AMLC
Anti-Money Laundering Council

DECEMBER 2022

TYPOLOGIES BRIEF: MONEY MULES

TABLE OF CONTENTS

TABLE OF ACRONYMS

AMLC	Anti-Money Laundering Council
ATM	Automated Teller Machine
CECCW	Withdrawal – Electronic Cash Card/Gift Card/Debit Cards
CWDLA	Withdrawal – ATM
CWDLO	Withdrawal – Over the counter
EMI	Electronic Money Issuer
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
MIN	Mobile Identification Number
RA	Republic Act
STR	Suspicious Transaction Report

EXECUTIVE SUMMARY

In the fight against money laundering and terrorism financing, the Anti-Money Laundering Council (AMLC) deemed it timely to issue this typologies brief, featuring the prominent and notable typologies employed by suspected money mules in the Philippines. These typologies were derived from a total of 821,979 money mule-related suspicious transaction reports (STRs) received by the AMLC between the first quarter of (Q1) 2016 and Q1 2022. Said STRs had an aggregate value of PHP510.17 billion.

Based on a descriptive analysis provided in Section 3 of this report, it was found that the STR filings related to money mules have been increasing in the past years leading to the year 2022. An influx of STRs was observed in 2021, possibly due to the accelerated adoption of digital banking and electronic wallets in the midst and in the wake of the COVID-19 pandemic.

A significant share of the sample STRs were filed on the basis of two suspicious circumstances, namely "There is no underlying legal or trade obligation, purpose, or economic justification (SI1)" and "The amount involved is not commensurate with the business or financial capacity of the client (SI3)." In terms of value, the suspicious circumstance, "The client is not properly identified (SI2)," topped the rank. Meanwhile, STRs on other predicate crimes constitute only 0.23% of the total volume and 0.03% of the total value of sample STRs. The top predicate crime in terms of both volume and value appeared to be swindling (PC9).

It was noted that the suspected money mules in the Philippines utilize three modes of withdrawing funds: electronic cash cards, automated teller machines (ATMs), and over the counter. Further, majority of the suspected money mules were found to be residing in Metro Manila, Rizal, Nueva Ecija, Cavite, Bulacan, and Laguna.

As observed in this report, the suspected money mules are involved in the following activities:

1. Fund transfers through self-service kiosks;
2. Opening of digital bank accounts and electronic wallets using sequential mobile identification numbers (MINs);
3. Multiple cash and check deposits followed by large-value withdrawals;
4. Cash and animal smuggling;
5. Opening an account on behalf of another individual;
6. Purporting to be a member of Marine Corps;
7. Receiving funds using drop accounts bought in the dark web;
8. Fund flipping; and
9. Illegal gambling, particularly illegal cockfighting.

Given the seemingly rampancy of money mules in the country, the report highlights the need to raise awareness among the covered persons so that they may prevent money mules from taking advantage of the existing financial infrastructures. Likewise, the study finds value in educating the general public about the suspicious activities and notable typologies of money mules, so they may protect themselves from being victimized. Thus, the dissemination of this report to law enforcement agencies (LEAs), supervising authorities, other government agencies, covered persons with Public-Private Partnership Agreement with the AMLC, other financial intelligence units (FIUs), and the general public is recommended.

1. Background of the Study

Money mules play a critical role in the consummation of certain money laundering offenses. They aid money launderers in obscuring the origin of illicit funds by knowingly or unknowingly moving illegally acquired money, typically broken down into smaller amounts, on behalf of perpetrators behind a larger illegal scheme. They add layers to the money trail of criminals to prevent raising suspicion from authorities.

Through time, the methods employed by money mules have quickly evolved to take advantage of the most recent financial and technological advancements. Early this year, Philippine banks have issued advisories on money mule scams and urged the public to be more vigilant to prevent being recruited as money mules themselves.

In an aim to combat the rising cases of money mules in the country, the AMLC is issuing this typologies brief to guide covered persons in identifying and detecting possible activities of money mules. It offers a stocktake of various schemes adopted by possible money mules throughout the years, which can serve as a warning for covered persons that may encounter these transactions as part of their normal business operations. Similarly, this typologies brief can aid the general public in protecting themselves from being victimized by the schemes employed by suspected money mules.

2. Scope and Methodology

This typologies brief is primarily derived from STRs submitted by covered persons to the AMLC. The dataset used in this report was generated by mining and pooling, from the entire population of STRs in the AMLC database, all STRs containing keywords related to money mules in the narrative field. Specific keywords considered were: “mule,” “mules,” and “money mules.” This yielded a total of 821,979 STRs pertaining to transactions completed between Q2 2010 and Q1 2022 (submitted by covered persons to the AMLC between Q1 2016 and Q1 2022). All reported subjects of said STRs were treated as suspected money mules.

The entire dataset comprising 821,979 STRs was used in determining the location of suspected money mules in the Philippines. As several subjects had multiple STRs filed on them, however, only unique subject-address pairs were considered in ranking the declared addresses by their respective provinces and computing their respective shares in terms of the volume and value of the corresponding STRs. Meanwhile, a sub-sample, which consists of STRs pertaining to withdrawal transactions, was utilized in identifying the location of the cash-out facilities used by the suspected money mules. For this purpose, the location of the cash-out facilities was assumed to be the same as the location of the reporting branch.

For comparison purposes, all transactions in the dataset were analyzed and presented in their Philippine Peso equivalent amounts. Analysis based on various possible groupings of the transactions was also performed, including:

a. Institution type;
b. Year of transaction;
c. Year of submission of STR;
d. Nature of transaction;

e. Declared address of accountholders/beneficiaries/counterparties/subjects; and
f. Address of the reporting branch.

An exercise of sound judgment was warranted in standardizing the declared addresses of the identified subjects, accountholders, and their beneficiaries and/or counterparties. This step was deemed necessary as the raw addresses reported by covered persons bore stark inconsistencies, mostly in terms of the reported cities and provinces.

Aside from the data submitted by covered persons through the STRs, this document also used open-source information whenever necessary.

The analysis is guided by the following confidence level matrix and estimative language usage:

Analytic Judgments and Confidence Levels

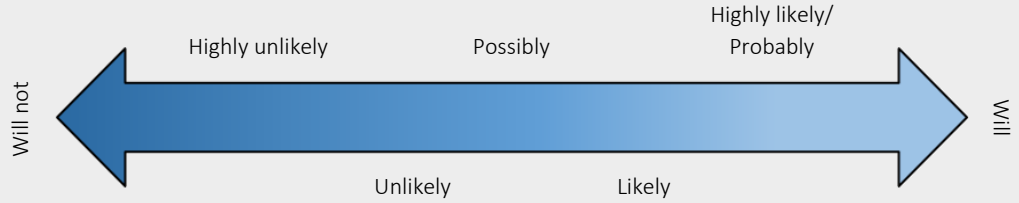
FIU Intelligence Assessments use phrases such as "we judge," "we assess," or "indicates" to convey analytical inferences (conclusions). These assessments are not statements of fact or proof, and do not imply complete knowledge. Analytic judgments are often based on incomplete information of varying quality, consistency, and reliability. Analytic judgments are distinct from the underlying facts and assumptions in which they are based and should be understood as definitive or without alternative explanation.

The AMLC assigns "high," "moderate," or "low" confidence levels to analytic judgments based on the variety, scope, and quality of information supporting that judgment.

- *"**High confidence**" generally indicates a judgment based on multiple, consistent, high-quality sources of information and/or that the nature of the issue makes it possible to render solid judgment.*
- *"**Moderate confidence**" generally means the information could be interpreted in various ways, we have alternative views, or the information is credible and plausible but not sufficiently corroborated to warrant a higher level of confidence.*
- *"**Low confidence**" generally means the information is scant, questionable, or very fragmented and it is difficult to make solid analytic inferences, or we have significant concerns or problems with the sources.*

Estimative Language

Certain words are used in this assessment to convey confidence and analytical judgment regarding the probability of a development or event occurring. Judgments are often based on incomplete or fragmentary information and are not fact, proof, or knowledge. The figure below describes the relationship of the terms to each other.



Considering the foregoing data availability and limitations, a moderate level of confidence is given on the analytical judgment presented in the succeeding discussions of prominent and notable typologies.

CAVEAT

The data provided in this report should not be interpreted as an assessment of the full amount of proceeds related to money mules. The actual volume and amount of proceeds may be larger than represented in the sample of STRs used, which consists of both consummated and attempted transactions reported to the AMLC.

The statements herein are not conclusive but are more descriptive of what has been observed on the gathered STRs. These STRs also need further verification and more in-depth investigation to substantiate likely linkage to a certain predicate crime, including but not limited to frauds and illegal exactions and transactions, fraudulent practices and other violations under the Securities Regulation Code of 2000, smuggling, swindling, and violations under the Electronic Commerce Act of 2000, among others.

DEFINITION OF TERMS

The following terms used in this report are hereby defined as follows:

a. **"Covered Person"** refers to financial institutions and designated non-financial businesses and professions under Rule 4, Section 1 of the 2018 Implementing Rules and Regulations of Republic Act No. (RA) 9160, as amended.

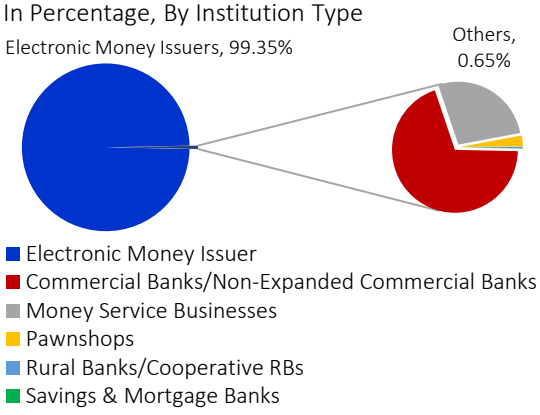
b. **"Suspicious Transaction"** refers to a transaction, regardless of amount, where any of the following suspicious circumstances exist:
    1. There is no underlying legal or trade obligation, purpose, or economic justification;
    2. The client is not properly identified;
    3. The amount involved is not commensurate with the business or financial capacity of the client;
    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 RA 9160, as amended;
    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;
    6. The transaction is in any way related to an unlawful activity or offense under RA 9160, as amended, that is about to be, is being or has been committed; or
    7. Any transaction that is similar or analogous to any of the foregoing.

c. **"Suspicious Transaction Report (STR)"** refers to a transaction, regardless of amount, where any of the above suspicious circumstances are determined, based on suspicion or, if available, reasonable grounds, to be existing.

3. Data Profile

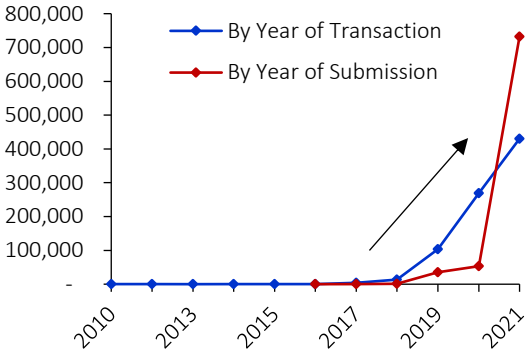
The 821,979 STRs used in this report were filed by various covered persons between Q1 2016 and Q1 2022 (**Figure 1**). Out of this sample, 816,674 STRs (or 99.35% of the total STR count) were submitted by electronic money issuers (EMIs). The remaining 5,305 STRs originated from commercial banks/non-expanded commercial banks (3,687 STRs or 0.45% of the total STR count), money service businesses (1,444 STRs or 0.18% of the total STR count), pawnshops (149 STRs or 0.02% of the total STR count), rural banks/cooperative banks (21 STRs), and savings and mortgage banks (4 STRs).

Figure 1. Composition of the Dataset
In Percentage, By Institution Type



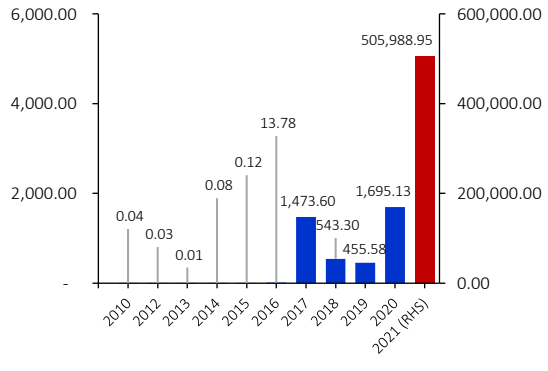
Breaking down the sample by year of transaction and year of submission, it can be noted that the STRs related to money mules have been monotonically increasing since the beginning of the observation period (**Figure 2**). In 2021, there was an influx of STRs related to money mules, which totalled to 732,392. This brought the year-on-year growth of money mule-related STRs from 50.50% in 2020 to 1,277.09% in 2021.

Figure 2. STRs Related to Money Mules
Total count, By year



The sharp increase in the number of submitted STRs in 2021 can be attributed to the emergence and accelerated adoption of digital banking and electronic wallets, which did not only provide alternative payment methods but also made financial transactions easier and safer in the midst and in the wake of the COVID-19 pandemic. This is consistent with the reported volume of PESONet[1] and InstaPay[2] transactions, which posted 164% and 223% growth, respectively, in the first half of 2021 alone.[3]

Figure 3. Value of STRs Related to Money Mules
In PHP millions



The annual values of STRs related to money mules likewise spiked in 2021, reaching PHP505.99 billion or 99.18% of the total value of the captured STRs (**Figure 3**). The sudden increase in the value of STRs

[1] PESONet is an electronic fund transfer scheme that enables the transfer of high-value funds in Philippine currency, between customers of participating banks, EMIs, or mobile money operators. (Source: https://www.philtrustbank.com/sites/default/files/FAQ_PESONet.pdf)

[2] Instapay is a real-time, low-value electronic fund transfer credit push payment scheme for transaction amounts up to PHP50,000. (Source: https://www.bsp.gov.ph/Pages/PAYMENTS%20AND%20SETTLEMENTS/National%20Retail%20Payment%20System/Empowering-Every-Juan-and-Maria.aspx).

[3] Agcaoili, Lawrence. "Metrobank cuts PESONet fee by half", PhilStar Global, 02 Nov. 2021, https://www.philstar.com/business/2021/11/02/2138277/metrobank-cuts-pesonet-fee-half (last visited: 29 Nov. 2022).

in 2021 is due to an attempted account opening with an initial deposit of USD10 billion (or equivalent value of PHP503.75 billion).[4]

Majority of the sample STRs were filed on the basis of suspicious circumstances enumerated under RA 9160, as amended, accounting for 99.77% of the total volume of STRs (**Table 1**). About 45.89% of the STRs filed under "there is no underlying legal or trade obligation, purpose, or economic justification (SI1)" pertain to the following: (1) inability of clients to provide documents supporting their claim that the funds in question represent their business proceeds, business investments, or their share in family inheritance; (2) failure of client to provide justification for funds given to him gratuitously by his brother's alleged friend; and (3) a transaction which was not aligned with clients' declared purpose for opening an account.

In terms of value, the suspicious circumstance "the client is not properly identified (SI2)" topped the rank, with a 98.75% share. This is commonly associated with the inability to establish the relationship between the sender and recipient of funds in question as well as the source of income of the suspected subjects.

Table 1. Suspicious Circumstances and Predicate Crimes with Money Mule-Related Keywords

Suspicious Circumstance/ Predicate Crime	Total Volume	Percent to Total Volume	Total Value (In PHP Millions)	Percent to Total Value
Suspicious Circumstances	**820,051**	**99.77%**	**510,003.17**	**99.97%**
There is no underlying legal or trade obligation, purpose, or economic justification (SI1)	377,247	45.89%	4,232.99	0.83%
The amount involved is not commensurate with the business or financial capacity of the client (SI3)	352,548	42.89%	1,096.25	0.21%
The transaction is similar, analogous, or identical to any of the foregoing (SI6)	88,329	10.75%	890.03	0.17%
The transaction is structured to avoid being reported (SI4)	1,091	0.13%	7.95	0.00%
The client is not properly identified (SI2)	830	0.10%	503,775.75	98.75%
There is a deviation from the client's profile/past transactions (SI5)	6	0.00%	0.20	0.00%
Predicate Crimes	**1,928**	**0.23%**	**168.02**	**0.03%**
Swindling (PC9)	971	0.12%	130.85	0.03%
Smuggling (PC10)	460	0.06%	4.84	0.00%
Violations under the Electronic Commerce Act of 2000 (PC11)	293	0.04%	20.11	0.00%
Fraudulent practices and other violations under the Securities Regulation Code of 2000 (PC33)	159	0.02%	6.95	0.00%
Frauds and Illegal Exactions and Transactions (PC16)	42	0.01%	5.26	0.00%
Violations of the National Internal Revenue Code of 1997	3	0.00%	-	0.00%
Total	**821,979**	**100.00%**	**510,171.18**	**100.00%**

[4] This suspicious transaction is elaborated in Section 4.6.a.

STRs on other predicate crimes constitute only 0.23% of the total volume and 0.03% of the total value of sample STRs. The top three predicate crimes in terms of volume are swindling (PC9), smuggling (PC10), and violations under the Electronic Commerce Act of 2000 (PC11). In terms of value, the top three predicate crimes were swindling (PC9), violations under the Electronic Commerce Act of 2000 (PC11), and fraudulent practices and other violations under the Securities Regulation Code of 2000 (PC33).

The top declared address of suspected money mules in the Philippines appeared to be Metro Manila, which accounted for 36.45% of all declared addresses. The other provinces that were commonly reported by suspected money mules as their place of residence include, among others, Rizal (12.81% share), Nueva Ecija (10.40% share), Cavite (9.61% share), Bulacan (7.49% share), and Laguna (5.88% share).

Table 2. Reported Addresses of Suspected Money Mules

Address	Total
Metro Manila	36.45%
Rizal	12.81%
Nueva Ecija	10.40%
Cavite	9.61%
Bulacan	7.49%
Laguna	5.88%
Others	17.35%
Total	**100.00%**

In addition, it was noted that that the suspected money mules in the Philippines utilize three modes of withdrawing funds: electronic cash cards (CECCW), automated teller machines (CWDLA), and over the counter (CWDLO). Using the available addresses of the reporting branches as proxy for the location of the cash-out facilities used by suspected money mules, it was observed that 54.91%[5] of the withdrawal transactions were performed in Metro Manila. This was followed by Cavite (38.08%), Negros Occidental (2.80%), Laguna (2.10%), Pampanga (1.64%), and Tarlac (0.47%).

Table 3. Common Location of Cash-Out Facilities Used by Suspected Money Mules By Province, Based on STR Count

Location	Volume				Percent to Total Volume
	CECCW	CWDLO	CWDLA	Total	
Metro Manila	-	10	225	235	54.91%
Cavite	-	7	156	163	38.08%
Negros Occidental	-	-	12	12	2.80%
Laguna	-	-	9	9	2.10%
Pampanga	-	1	6	7	1.64%
Tarlac	-	2	-	2	0.47%
Total	**-**	**20**	**408**	**428**	**100.00%**

[5] STRs with unknown reporting branch address were excluded from the calculation.

Within Metro Manila, the withdrawal transactions by suspected money mules were done in Makati City (76.60% of total transactions in Metro Manila), Parañaque City (17.45%), City of Manila (2.98%), Quezon City (2.55%), and Pasay City (0.43%).

Table 4. Commonly Used Cash-Out Facilities in Metro Manila
By City, Based on STR Count

City	Volume				Percent to Total Volume
	CECCW	CWDLO	CWDLA	Total	
Makati City	-		180	180	76.60%
Parañaque City	-	2	39	41	17.45%
City of Manila	-	7		7	2.98%
Quezon City	-		6	6	2.55%
Pasay City	-	1		1	0.43%
Total	**-**	**10**	**225**	**235**	**100.00%**

The amount of withdrawn funds related to money mules is estimated at PHP46.60 million. Out of this, 43.16% were transacted in Metro Manila, 6.39% in Cavite, and 3.43% in Tarlac.

Table 5. Common Location of Cash-Out Facilities Used by Suspected Money Mules
By Province, Based on STR Values

Location	Value (In PHP Millions)				Percent to Total Value
	CECCW	CWDLO	CWDLA	Total	
Metro Manila	-	18.42	1.69	20.11	43.16%
Cavite	-	1.50	1.48	2.98	6.39%
Tarlac	-	1.60	-	1.60	3.43%
Pampanga	-	0.16	0.05	0.21	0.46%
Negros Occidental	-	-	0.16	0.16	0.33%
Laguna	-	-	0.11	0.11	0.24%
Unknown	0.93	-	20.50	21.43	45.99%
Total	**0.93**	**21.68**	**23.99**	**46.60**	**100.00%**

Within Metro Manila, although the highest volume was reflected in Makati City (Table 4), the highest amount of withdrawals as shown in Table 6 was seen in the City of Manila (90.70%), followed by Makati City (4.99%) and Parañaque City (3.64%) in the second and third ranks, respectively.

Table 6. Commonly Used Cash-Out Facilities in Metro Manila
By City, Based on STR Values

City	Value (In PHP Millions)				Percent to Total Value
	CECCW	CWDLO	CWDLA	Total	
City of Manila	-	18.24	-	18.24	90.70%
Makati City	-	-	1.00	1.00	4.99%
Parañaque City	-	0.12	0.61	0.73	3.64%
Quezon City	-	-	0.08	0.08	0.39%
Pasay City	-	0.06	-	0.06	0.27%
Total	**-**	**18.42**	**1.69**	**20.11**	**100.00%**

4. Prominent and Notable Typologies

4.1. Transactions Made Using Self-Service Kiosks

Between 1 February 2019 and 4 September 2020, a total of 91,726 STRs with an aggregate value of PHP593.96 million were filed by covered person PQR on 2,508 individuals, whose accounts have shown unusual inflow and outflow transactions that had been completed using self-service kiosks found in a convenience store chain. As reported by said covered person, these individuals were identified to have had suspicious cash-ins that were subsequently withdrawn via ATMs and/or wallet-to-wallet transfers to various MINs.

Based on addresses disclosed by these 2,508 individuals, 73% were identified to be residents of Pampanga (31%), Laguna (21%), Manila (9%), Caloocan (7%), and Cavite (5%). Further, majority of them declared remittances and self-generated income (e.g., as a tricycle driver) as sources of funds, which led the reporting covered person to file STRs on the basis of the following: (1) the amount involved in the review is not commensurate with the financial capacity of the clients; (2) the relationship between the clients and beneficiaries together with purpose of transaction cannot be established; and (3) the movement of funds shows the same pattern for identified MINs with unusual activities.

The rapid movement of funds through a digital payment platform (inflows) and an online transfer facility (outflows) suggests that the accounts involved are possibly used as pass-through accounts.

4.2. Transactions by Individuals with Sequential MINs

Covered person PQR flagged 308 individual clients who are involved in multiple fund transfers that amounted to PHP63,195,041.59 in less than seven months. Said transactions were made in favor of a certain LMN who has an account with another domestic bank.

Based on an investigation conducted by PQR, it was found that majority of the subject clients had opened their accounts between November 2019 and March 2020. The subject clients as well as their counterparties, who enrolled in succession under sequential MINs, used the same background in their know-your-customer videos, thereby giving rise to the hypothesis that they opened their accounts from only one location.

Most of the subject clients were identified to be residents of various cities in Laguna (i.e., Biñan, Cabuyao, Calamba, San Pedro, and Sta. Rosa). They declared obtaining their funds from being a factory worker, fish and food vendor, jeepney driver, loading station owner, sari-sari store owner, and tricycle driver.

As reported by PQR, notable transactions associated with the subject clients' accounts involved multiple high-value credits, ranging from PHP10,000 to PHP20,000. These were usually followed by fund transfers to the account of LMN.

4.3. Successive Deposits and Withdrawals

On 21 October 2014, JKL opened a regular account with Bank ABC with an initial deposit of PHP449,000. He declared having a consultancy business, from which he generates his funds.

From 27 March 2017 to 20 April 2017, JKL was found to have several cash and check deposits (ranging from PHP357,000 to PHP4.90 million) followed by large-value withdrawals (ranging from PHP605,600 to PHP7.08 million).

In the conduct of enhanced due diligence, Bank ABC discovered that JKL acts as a money mule who carries cash to casinos. JKL himself disclosed to the branch that his friends deposit funds to his accounts, which he then delivers to them should they need cash at Casino DEF. Upon inquiry by the branch on the nature of his transactions, JKL stopped using his personal account.

Meanwhile, Bank ABC also filed STRs on GHI, which appeared to be JKL's consultancy business. Since GHI's account opening on 20 June 2014 up until April 2017, there were no significant transactions observed. Between 3 April 2017 and 24 January 2018, however, the branch noted 853 transactions, ranging from PHP126,500 to PHP10.09 million. Additional 132 transactions with amounts ranging from PHP17,000 to PHP13 million were recorded from 23 March 2018 to 8 November 2018. The covered person deemed the transactions of JKL and GHI as having no underlying legal or trade obligation, purpose, or economic justification.

4.4. Smuggling

4.4.a. Cash Smuggling

On 26 September 2019, RST arrived at Ninoy Aquino International Airport, carrying US dollar-denominated notes that he failed to declare in writing. RST is one of the named members of "RDG Group," which was suspected of sneaking foreign currencies into the country from September 2019 to March 2020.

Bank MNO noted that from their opening up until their closing in 2020, RST's savings accounts had significant cash/check deposits and fund transfers to multiple MNO and non-MNO accounts with amounts ranging from PHP1,000 to PHP100,000. His debit transactions consist of check-clearing, withdrawals over the counter and via ATMs, and fund transfers to multiple MNO and non-MNO accounts.

4.4.b. Animal Smuggling

Bank MNO client ABR, born on 11 April 2006, is a student with a declared income of PHP1,000. She is a granddaughter of ABF, a business owner of ABF Pet Supply with a monthly income of PHP50,000. Open-source information tells that ABF has been repeatedly arrested and charged with violations of RA 9147 or the Wildlife Resources Conservation and Protection Act, by the Department of Environment and Natural Resources and agents from the National Bureau of Investigation and the Philippine National Police.

ABR was suspected of being a money mule due to large turnover of funds seen in her account. According to Bank MNO, ABR opened a savings account on 12 December 2017 with a starting balance of PHP1,983,088.89. From this amount, a total of PHP1,508,088.88 was transferred to ABR's time deposit account, which recorded no prior movements. ABR was also reported to have an active joint account with his grandfather.

It was noted that the flow of funds to and from ABR's savings account is not commensurate with her profile. Her credit transactions ranged from PHP10,000 to PHP620,000, while her debit transactions ranged from PHP10,000 to PHP1,070,000.

Given that ABR was only 13 years old at the time of filing the STRs, the covered person inferred that the bulk of the incoming and outgoing transactions in her account possibly represents the payment/proceeds from the illegal activities of her grandfather.

4.5. Accounts Used in the Dark Web

Based on the sample dataset, a total of 24 distinct bank accounts belonging to 19 individuals were reportedly sold in the "dark web" as drop accounts. Dark web refers to encrypted online content that is not catalogued by conventional search engines. Also known as the "dark net," dark web is where stolen information, such as electronic mail accounts, bank details, and illegal and prohibited items (e.g., arms and ammunitions, illegal drugs, etc.) are being sold.

According to the bank's report, the subject accounts were likely utilized by fraudsters as drop accounts to receive payments for stolen credentials and other sold items. There is also a possibility that mules use said bank accounts to receive from account hackers' fraudulent transfers that are subsequently cashed out through either ATM withdrawals or remittance agents.

There were no notable similarities observed among the accountholders, in terms of age, sex, source of funds, or declared monthly income. In terms of location, many of them declared Las Piñas and Laguna as their mailing addresses. Meanwhile, 47.36% of them are employed with monthly incomes ranging from PHP10,000 to PHP50,000; 21.05% are self-employed with monthly incomes ranging from PHP10,000 to PHP250,000; and 26.32% are unemployed with declared allowances as source of funds, ranging from PHP999 to PHP30,000.

One of the reporting covered persons narrated that one bank account recorded total inflows amounting to PHP1.07 million, which consisted of online payments, inward remittances, and cash deposits. Said funds, however, were also immediately withdrawn via ATM. It is worth noting that these transactions are not aligned with the accountholder's declared purpose of opening said account, i.e., for personal savings.

4.6. Opening an Account on Behalf of Another Individual

4.6.a. In Exchange of an Award

On 24 June 2021, Bank WXY's branch in Bonifacio Global City received a phone inquiry from a certain LCD, who claimed to be calling on behalf of an unnamed friend, X. According to LCD, X was interested in opening a dollar account where he could place USD10 billion worth of funds paid by the US Treasury

to him. LCD also disclosed that X gave her a video and a document where the latter mentioned that whoever would be able to open a revolving account on his behalf will be awarded. Upon further probing, however, the reporting covered person was not able to validate the source of funds involved as LCD only provided vague answers.

4.6.b. Modus Operandi of Nigerian Fraudsters

Two STRs corresponding to suspicious transactions dated 31 March 2016 were filed by Bank DCB on two individuals—a Filipino and a Nigerian—for their alleged involvement in a modus operandi of Nigerian fraudsters. Based on Bank DCB's disclosure, said modus operandi involved Filipino women who are being used by Nigerian fraudsters to facilitate the opening of their fly-by-night businesses. These businesses are supported by business registration certificates from the Department of Trade and Industry which in turn are presented by Nigerians as supporting documents during account opening.

As observed by the reporting covered person, the accounts owned by the alleged Nigerian fraudsters would have a minimum balance upon opening. The accounts would remain inactive for a year or so until such time that a highly suspicious, questionable amount of money would be transferred/credited thereto.

4.7. Romance Scam

A reporting covered person discovered multiple online posts involving an account allegedly used in a romance scam. Romance scams involve feigning romantic intentions towards a victim, who will later be defrauded once the former gains the latter's trust and confidence.

The reporting covered person narrated that the social media posts identified the scammer as PRO. At the beginning, PRO would introduce himself to his victims as a member of the Marine Corps. Thereafter, he would send a message supposedly from his superiors, asking for money to fund his flight which will be booked by a military agent. PRO would have the money sent to an alleged Bank DCB mule account under the name of CDV.

4.8. Flipping of Funds

A total of 74 STRs were filed by covered person PQR on WBA for wallet-to-wallet transfers completed on 18 September 2021, 19 October 2021, 22 October 2021, and 25 October 2021. Said transactions were deemed to be not commensurate with the business or financial capacity of WBA, whom PQR profiled as a driver.

WBA's transaction-level data reveal a notable pattern that displays indicators of being a possible mule account. The chain of transactions involving WBA begins with a single sender, transmitting funds exactly amounting to PHP10,000. Thereafter, the money would be passed to another person who will then send the money back to WBA.

Upon closer inspection of the transaction-level data submitted by PQR, it was noted that WBA's transactions coincided with PQR's promo gaming activity called the "Send Money Challenge." Said promo allows PQR's consumer accountholders that are residing in the Philippines to earn a voucher

when they send a minimum of PHP10,000 to a unique verified client of PQR, through PQR's Send Money feature. Each user can participate up to 10 times to get the maximum reward.

Figure 4: Transactions dated 18 September 2021

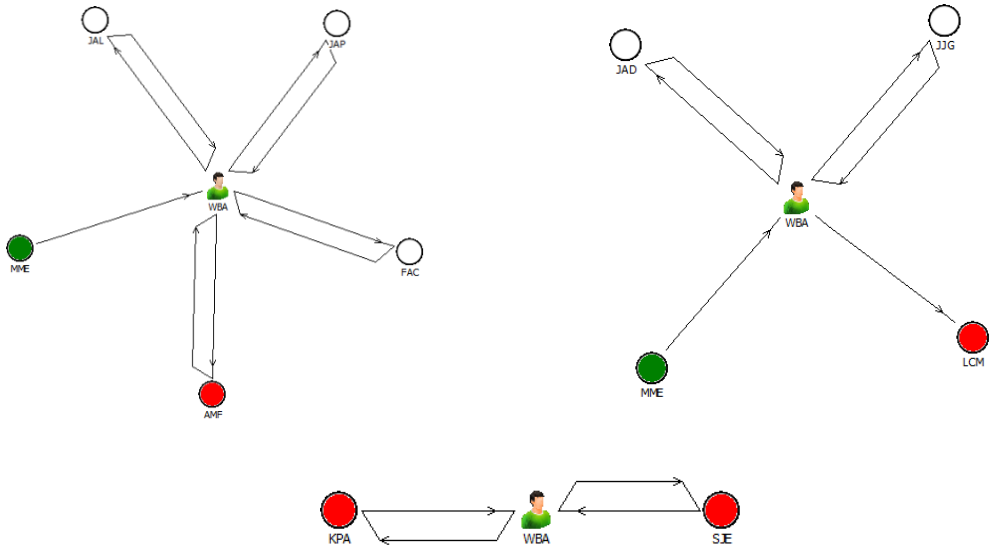


Figure 5a: Transactions dated 19 October 2021

Figure 5b: Transactions dated 19 October 2021

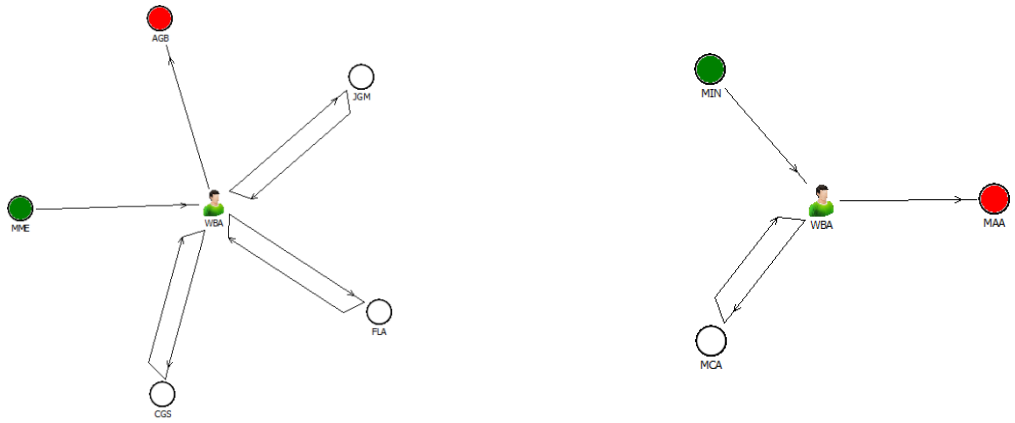


Figure 6: Transactions dated 22 October 2021

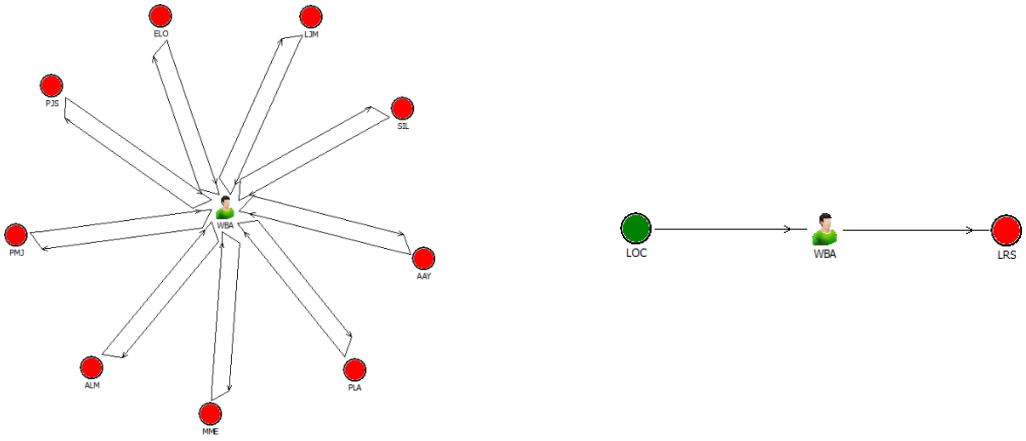
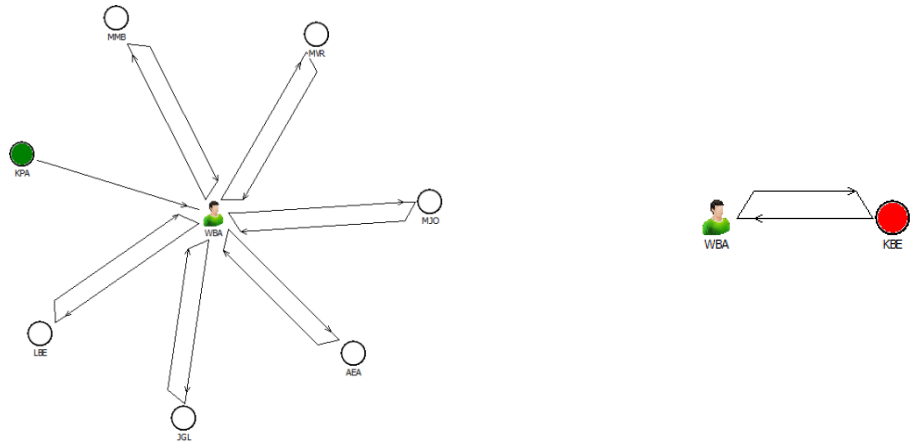


Figure 7: Transactions dated 25 October 2021



As depicted in the preceding charts, WBA transacted with at least two sets of PQR accountholders on each of the indicated transaction dates. WBA, who had a reported address in Antipolo, Rizal, appeared to have been sending and receiving funds from individuals residing not only in Rizal but also in Albay, Bulacan, Cavite, Davao Del Norte, Metro Manila, Sorsogon, and South Cotabato. Notwithstanding the geographical distance between them, WBA and her individual counterparts were able to complete their transactions in a matter of minutes. As summarized in **Table 7**, the fastest transaction was processed within seconds, while the longest transaction was done in 248 minutes.

Table 7. Duration of Transactions for Select Group

Reference Chart	First Sender	Last Recipient	Duration of Transaction
Figure 4	MME	AMF	47 minutes
Figure 4	MME	LCM	66 minutes
Figure 4	KPA	KPA	3 minutes
Figure 4	SJE	SJE	2 minutes
Figure 5a	RPR	RPR	4 minutes
Figure 5a	SMH	SMH	0 minutes
Figure 5b	MME	AGB	111 minutes
Figure 5b	MIN	MAA	71 minutes
Figure 6	MME	MME	248 minutes
Figure 6	LOC	LRS	3 minutes
Figure 7	KPA	WBA	142 minutes
Figure 7	KBE	KBE	0 minutes

4.9. Illegal Gambling

4.9.a. Online Sabong

A total of 375 STRs with an aggregate amount of PHP746,557.00 were filed by covered person PQR on MBC, a Filipino residing in Puerto Princesa City, Palawan. Said suspicious transactions correspond to inter-account transfers and inward and outward remittances (domestic) credit to beneficiary account via electronic banking (**Table 8**). Based on PQR's report, MBC is allegedly involved in fund-flipping. Compared to the previous typology, however, MBC was observed to be transacting with multiple users. Further, the reporting covered person disclosed that one of MBC's transactions had a remark indicating "Talpak," which is a colloquial term for online sabong.

Table 8. Summary of Transactions of MBC

Transaction	Volume of STRs		Value of STRs	
	Count	Share to Total	Value (In PHP)	Share to Total
Inter-account transfers (same bank)	349	93.07%	633,817	84.90%
Outward remittance (domestic) credit to beneficiary account via electronic banking	25	6.67%	110,740	14.83%
Inward remittance (domestic) credit to beneficiary account via electronic banking	1	0.27%	2,000	0.27%
Total	**375**	**100.00%**	**746,557**	**100.00%**

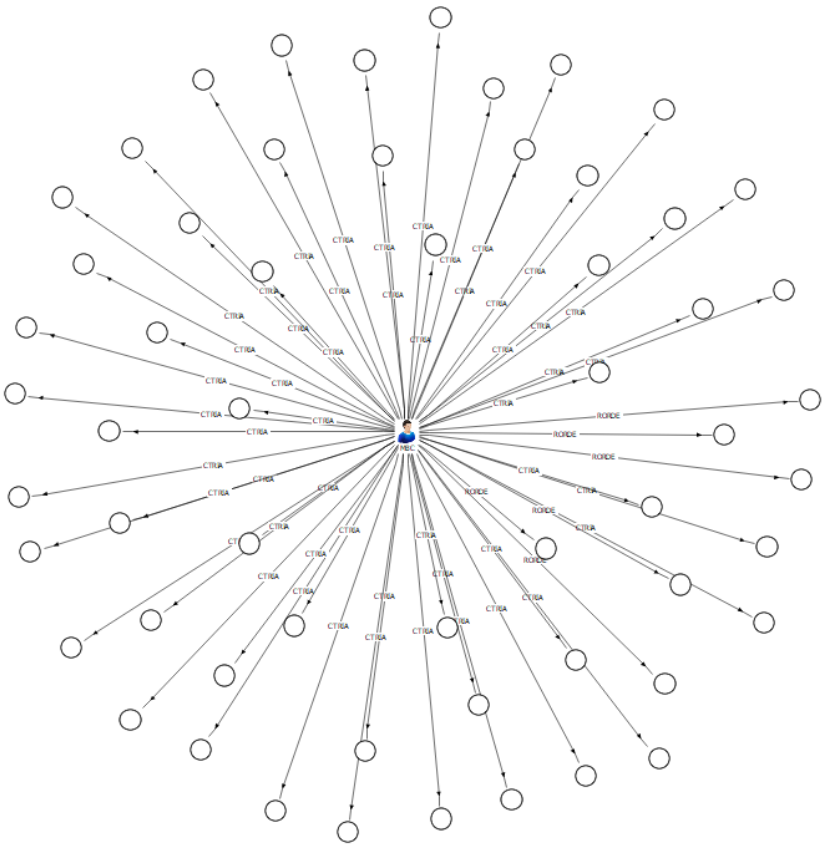
Based on the submitted STRs, MBC's transactions were completed between July 2020 and June 2021. Out of his 375 suspicious transactions, 310 transactions valued at PHP628,374.00 involved other individuals (**Table 9**). Based on STR count, MBC's counterparts are mainly located in Metro Manila,

Palawan, Laguna, Rizal, and Cavite. In terms of the amount transacted, Metro Manila ranked first, followed by Palawan, Laguna, Maguindanao, and Cavite.

Table 9. Summary of Transactions of MBC
By Location

Location	Volume of STRs		Value of STRs	
	Count	Share to Total	Value	Share to Total
Unknown	235	75.81%	443,294.00	70.55%
Metro Manila	36	11.61%	114,250.00	18.18%
Palawan	14	4.52%	18,520.00	2.95%
Laguna	6	1.94%	12,100.00	1.93%
Rizal	5	1.61%	9,350.00	1.49%
Cavite	5	1.61%	9,700.00	1.54%
Pampanga	3	0.97%	6,100.00	0.97%
Maguindanao	2	0.65%	10,000.00	1.59%
Bulacan	2	0.65%	2,060.00	0.33%
Bataan	1	0.32%	2,000.00	0.32%
Negros Oriental	1	0.32%	1,000.00	0.16%
Total	**310**	**100.00%**	**628,374.00**	**100.00%**

Figure 8. Transactions of MBC



A depiction of MBC's transactions in **Figure 8** shows that MBC was the only source of funds in his network. There were 65 suspicious transactions showing movement of funds to MBC's accounts. The corresponding STRs, however, show that the said funds also came from his personal funds.

4.9.b. Cockfighting show on television

In 2020, covered person PBY filed 46 STRs on MBO, a Filipino and resident of Manila. STRs submitted by PBY showed that MBO received regular but small-value remittances from an unusually high number of senders located in different countries, namely, United Arab Emirates, Italy, and Qatar (**Table 10**).

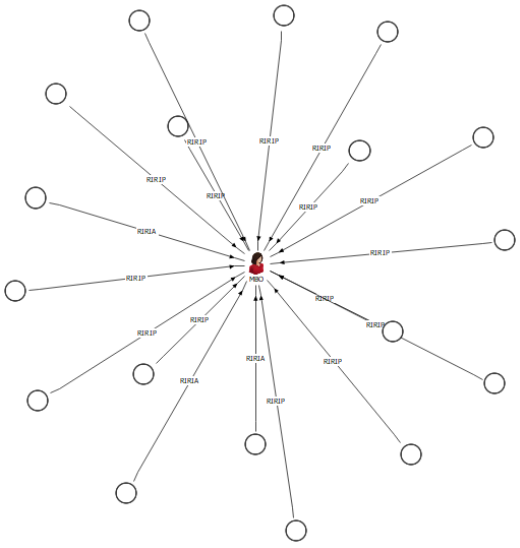
Table 10. Summary of Transactions of MBO
By Country

Country	Volume of STRs		Value of STRs	
	Count	Share to Total	Value	Share to Total
United Arab Emirates	38	82.61%	334,395.00	77.64%
Italy	6	13.04%	49,572.00	11.51%
Qatar	2	4.35%	46,759.00	10.86%
TOTAL	**46**	**100.00%**	**430,726.00**	**100.00%**

Based on PBY's investigation, MBO is associated with a cockfighting show on Philippine television and an online cockfighting betting operator that requires its participants to give a foreign Internet Protocol address.

Supporting documents collected by PBY on MBO revealed that her relationship with the senders is on a customer basis only. Consistent with this, said senders indicated "payment" as the purpose of transaction. In the Philippines, MBO cashed out the funds through three pawnshop chains.

Figure 9. Transactions of MBO



5. Conclusion and Recommendations

STRs associated with money mules show a monotonically increasing trend for the past years leading to 2022. The number of STRs spiked significantly in the year 2021 which coincided with the emergence of digital banking and electronic wallets. A significant share of the sample STRs were filed on the basis of two suspicious circumstances, namely "there is no underlying legal or trade obligation, purpose, or economic justification (SI1)" and "the amount involved is not commensurate with the business or financial capacity of the client (SI3)." In terms of value, the suspicious circumstance "the client is not properly identified (SI2)" topped the rank. Meanwhile, STRs on other predicate crimes constitute only 0.23% of the total volume and 0.03% of the total value of sample STRs. The top predicate crimes in terms of both volume and value appeared to be swindling (PC9).

It was noted that the suspected money mules in the Philippines utilize three modes of withdrawing funds: electronic cash cards, ATMs, and over the counter. Further, the suspected money mules were found to be residing in Metro Manila, Rizal, Nueva Ecija, Cavite, Bulacan, and Laguna.

As observed in the 821,979 STRs used in this report, the suspected money mules are involved in the following activities:

1. Fund transfers through self-service kiosks;
2. Opening of digital bank accounts and electronic wallets using sequential MINs;
3. Multiple cash and check deposits followed by large value withdrawals;
4. Cash and animal smuggling;
5. Opening an account on behalf of another individual;
6. Purporting to be a member of Marine Corps;
7. Receiving funds using drop accounts bought in the dark web;
8. Fund flipping; and
9. Illegal gambling, particularly illegal cockfighting.

Moving forward, the AMLC may consider including the typologies identified in the study on Targeted Intelligence Packaging Workshops with LEAs to further both parties' knowledge on this matter. In addition, the AMLC may consider issuing a notice discouraging promo gaming activities such as "Send Money Challenge" as this can be exploited for money mules, as discussed in subsection 4.8 Flipping of Funds. With the growing popularity of these alternative platforms, the need to raise awareness about the suspicious activities and modus operandi of money mules is underscored. Consequently, the following actions are recommended:

1. Dissemination of the report to external stakeholders such as relevant LEAs, supervising authorities, other government agencies, covered persons with Public-Private Partnership Agreement with the AMLC, and other FIUs;
2. Sharing the full version of this brief with internal AMLC groups/divisions; and
3. Publication of a redacted version of this report on the AMLC website.