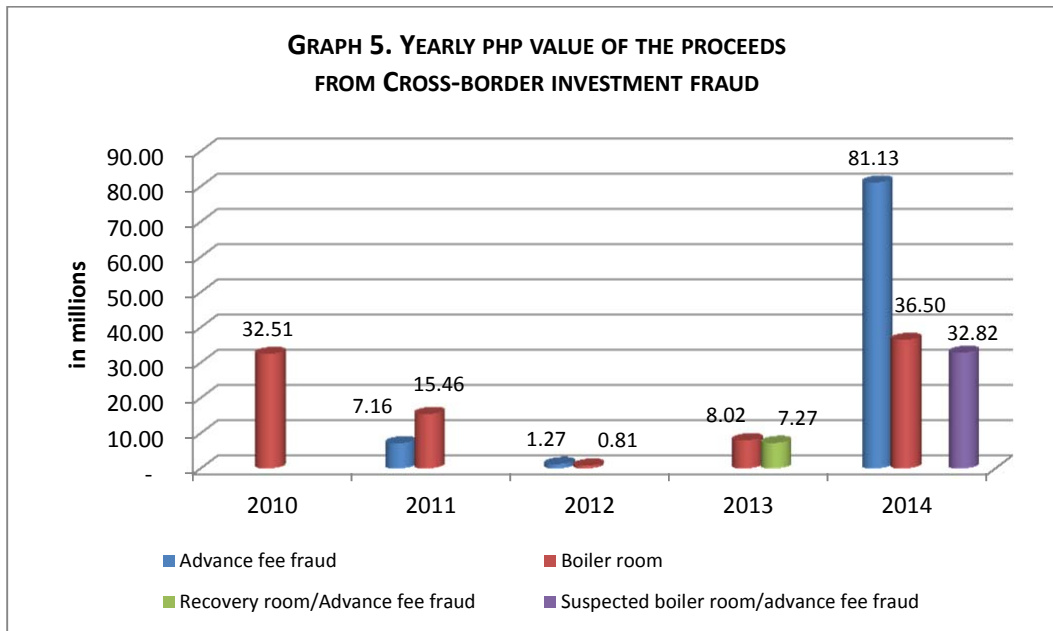


Table 11 and figure 1 show the countries where the cross border investment fraud proceeds originated in terms of volume of STRs. Among the major sources of remittances are Canada, Singapore and USA. Out of the one hundred seventy-eight (178) cross border investment fraud STRs, nine (9) did not have details of the remitters while ninety-one (91) did not have any information on the source of remittances.

Table 11. Volume of STRs per Location of Counterparty

Location of Counterparty	Counterparty's alleged Participation in the Transaction	No. of STRs
Canada	Presumed victim	32
Singapore	Suspected fraudster/associate	18
	Presumed victim	10
United States of America	Presumed victim	7
	Suspected fraudster/associate	3
Indonesia	Presumed victim	2
Netherlands	Presumed victim	2
Bahamas	Suspected fraudster/associate	1
Europe	Presumed victim	1
Japan	Presumed victim	1
Zimbabwe	Presumed victim	1
Sub Total		78
No address details provided on the remitter	Presumed victim	9
<i>No information obtained on the source of remittances or proceeds of fraud</i>		91
Total		178



**Figure 1. Source Country of Remittances/Proceeds
from Cross-Border Investment Fraud**

The remitters/counterparties are classified either as *presumed victims* or *suspected fraudsters/associates*. Presumed victim remitters are usually characterized as individuals not identified with investment fraud scams or whose profile fit that of a victim, who make remittances to individuals or entities in this jurisdiction once or over a period of time. The transactions of the recipients (identified with the fraudsters) are remittances from various individuals in foreign jurisdictions. Suspected fraudsters/associates remitters are usually entities or individuals overseas who, based on open source information or cross border investment fraud evaluation, are suspected to be part of a network of boiler room operators. This classification is useful in determining the stage of money laundering perpetrated. Remittances from counterparties/remitters tagged as victims are considered money laundering at the *placement stage*. Remittances from counterparties tagged as suspected fraudsters are presumed to be sending funds to their associates in the Philippines; this can be perceived as *layering stage* of money laundering.

Figure 2 shows that some of the remittances to the Philippines passed through banks and remittance agents situated in Belgium, Canada, USA, Hongkong and Singapore. Based on the data collected, only 43.82% or 78 out of 178 STRs contained information on correspondent bank.



Figure 2. Country of Correspondent Bank

Table 12. Volume and PHP Value of Cross-border Investment Fraud per Location of Beneficiary

Location	Volume of STRs	% of STRs	Estimated Amount Involved, in Peso value	% of Amount
Paranaque City	25	14.04%	47,535,089.77	21.32%
Makati City	20	11.24%	42,116,630.00	18.89%
Cavite	11	6.18%	40,212,725.00	18.04%
Iloilo	1	0.56%	32,505,004.40	14.58%
Muntinlupa	3	1.69%	15,669,676.61	7.03%
Cebu	2	1.12%	11,276,173.00	5.06%
Pampanga	8	4.49%	8,422,618.65	3.78%
Cainta	18	10.11%	7,265,688.52	3.26%
Taguig City	18	10.11%	6,100,000.00	2.74%
Quezon City	5	2.81%	3,984,098.86	1.79%
Subic	10	5.62%	2,573,247.00	1.15%
Butuan	12	6.74%	2,258,270.72	1.01%
Benguet	6	3.37%	1,754,283.26	0.79%
Pasig	5	2.81%	797,140.88	0.36%
Naga City	32	17.98%	463,143.32	0.21%
Manila	1	0.56%	503.11	0.00%
Marikina	1	0.56%		
Total	178	100.00%	222,934,293.10	100.00%

Table 12 above illustrates the number of STRs per location of the domestic beneficiaries. The top three (3) cities for 2014 in terms of volume of STRs and estimated value of proceeds are Makati City, Paranaque City and Cavite. In 2013, Cainta and Taguig ranked 1st and 2nd in terms of volume and value of proceeds.

For the period covered by the study, 79.86% of the cross border investment fraud proceeds or PHP178 million was received by beneficiaries situated in Paranaque City, Makati City, Cavite, Iloilo and Muntinlupa. In terms of volume of STRs, Naga City ranked 1st with thirty-two (32) STRs while Paranaque City and Makati City ranked 2nd and 3rd with twenty-five (25) and twenty (20) STRs, respectively. While Butuan and Benguet were not in the top 5 domestic locations in terms of volume and value of STRs, the provinces however were recurrent destination of cross-border investment fraud proceeds. Butuan was a destination from 2011 to 2014 and Benguet from 2012-2014. Table 13 and Graph 6 below show the number of STRs per area of domestic beneficiary.

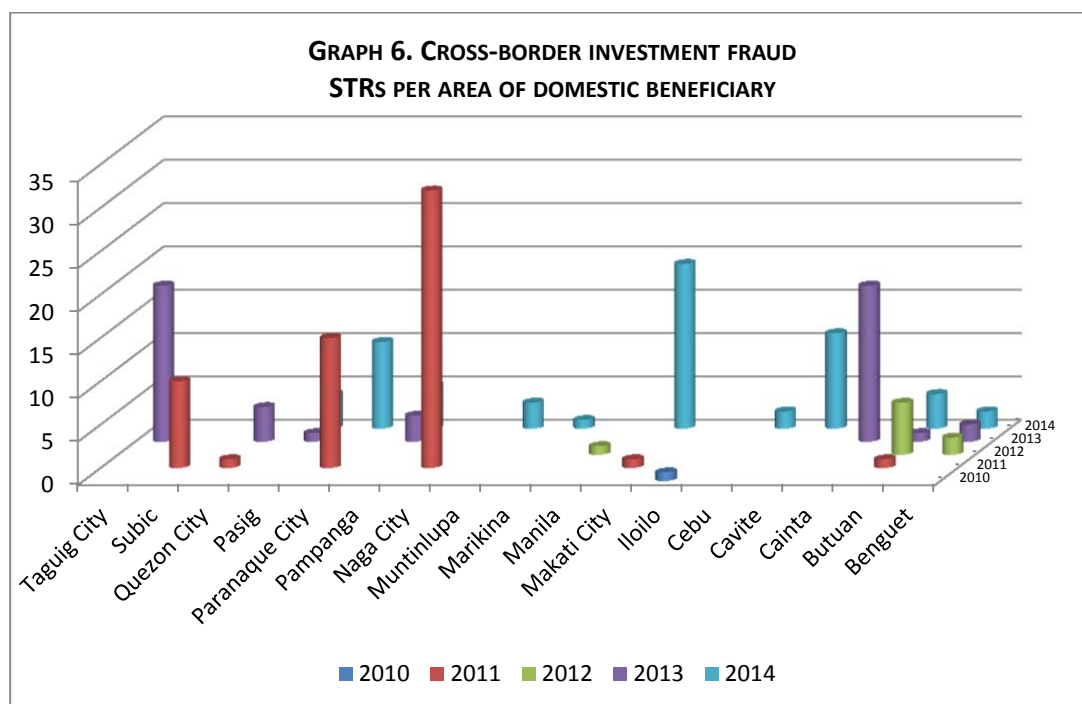


Table 13. Yearly Volume and PHP Value of Cross-border Investment Fraud per Location of Domestic Beneficiary

Year	City/Province	No. of STRs	Estimated Amount Involved per Peso value
2010	Iloilo	1	32,505,004.40
2011	Makati City	1	8,730,000.00
	Paranaque City	15	6,728,884.49
	Quezon City	1	3,984,098.86
	Subic	10	2,573,247.00
	Naga City	32	463,143.32
	Butuan	1	135,856.76
2012	Benguet	2	1,267,292.00
	Butuan	6	809,913.96
	Manila	1	503.11
2013	Cainta	18	7,265,688.52
	Taguig City	18	6,100,000.00
	Butuan	1	1,312,500.00
	Benguet	2	376,991.26
	Pampanga	3	231,343.70
	Pasig	1	<i>No amount involved</i>
	Quezon City	4	<i>No amount involved</i>
2014	Paranaque City	10	40,806,205.28
	Cavite	11	40,212,725.00
	Makati City	19	33,386,630.00
	Muntinlupa	3	15,669,676.61
	Cebu	2	11,276,173.00
	Pampanga	5	8,191,274.95
	Pasig	4	797,140.88
	Benguet	2	110,000.00
	Butuan	4	<i>No amount involved</i>
	Marikina	1	<i>No amount involved</i>
Total		178	222,934,293.10

Table 14 illustrates the transaction flow based on the details in the STRs. This may indicate the extent of cross-border fraud in terms of the number of beneficiaries and counterparties. It can be seen that some beneficiaries, particularly those in Subic, Paranaque City and Cavite, are receiving proceeds from 2 or more possible victims or counterparties/remitters.

Table 14. Number of Beneficiaries and Counterparties

Country of Counterparty	No. of Counterparties	City/Province of Domestic Beneficiaries	No. of Beneficiaries
Bahamas	1	Cebu	1
Canada	1	Naga City	1
Japan	1	Manila	1
Netherlands	1	Quezon City	1
Singapore	6	Subic	1
	1	Taguig City	1
United States of America	2	Pasig	2
	5	Paranaque City	1
Zimbabwe	1	Benguet	1
<i>Location of the remitter was not disclosed</i>	1	Benguet	2
	1	Cainta	1
	2	Makati City	5
	2	Butuan	1
	4	Cavite	1
	1	Muntinlupa	1
<i>No counterparty details</i>		Butuan	6
		Iloilo	1
		Marikina	1
		Muntinlupa	2
		Pampanga	2
		Paranaque City	1
		Pasig	1
		Quezon City	1
		Total	36
Total	30		

As illustrated in Table 15, there were 7 and 5 individuals/entities in Butuan and Makati, respectively, who/which received cross border investment fraud proceeds; the areas of Benguet, Muntinlupa and Pasig each had 3 recipients of cross border investment fraud proceeds while other locations had 1 or 2 beneficiaries each.

Table 15. Top 5 Areas with Beneficiaries

City/ Province	No. of Beneficiaries	% of Total Beneficiaries
Butuan	7	19.4%
Makati City	5	13.9%
Benguet	3	8.3%
Muntinlupa	3	8.3%
Pasig	3	8.3%

From the 178 STRs related to cross-border investment fraud, AMLC was able to identify 45 STR subjects, 17 of which were individuals and the remaining 28 were

entities/companies. Twenty-four (24) of these STR subjects had been subjects of requests for information from law enforcement agencies and foreign financial intelligence units.

IV. TYPOLOGIES AND INDICATORS

The following typologies were culled from various requests for information and STRs received by the AMLCS on cross-border investment fraud. These typologies and indicators are intended to assist reporting institutions and the FIU in identifying suspicious financial transactions involving *boiler room*, *recovery room schemes* and *advance fee fraud*, and the laundering of the proceeds thereof. This will lead to the proper implementation of preventive measures including customer due diligence and suspicious transaction reporting.

TYPLOGIES

1. Individuals representing themselves as investment advisors contacted Mr. Cy Toil, an Australian citizen and owner of Eyes Arc Ltd., enticing him to open a trading account with Weasle and Weasle Co., an Australian entity posing as a legitimate investing firm that provides advice and brokerage services for US securities. Mr. Toil acceded and engaged in several non-existent purchase and sale of stocks. In a span of six months, he lost approximately USD1.8 million.

Mr. Toil remitted his payments to King Bottom Ltd, an entity based in Hong Kong, which allegedly conducts securities clearing services for Weasle and Weasle Co. Portions of the remittances of Mr. Toil to King Bottom Ltd. were also traced to have been sent to a Philippine SEC-registered entity named Diamond Ring Realty. The funds remitted to Diamond Ring Realty were immediately withdrawn after receipt of the wired funds.

Diamond Ring Realty also received funds from various overseas entities tagged in several online forums as involved in boiler room scam. These remittance senders are Galaxy Advisory Co. (Hong Kong); Counter Barter Paint (Macau); Agtra Group (USA); and Southern Money Brokerage (USA).

Mr. Toil, through investigations done by his legal counsels, discovered that a significant number of Internet Protocol (IP) addresses used by individuals associated with Weasle and Weasle Co. to open tracked emails from him were traced in a major city in the Philippines.

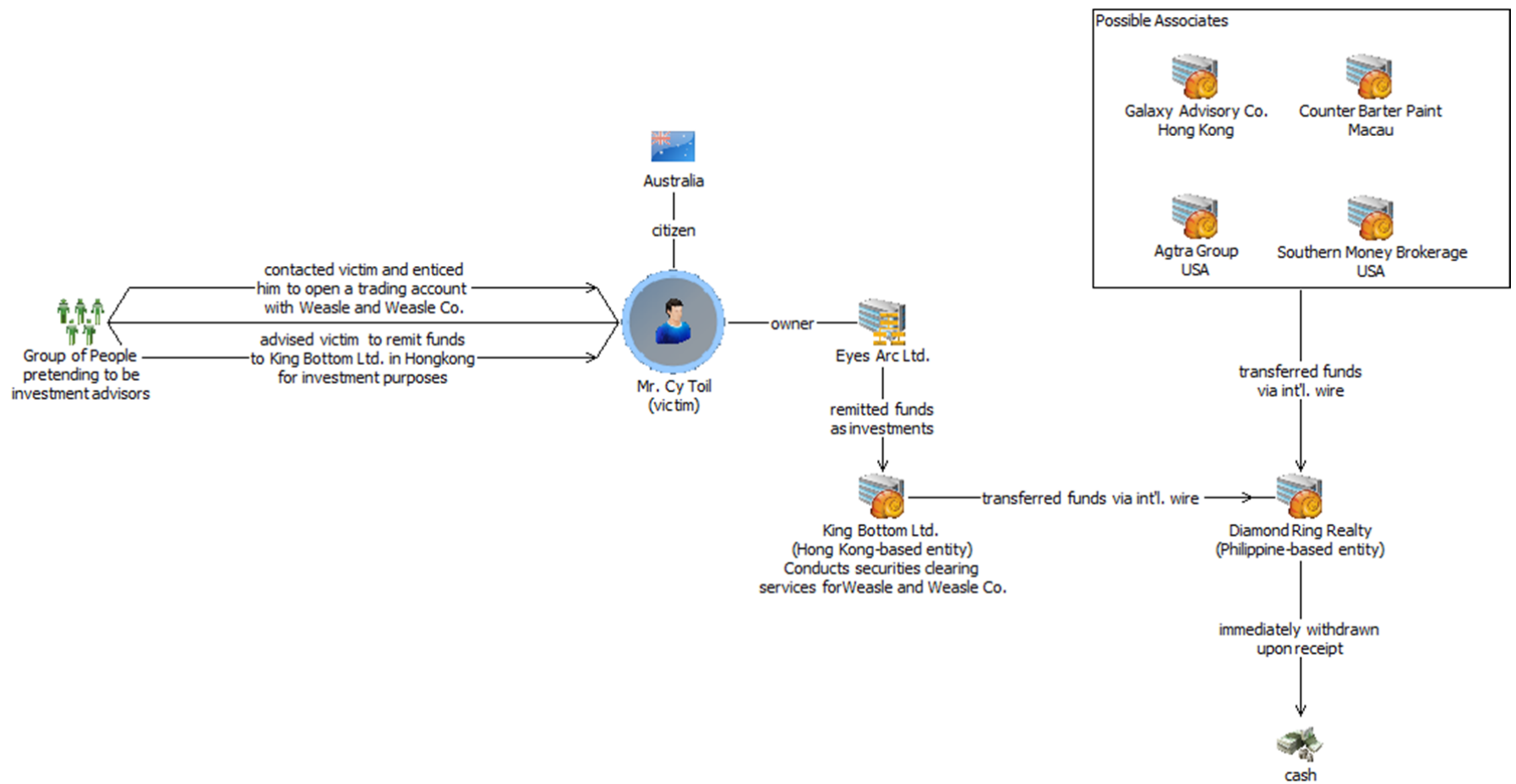


Figure 3. Diamond Ring's Case Link Chart

2. Bank XYZ reported that Brond Trading, Mondae Trading, domestic entities allegedly engaged in call center business and retail of imported goods, respectively, are involved in advance fee fraud according to U.S. Internal Revenue Services (IRS). The bank likewise disclosed that a certain Ms. Marcy Paging is the sole signatory for accounts of Brond Trading and Mondae Trading.

There have been reports that Ms. Paging has links to 5 other companies - ABC Trading, Merg Trading, MS Trading, Prom Retail Marketing and Siogon Marketing which have declared that they are engaged in the buying and selling of properties or retail of dry goods. Most of these entities were established in 2011 and 2012.

AMLC database shows that:

- Most of the subject entities are located in the southern part of the Philippines. ABC Trading, Mondae Trading, MS Trading, Prom Retail Marketing and Siogon Marketing are all located in Butuan City while Merg Trading is located in Davao.
- The accounts of the entities – Brond Trading, Mondae Trading, ABC Trading, Merg Trading, MS Trading, Prom Retail Marketing and Siogon Marketing are beneficiaries of remittances from 2012 to 2013 from various individuals located in different countries; the remittances do not appear to be connected to the businesses of said entities.
- Remittances to the account of Brond Trading range from US\$12,000 to US\$90,000 while remittances to the account of Mondae Trading range from US\$595 to US\$69,000. The funds in the said accounts appear to have been withdrawn in cash. Proprietor of Brond Trading, James Nonez, claims that the money is intended as payment for his computer business.
- Prom Retail Marketing and ABC Trading are under AML investigation for alleged link to investment scam.
- The account of ABC Trading has been receiving remittances ranging from US\$9,900 to as high as US\$1,100,000 from different individuals located in various countries. Range of remittances to MS Trading, Siogon Marketing, Merg Trading and Prom Retail Marketing is from US\$2,900 to US\$214,000.00.
- Transaction movements in the accounts show that the international remittances were withdrawn shortly after they were credited to the respective accounts. Most of these accounts were closed in 2013.
- Information gathered by the reporting banks as to the purposes of the remittances are as follows: ABC Trading and Siogon Marketing claimed that the funds are payments for properties in the Southern Luzon areas; Merg Trading and Prom Retail Marketing stated that the funds received are intended to finance activities of foreign nationals in the country; MS Trading alleged that the remittances are to be used for the purchase of properties in Southern Luzon and to finance the activities of foreign nationals in the country.

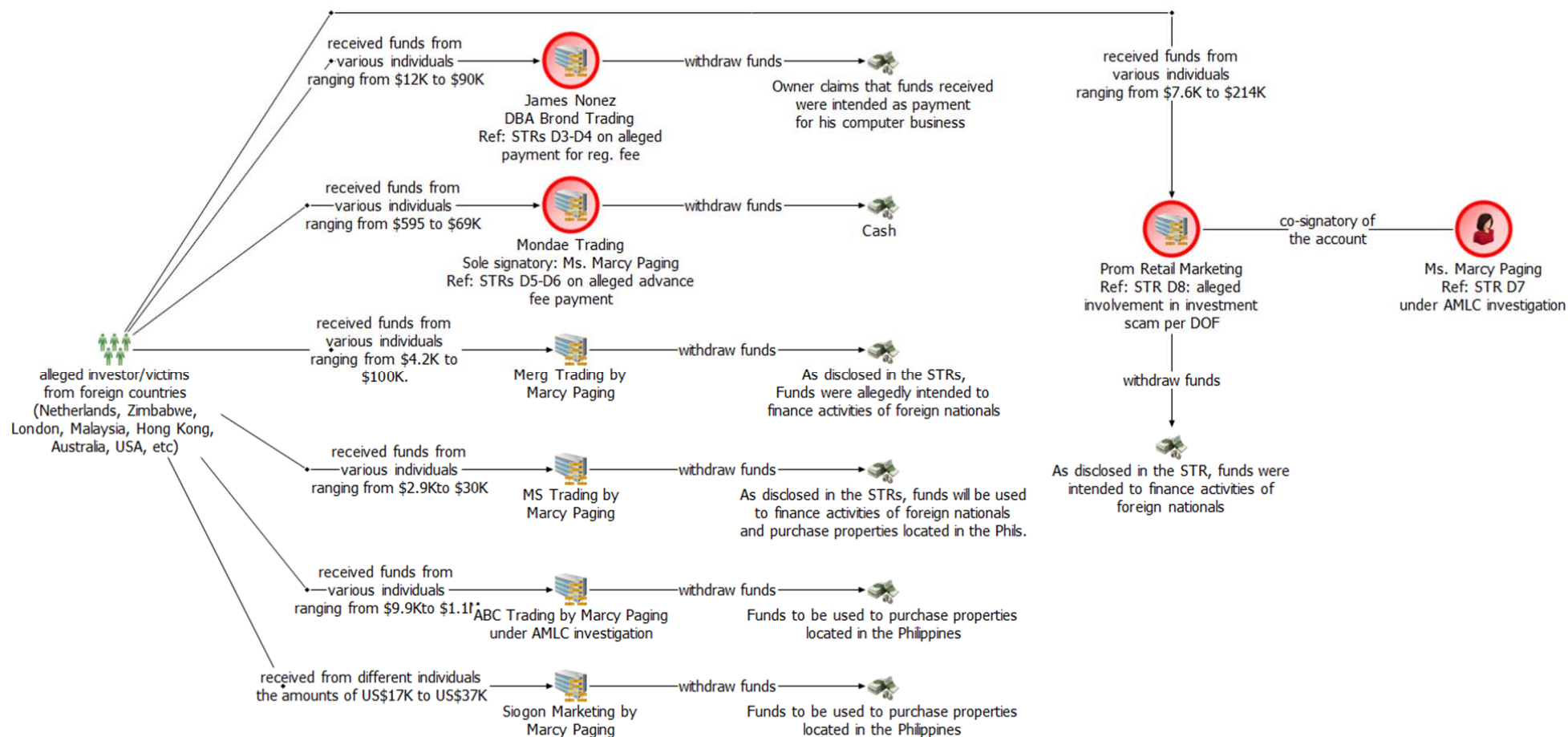


Figure 4. Marcy Paging's Case Link Chart

3. *U.S. Department of Justice* reported that entities located in the Philippines were operating call centers suspected of involvement in large scale investment fraud. The modus operandi of the scam is as follows: call centers use “Magic Jack” devices which are plugged into the USB port of a personal computer. The “Magic Jack devices” are assigned area codes corresponding to major cities in the U.S., including Chicago, New York, San Diego and Miami. These devices are used to call elderly individuals residing in the U.S. giving the victims the impression that the callers are from the U.S. when they are, in fact, physically located in the Philippines.

Moreover, the call center operators have associates in the U.S., particularly from San Diego California and Hallandale Florida, who mailed fraudulent marketing materials and account statements to the victims. It was alleged that at least 40 U.S. residents have been victimized by this scheme within the period February 2011 – August 2013 amassing more than USD3 million. The victims were instructed to issue personal checks for the amount of the investment to be picked up by FedEx courier; the checks were subsequently forwarded to ADV in Muntinlupa City, Philippines. AMLCS was able to verify some of the accounts where the funds were allegedly deposited.

4. The National Bureau of Investigation (NBI) reported that certain Filipino individuals are creating fictitious web domains and soliciting investments online using fraudulent US Internal Revenue Service (USIRS) and Philippine Government seals and documents. Victims have been advised to transfer purported advance fees and charges to bank account 1 and bank account 2. Bank account 1 is under the account name of ABCD Trading System with address in Cebu City. Transactions in this account are characterized by international remittances (from individuals in the United Kingdom, Australia, Norway and Sweden and an entity in Indonesia) which are immediately withdrawn. One remitter also remitted funds to CD and Associates, USR Trading, XYZ Trading Services which are all based in Cebu; another remitter transferred funds to NL Distribution and Logistics located in Pangasinan. AMLC database showed the same pattern of transactions in the accounts of CD and Associates, USR Trading, XYZ Trading Services and NL Distribution and Logistics as those found in the account of ABCD Trading. A bank has filed an STR on USR because of a complaint from a remitter in China. It was narrated that the complainant remitted money upon advice allegedly by the Department of Treasury Internal Revenue Service for payment of his tax to the account of USR Trading (in connection with the recovery of an earlier investment).

INDICATORS AND SUSPICIOUS TRIGGERS

Indicators for the Reporting Institutions and the FIU

1. Accountholders or clients are individuals or entities, which have just been registered with SEC or DTI. There may be a common signatory for the accounts opened. Normally, the signatory is not an incorporator. In some instances, the individuals opening the account present themselves as owners of a domestic company, branch head or consultant of a foreign entity.
2. Transactions in the domestic account are mostly inward remittances which are immediately withdrawn in cash or by check issuances to different individuals. Said transactions may also be “wire transferred” to another account in the Philippines or overseas, leaving the account with minimal balance.
3. The remitters are located largely in the United States of America, United Kingdom, Canada, Germany, Singapore, Hong Kong and Indonesia.
 - a. Remitters may be individuals, who are most likely victims of cross border investment fraud. This may be considered as the *placement stage* of money laundering.
 - b. Remitters may be companies/entities, which may be considered perpetrators or their cohorts. Funds remitted could have been received from victims of investment fraud in the foreign jurisdiction and subsequently remitted to the Philippines to *layer* the funds.
4. An individual or consultancy firm sets-up two or more companies, mainly engaged in trading, retail and call center business.
5. The accounts are usually active for a period of one (1) year. Entities operate within a limited period to avoid detection. Thereafter, a new company with a similar nature of business will emerge.
6. Multiple companies are linked by common addresses and signatories. These companies maintain accounts at different banks to conceal their business activities.
7. Recipients of remittances are individuals or companies having common counterparties or remitters.

Indicators of Fraud

1. Potential victim-investors are contacted either through email and phone calls with offers of remarkable returns. Some of the phone calls originate from call centers or business process outsourcing companies (BPOs).
2. Callers apply high pressure sales tactics to sell stocks or products to potential victims.
3. Callers present themselves as investment advisors, brokers, lawyers, or accountants and ask outright payment of fees, i.e. taxes, liquidation, clearing, or service fees.

V. CONCLUSION

Study of the STRs and CTRs related to cross-border investment fraud showed a significant value of about PHP4.656 billion remitted to our jurisdiction over a 5-year period covering the period 2010 – 2014. The remittances originated from various jurisdictions of presumed victims or perpetrators and associates. The considerable figures involved would indicate that the country is being used as a laundering site for fraudulently acquired funds. Though it is not clear whether the fraudsters were located in this jurisdiction, funds are being funneled into the country from overseas victims and perpetrators of cross-border investment fraud and their cohorts.

The study also showed that cross-border investment fraud perpetrated through *boiler room operations*, *recovery room scheme* and *advance fee scam* will potentially rise due to several existing factors –

First, the rapid technological advancement particularly in the areas of communication and connectivity provide easy access for perpetrators to secure profiles of potential victims; the creation of websites are not regulated, hence, are being exploited by scammers in setting up fake or bogus web domains or sites to lure potential victims; use of VOIP and other devices (i.e. Magic Jack) that could mask the actual location of scammers making them more difficult to track.

Secondly, as the term suggests, the nature of cross-border investment fraud encompasses international dimensions affecting various jurisdictions with diverse AML controls. The ease by which these funds are moved from one jurisdiction to the other impedes chances of recovery. In some instances, even without a court issued freeze order, banks have taken the initiative to close the account/s suspected to have links to fraud and release the remaining balance, which are normally minimal, to the account holder.

Lastly, most targets are people who are vulnerable such as retired pensioners, and those used to receiving cold calls and taking risks in anticipation of significant returns. Perpetrators of these frauds simulate the methods used by legitimate investment brokers to entice unsuspecting victims.

The study of the cross-border investment fraud CTRs and STRs also disclosed deficiencies in the reports filed such as:

1. The incorrect or improper use of transaction codes in the cross-border investment fraud CTRs and STRs. For international inward remittances, reporting institutions

used transaction codes other than *RIRIC*¹⁶, *RIRIA*¹⁷ and *RIRIP*¹⁸. Some of the transaction codes used are *CDEPC* for deposit, *MSC* for miscellaneous, *CWDLO* for withdrawal and *ZSTR* for STR transaction.

2. Mandatory information and details such as counterparty details, beneficiary information and correspondent bank details were omitted in the reports. Moreover, a number of STRs did not provide in the narrative data field the details as to why the transactions were considered suspicious.
3. There is no clear indication if the branch of the reporting institution is the transacting branch or the maintaining branch of the account of the subject.

Above deficiencies rendered it difficult to get a complete picture of the real situation in this jurisdiction of cross border investment fraud and the laundering of the proceeds thereof, and thereby hampered investigations.

A significant number of reporting institutions have not filed STRs for cross border investment frauds. Study shows that there were many covered transaction reports filed which should have warranted the filing of STRs.

A heightened international and domestic cooperation particularly the prompt sharing of information concerning suspected and identified participants of these fraud types may lessen the exposure of existing and prospective victims from other jurisdictions.

It is intended that through this study, policy will be adopted re-shaping prioritization of this crime type against others more traditionally viewed as higher priority.

¹⁶ RIRIC – Inward Remittance (International) – Credit to Beneficiary’s Account

¹⁷ RIRIA – Inward Remittance (International) – For Further Credit to Another Account

¹⁸ RIRIP – Inward Remittance (International) – Advise and Pay Beneficiary

ANNEXES

The PHP amounts presented in tables 3, 5, 7 and 8 of those in other currencies were converted using the average rate presented in Table 1, page 8 of the report.

The figures in its actual currencies and the annual distribution per area are presented in the tables below.

Annex 1. Actual Currency Value of Remittance PHP Value per Area of Domestic Beneficiary (in reference to Table 3)

CITY	PHP (PHILIPPINE PESO)	USD (US DOLLARS)	EUR (EURO)	GBP (BRITISH POUND)	CHF (SWISS FRANC)	JPY (JAPANESE YEN)
MAKATI		16,967,258.54	5,854,244.29		619,994.00	110,084,000.00
PASIG		11,798,766.11	9,523,945.50			
QUEZON CITY		17,133,357.08				
CEBU		16,601,037.07				
BUTUAN		6,797,911.95				
PARAÑAQUE		2,783,471.36				
BAGUIO		2,621,513.58				
MUNTINLUPA	57,536,229.95	574,572.18		96,222.68		
ANGELES	5,071,457.66	1,100,415.00				
PANGASINAN	28,931,995.13					
RIZAL		506,456.87				
MANILA		199,636.19				
LAGUNA		156,936.95				
CAVITE	2,332,813.15					
PASAY	839,572.50					
Grand Total	94,712,068.39	77,241,332.88	15,378,189.79	96,222.68	619,994.00	110,084,000.00

Annex 2: Actual Currency Value of Yearly PHP Value of Remittance per Area of Domestic Beneficiary (in reference to Table 5)

YEAR/CITY	PHP	USD	EUR	GBP	CHF	JPY
2010						
ANGELES		277,490.00				
BUTUAN		781,208.60				
CEBU		280,341.81				
MAKATI		3,797,889.18	987,314.00			93,089,000.00
PASIG		972,773.76	6,880,449.28			
Sub-total		6,109,703.35	7,867,763.28			93,089,000.00
2011						
ANGELES		822,925.00				
BAGUIO		1,546,971.09				
BUTUAN		1,678,863.40				
CEBU		1,223,793.45				
LAGUNA		55,158.27				
MAKATI		4,939,662.33	179,500.00			16,995,000.00
MANILA		39,462.00				
PARAÑAQUE		29,987.00				
PASIG		665,791.00	2,643,496.22			
Sub-total		11,002,613.54	2,822,996.22			16,995,000.00
2012						
BAGUIO		1,074,542.49				
BUTUAN		2,060,475.05				
CEBU		12,369,514.48				
LAGUNA		11,975.00				
MAKATI		4,914,778.22	4,536,718.29		619,994.00	
MUNTINLUPA	6,045,983.28					
PARAÑAQUE		1,701,848.36				
QUEZON CITY		14,450,553.14				
Sub-total	6,045,983.28	36,583,686.74	4,536,718.29		619,994.00	
2013						
ANGELES	3,329,942.64					
BUTUAN		1,907,374.58				
CEBU		2,165,377.13				
LAGUNA		89,803.68				
MAKATI		2,001,610.83				
MUNTINLUPA	22,033,985.99					
PANGASINAN	19,917,899.40					
PARAÑAQUE		1,051,636.00				
PASAY	839,572.50					
PASIG		291,655.63				
QUEZON CITY		2,682,803.94				
RIZAL		37,281.25				
Sub-total	46,121,400.53	10,227,543.04				

2014						
ANGELES	1,741,515.02					
BUTUAN		369,990.32				
CAVITE	2,332,813.15					
CEBU		562,010.20				
MAKATI		1,313,317.98	150,712.00			
MANILA		160,174.19				
MUNTINLUPA	29,456,260.68	574,572.18		96,222.68		
PANGASINAN	9,014,095.73					
PASIG		9,868,545.72				
RIZAL		469,175.62				
Sub-total	42,544,684.58	13,317,786.21	150,712.00	96,222.68		
Grand Total	94,712,068.39	77,241,332.88	15,378,189.79	96,222.68	619,994.00	110,084,000.00

Annex 3: Actual Currency Value of Yearly PHP Value of Remittances from Presumed Victims per Country of Origin (in reference to Table 7)

YEAR/COUNTRY	PHP	USD	EUR	GBP	CHF
2010					
AUSTRALIA		97,960.00			
MALAYSIA		65,937.82			
SWITZERLAND		201,700.00			
UK		52,291.00			
USA		1,393,482.84			
Sub-total		1,811,371.66			
2011					
AUSTRALIA		1,209,859.27			
AUSTRIA		29,943.50			
IRELAND		15,842.41			
SOUTH AFRICA		324,288.52			
SWEDEN		100,135.63			
SWITZERLAND		316,437.91			
UK		561,186.61			
USA		2,838,557.13			
Sub-total		5,396,250.98			
2012					
AUSTRALIA		264,033.10			
AUSTRIA		958,919.98			
BELGIUM		818,339.51			
CANADA		168,306.11			
DENMARK		146,143.60			
FINLAND		2,037,816.50			
GERMANY		54,107.81	11,988.00		
HONG KONG		1,019,219.47			
IRELAND		342,832.41			
JAPAN		2,790,289.78			
KENYA		14,965.00			
MALAYSIA	618,678.70	52,976.50			
NEW ZEALAND	1,267,942.50	299,560.15			
NORWAY		377,599.84			
SAUDI ARABIA		279,790.20			
SINGAPORE		51,125.00			
SWEDEN	2,912,441.70	467,437.97			
SWITZERLAND		790,633.60			619,994.00
UK	1,246,920.38	7,630,073.01			
USA		1,206,556.70			
Sub-total	6,045,983.28	19,770,726.24	11,988.00		619,994.00

2013					
AUSTRALIA		1,257,663.78			
AUSTRIA		16,322.00			
BELGIUM		25,459.00			
FINLAND		31,754.50			
HONG KONG		37,847.53			
INDONESIA		37,281.25			
ISRAEL		23,902.00			
MALAYSIA		149,797.25			
NETHERLANDS		97,456.68			
NEW ZEALAND	1,943,775.68	139,433.38			
NORWAY		17,890.47			
SINGAPORE		81,208.00			
SLOVENIA	526,767.84				
SOUTH AFRICA	1,715,380.00				
SWEDEN	14,408,673.23	152,357.84			
SWITZERLAND		425,723.85			
UAE		73,985.00			
UK	11,038,917.51	1,110,878.70			
USA	1,471,041.08	15,592.50			
Sub-total	31,104,555.34	3,694,553.73			
2014					
AUSTRALIA	3,478,044.01	459,998.50			
CANADA		35,929.50			
FINLAND		199,332.09			
GERMANY	2,270,090.86	27,097.50			
HONG KONG		88,160.06			
INDONESIA		188,601.20			
IRELAND		21,495.00			
ISRAEL		35,625.00			
ITALY		164,359.19			
JAPAN		69,122.69			
KUWAIT		171,516.83			
MALAYSIA		4,004,239.79			
NETHERLANDS		154,727.62			
NEW ZEALAND	9,726,038.43	410,979.43			
NORWAY		82,500.00			
RUSSIA		76,870.00			
SINGAPORE	2,532,513.77	2,926,126.86			
SLOVENIA		13,658.80			
SOUTH AFRICA		1,159,674.23			
SPAIN		124,399.10			
SWEDEN	3,087,022.15	674,132.27			
SWITZERLAND		151,197.50			
UK	10,801,306.65	488,605.88		96,222.68	
USA	5,316,621.90	105,922.00			
Sub-total	37,211,637.77	11,834,271.04		96,222.68	
Grand Total	74,362,176.39	42,507,173.65	11,988.00	96,222.68	619,994.00

Annex 4: Actual Currency Value of Yearly PHP Value of Remittances from Possible Associates per Country of Origin” (in reference to Table 8)

YEAR/COUNTRY	PHP	USD	EUR	JPY
2010				
FRANCE		146,944.80		
GERMANY			6,009,582.53	
HONG KONG		29,713.80		
JAPAN				93,089,000.00
MACAU		249,730.00		
MALAYSIA		11,915.40		
SPAIN		185,100.00		
UK			1,858,180.75	
USA		3,674,927.69		
Sub-total		4,298,331.69	7,867,763.28	93,089,000.00
2011				
FRANCE		58,841.85		
GERMANY			2,822,996.22	
HONG KONG		549,960.00		
JAPAN				16,995,000.00
SINGAPORE		230,537.18		
SOUTH KOREA		29,987.00		
USA		4,737,036.53		
Sub-total		5,606,362.56	2,822,996.22	16,995,000.00
2012				
AUSTRALIA		29,923.00		
GERMANY			392,896.07	
HOLLAND			219,144.50	
HONG KONG		1,188,363.00		
INDONESIA		543,421.89	202,533.00	
MALAYSIA			123,241.33	
SAMOA			2,155,578.00	
SEYCHELLES			1,431,337.39	
SINGAPORE		12,871,511.33		
SOUTH KOREA		1,603,657.68		
SWITZERLAND		255,902.92		
USA		320,180.68		
Sub-total		16,812,960.50	4,524,730.29	
2013				
BELIZE		664,139.58		
FRANCE		686,592.71		
HONG KONG		611,311.32		
INDONESIA		2,300,133.25		
SINGAPORE	15,016,845.19	634,561.60		
SOUTH KOREA		1,051,636.00		
SWITZERLAND		180,817.00		
USA		403,797.85		
Sub-total	15,016,845.19	6,532,989.31		

2014				
BELIZE		682,983.48		
FRANCE		54,963.00		
HONG KONG		482,994.07	139,200.00	
INDONESIA		205,985.62		
SINGAPORE	5,333,046.81			
SWITZERLAND			11,512.00	
USA		56,589.00		
Sub-total	5,333,046.81	1,483,515.17	150,712.00	
Grand Total	20,349,892.00	34,734,159.23	15,366,201.79	110,084,000.00