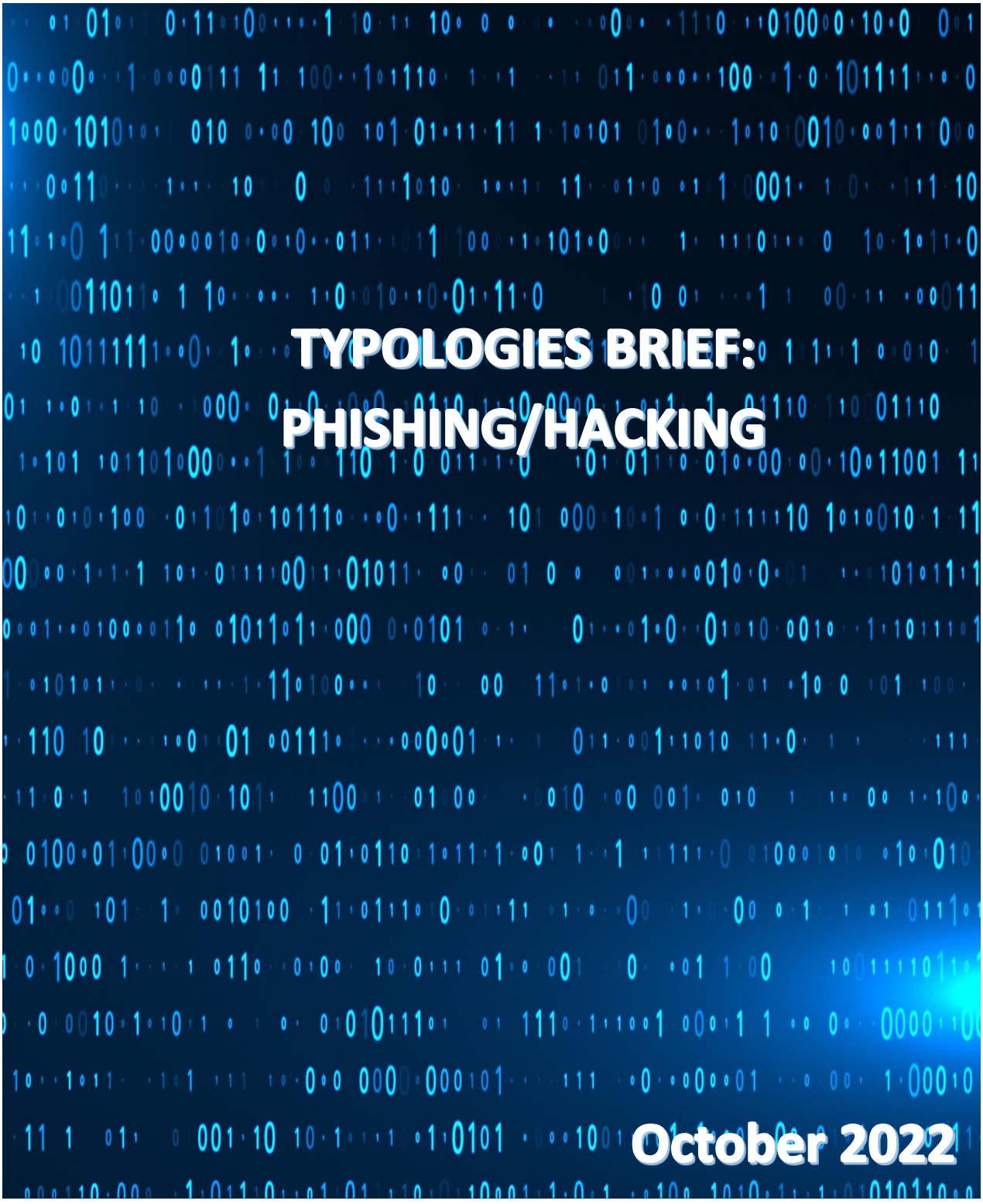

TYPOLOGIES BRIEF:
PHISHING/HACKING
October 2022

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Anti-Money Laundering Council (AMLC) prepared a typologies brief centering on phishing/hacking. This covers 50,521 suspicious transaction reports (STRs)[1] filed by covered persons (CPs) from the year 2011 to February 2022. The first part of the paper provides a descriptive analysis of the trends observed on the selected STRs. The second part focuses on the typologies observed using the sample STRs.

The descriptive analysis showed an increasing trend in the STRs involving phishing/hacking, except for the year 2020, where a considerable drop is observed. Majority of the STRs filed by CPs are for the following the reasons: swindling (65%) and violations of the Electronic Commerce Act of 2000 (23%). Certain suspicious indicators, such as the amount involved is not commensurate with the business or financial capacity of the client, are also among the reasons used by CPs. For common transactions used, majority are inter-account transfers, electronic cash card loading, credit card purchases/availment, and electronic cash card withdrawal.

It should also be noted that majority or 99.73% of the STRs are domestic transactions, while only 0.27% are international remittance transactions. About 50.45% of the total domestic transactions are reported from the National Capital Region, CALABARZON, Central Luzon, Central Visayas, Ilocos Region, Davao Region, and Western Visayas, while 44.62% of the transaction locations are unknown or cannot be determined given the available data. For international remittances, 27.21% of the transactions were from/sent to the United States of America (USA).

Noted typologies/suspicious indicators in the STR dataset include but are not limited to the following:

1. Transaction is not commensurate with the business or financial capacity of the client;
2. There is no underlying legal or trade obligation, purpose, or economic justification;
3. Account holders receiving calls from people pretending to be employees of banks or third-party callers who gather information on the client's account;
4. A group of people possibly related to each other receiving international inward remittance transactions on behalf of another person; and
5. Client withdrawing in cash, leaving no audit trail.

The typologies also include different types of phishing/hacking, such as vishing, SMS phishing, business e-mail compromise, and user account hacking, among others. It was also observed in some typologies that illegal proceeds were mostly transferred through banks and non-bank financial institutions, such as electronic money issuers and money service businesses.

With the increasing trend of STRs involving phishing/hacking, it is important for CPs to be cautious as perpetrators could be maximizing the use of technology in the facilitation of said crimes. Hence, it is recommended to share this brief with relevant AMLC units and external stakeholders,[2] such

[1] These include STRs with the following key words: phishing, hack, hacks, hacking, and pharming in the narrative field of the STRs filed from 2011 to February 2022.

[2] It is recommended to provide the redacted version of the study to external stakeholders.

as appropriate law enforcement agencies (LEAs), supervising authorities (SAs), AMLC Public-Private Program partners (PPPPs), and other financial intelligence units (FIUs) with transactional links to the Philippines to increase awareness of the presence of phishing/hacking domestically. In addition, a redacted version of the study is recommended to be posted on the AMLC website.

II. BACKGROUND AND SCOPE OF THE STUDY

Phishing is one of the most common fraudulent activities in the country. Various agencies have noted the importance of public awareness of this type of scam and have even posted phishing information on their websites. The Department of Justice – Office of the Cybercrime defined phishing as a "*cybercrime in which the perpetrator posing as a legitimate institution, such as a bank, an auction site, or an online commerce site, devises a message through phone call, electronic mail, or text message that lures individuals into providing sensitive data, such as personally identifiable information, banking and credit card details, and passwords. It is very often that the perpetrators indicate a sense of urgency in phishing messages, such as the threat of account suspension, to motivate the user to take the bait*."[3] In addition, the Bangko Sentral ng Pilipinas issued a primer on "Protect Yourself from Fraud and Scam," where it was mentioned that phishing is one of the common types of fraud and scam.[4]

This study covers 50,521 selected STRs filed by CPs from the year 2011 to February 2022. This paper intends to provide a descriptive analysis of the trends as well as describe the typologies observed using the sample STRs.

III. METHODOLOGY AND LIMITATIONS

Descriptive analysis was performed on the extracted STRs filed by CPs. Primary basis for STR selection is the presence of either one or a combination of keyword/s, such as phishing, pharming, hack, hacks, and hacking, in the narrative field of the STRs.

The STRs were initially checked for completeness and consistency especially in the address fields. The challenge, however, is on the standardization of the data. There is lack of uniformity among the STRs submitted by CPs as the address field is a text field, where the CP can encode any characters/numbers, subject to a length requirement. Hence, for international remittance transactions, in the absence of clear beneficiary and counterparty addresses, the correspondent bank address was used to determine the fund's potential country of source or destination. In cases where it is still not possible to identify the country, the word "UNKNOWN" was used.

For domestic transactions, the address used is the address of the branch of the CPs. There is, however, a case where the branch of a CP has multiple addresses, hence, the word "UNKNOWN" was also used. In cases where there is no CP's branch indicated in the STR, the address of the subject was used. In cases where the address of the subject is unknown or is not filled up or contains a mix of different places or in a different country, the word "UNKNOWN" was also used.

[3] https://cybercrime.doj.gov.ph/what-is-phishing/. Accessed on 23 September 2022.
[4] https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/Protect_yourself_from_Fraud_and_Scam.pdf. Downloaded on 23 September 2022.

The analyst then provided a trend analysis in terms of reporting year, reason for filing, and location. Further, the analysis is guided by the following confidence level matrix and estimative language usage:

Analytic Judgments and Confidence Levels

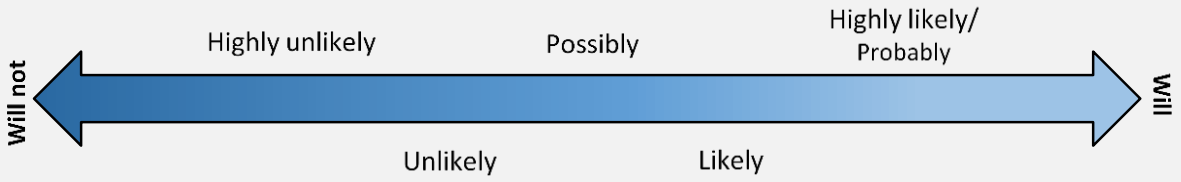
FIU Intelligence Assessments use phrases such as "we judge," "we assess," or "indicates" to convey analytical inferences (conclusions). These assessments are not statements of fact or proof and do not imply complete knowledge. Analytic judgments are often based on incomplete information of varying quality, 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 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.



Based on the data scope and limitations, a moderate level of confidence is given on the analytical judgments presented in the succeeding discussions pertaining to results of analysis.

CAVEAT

It should be noted that the data provided in this report should not be interpreted as an assessment of the full amount of proceeds on phishing/hacking. The actual volume and amount of proceeds may be larger than represented in the sample. In addition, the study also considered all

consummated and attempted transactions reported to the AMLC. Moreover, the statements in the study are not conclusive but are more descriptive of what has been observed on the gathered STR data. These STRs also need further verification and more in-depth investigation to substantiate likely linkage to a certain crime, such as swindling and violation of Electronic Commerce Act of 2000, among others.

DEFINITION OF TERMS

Term	Description
STRs	Suspicious Transaction Reports Suspicious Transactions, as defined under Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001 (AMLA), as amended, refer to any transaction with covered persons, regardless of the amount involved, where any of the following circumstances exists: (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 the AMLA; (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 any money laundering activity or offense that is about to be committed, is being or has been committed; or (7) Any transaction that is similar, analogous, or identical to any of the foregoing.
CPs	Covered Persons A Covered Person refers to natural or juridical persons, supervised or regulated by the Bangko Sentral ng Pilipinas, Securities and Exchange Commission, Insurance Commission, and other covered persons defined under Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001 (AMLA), as amended.
Phishing	Phishing is defined as a "cybercrime in which the perpetrator posing as a legitimate institution, such as a bank, an auction site, or an online commerce site, devises a message through phone call, electronic mail, or text message that lures individuals into providing sensitive data, such as personally identifiable information, banking and credit card details, and passwords. It is very often that the perpetrators indicate a sense of urgency in phishing messages, such as the threat of account suspension, to motivate the user to take the bait."[5]
Pharming	Pharming refers to "redirection of a user to a fake website to steal personal information or account information details."[6]

[5] https://cybercrime.doj.gov.ph/what-is-phishing/. Accessed on 23 September 2022.
[6] https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/Protect_yourself_from_Fraud_and_Scam.pdf. Downloaded on 23 September 2022.

Vishing	Vishing refers to "voice calls, automated voice recording, or Voice over Internet Protocol (VoIP) from someone pretending to be an employee of a bank or a popular company and asking for account details."[7]

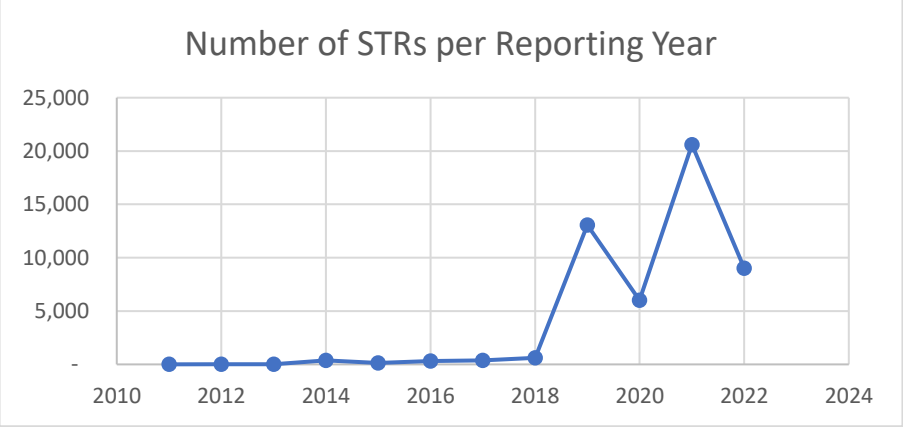
IV. DATA ANALYSIS/FINDINGS

A. PATTERNS AND TRENDS

Per Reporting Year

As can be seen in Figure 1, the number of STRs is generally increasing, and there is a significant surge in 2019. There is, however, a drop in the numbers reported in 2020. Nonetheless, this was followed by an abrupt increase in 2021.[8] In 2019, 68% of the total STRs for the year or 8,847 transactions were reported by EMI 1, an electronic money issuer, due to an investigation conducted by its Fraud Unit following the complaints raised by some banks involving account takeover where some bank accounts maintained with these banks were compromised and proceeds were transferred to different EMI 1A wallets. Other reasons for filing include online banking fraud, phishing, unauthorized transactions, and Internet fraud-online hacking, among others. In 2021, 64% of the total or 13,116 STRs were again reported by EMI 1 due to complaints pertaining to account takeover that involved incidents of EMI 1A customers as victims of phishing through various means, such as calls, SMS, e-mails, phishing links, fake EMI 1A pages, other fake pages in social media platform, chat via an e-commerce platform app, stolen phones, and other unknown means initiated by perpetrators.

Number of STRs related to Phishing/Hacking Per Reporting Year
Figure 1



Reason for Filing

The bulk of STRs in terms of volume count or 88% are filed by CPs under swindling and violations of the Electronic Commerce Act of 2000. The combined amounts of these top predicate crimes likewise dominated the total peso value of the STR dataset at 99%. Considering that phishing and hacking involve both fraud and technology, these reasons for filing are likely expected. Other

[7] Ibid.
[8] Year-on-year trend analysis considered the period 2011 to 2021 since the number of STRs filed for 2022 only covers January to February.

reasons used by CPs are the following suspicious indicators and predicate crimes: The transaction is similar, analogous, or identical to any of the foregoing (9%); the amount involved is not commensurate with the business or financial capacity of the client (2%); and others (1%). Others include reasons, such as fraud and illegal exactions and transactions; there is no underlying legal or trade obligation, purpose, or economic justification; and phishing, among others.

Number of STRs per Reason for Filing:
Table 1

REASON FOR FILING	NO. OF STRS	% AS TO THE TOTAL NO. OF STRs	PHP AMOUNT (in millions)	% AS TO THE TOTAL AMOUNT
SWINDLING	32,625	65%	15,689.1	96%
VIOLATIONS OF THE ELECTRONIC COMMERCE ACT OF 2000	11,843	23%	482.3	3%
THE TRANSACTION IS SIMILAR, ANALOGOUS, OR IDENTICAL TO ANY OF THE FOREGOING.	4,621	9%	78.1	0%
THE AMOUNT INVOLVED IS NOT COMMENSURATE WITH THE BUSINESS OR FINANCIAL CAPACITY OF THE CLIENT.	957	2%	38	0%
OTHERS	475	1%	92.1	1%
TOTAL	50,521	100%	16,379.6	100%

Transactions Used in Phishing/Hacking

In terms of volume, most of the transactions involving phishing/hacking are inter-account transfers (24%), electronic cash card loading (20%), credit card purchases/availment (16%), and electronic cash card withdrawal (13%). In terms of peso value, the generic code “ZSTR” has the largest chunk at 95.4% as this includes an attempted transaction to deposit a bogus EUR250 million bank draft (approximately PHP15,205.8 million).

Common Transactions Used in Phishing/Hacking
Table 2

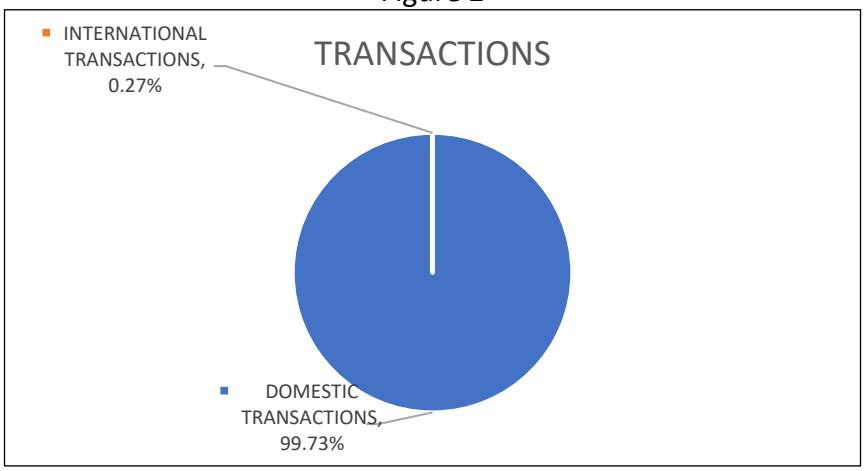
TRANSACTION	NO. OF STRS	% AS TO THE TOTAL NO. OF STRs	PHP AMOUNT (in millions)	% AS TO THE TOTAL AMOUNT
INTER-ACCOUNT TRANSFERS (SAME BANK)	12,111	24%	131.4	0.8%
ELECTRONIC CASH CARD – LOADING	10,337	20%	84.1	0.5%
CREDIT CARD PURCHASES/AVAILMENT	8,187	16%	97.9	0.6%
ELECTRONIC CASH CARD – WITHDRAWAL	6,472	13%	25.4	0.2%
BILLS PAYMENT – DEBIT MEMO	3,164	6%	14.6	0.1%
STR TRANSACTIONS (ZSTR) [9]	2,414	5%	15,625.3	95.4%
ELECTRONIC CASH CARD – PURCHASE	1,827	4%	32.9	0.2%
OUTWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	1,764	3%	18.6	0.1%
DEPOSIT – CASH	1,623	3%	49.8	0.3%
WITHDRAWALS – ATM	865	2%	9.8	0.1%
PREPAID CARD LOADING	467	1%	0.3	0.0%
LOAN AVAILMENT (REGULAR/FOREIGN CURRENCY DENOMINATED UNIT – CREDIT MEMO	268	1%	0.8	0.0%
OUTWARD REMITTANCE/TT (DOMESTIC) – CREDIT TO BENEFICIARY'S ACCOUNT	265	1%	7.4	0.0%
INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	234	0%	6.3	0.0%
OUTWARD REMITTANCE/TT (DOMESTIC) – ADVISE AND PAY BENEFICIARY	107	0%	0.8	0.0%
INWARD REMITTANCE (DOMESTIC) – ADVISE AND PAY BENEFICIARY	93	0%	1.8	0.0%
INWARD REMITTANCE (DOMESTIC) – FOR FURTHER CREDIT TO ANOTHER ACCOUNT	60	0%	1.5	0.0%
INWARD REMITTANCE (INTERNATIONAL) – CREDIT TO BENEFICIARY'S ACCOUNT	55	0%	50.8	0.3%
WITHDRAWALS – OTC	43	0%	35.4	0.2%
INWARD REMITTANCE (INTERNATIONAL) – ADVISE AND PAY BENEFICIARY	40	0%	1.2	0.0%
OUTWARD REMITTANCE/TT (DOMESTIC) – FOR FURTHER CREDIT TO ANOTHER ACCOUNT	36	0%	8.6	0.1%
OUTWARD REMITTANCE/TT (INTERNATIONAL) – CREDIT TO BENEFICIARY'S ACCOUNT	26	0%	36.8	0.2%
INWARD REMITTANCE (DOMESTIC) – CREDIT TO BENEFICIARY'S ACCOUNT	13	0%	3	0.0%
OTHERS	50	0%	135	0.8%
TOTAL	50,521	100%	16,379.60	100.0%

[9] The transaction code "ZSTR" shall be used if the subject is not an account holder of the reporting institution or is an account holder but has no monetary transaction with the CP at the time the suspicious activity is determined. (Item M [4] - Page 152 of the 2021 AMLC Registration and Reporting Guidelines)

Transactions

In terms of volume, only 0.27% of the transactions are international remittance transactions, while the bulk or 99.73% are domestic transactions. Total peso value follows a similar trend with domestic transactions, cornering 99.4%.

Type of Transactions (Domestic or International)
Figure 2



Transaction Type (Domestic/International)
Table 3

TRANSACTIONS	NO. OF STRS	% AS TO THE TOTAL NO. OF STRS	PHP AMOUNT (in millions)	% AS TO THE TOTAL AMOUNT
DOMESTIC TRANSACTIONS	50,385	99.73%	16,285.73	99.4%
INTERNATIONAL REMITTANCE TRANSACTIONS	136	0.27%	93.85	0.6%
TOTAL	50,521	100.00%	16,379.58	100%

International Transactions

Of the 136 international remittance STRs, 37 or 27.21% involved the USA. Further, of the 37 USA-related transactions, 30 are inward remittances, while seven (7) are outward. Transactional nexus with the USA amounted to PHP41.38 million, controlling a 44.1% share of the total international remittances' peso value. Nine (9) of the inward remittances to the USA involve a group of individuals potentially engaged in an illegal activity. The customers were allegedly receiving remittances on behalf of an unidentified[10] female customer. It was also noted that these customers have suspicious e-mail addresses in their records and are apparently related to each other because of their similar family names, residential location, and occupation. According to the report, these individuals are potentially linked to illegal activities, such as hacking and blackmailing.

[10] (Or identified). Three (3) out of nine (9) reports mentioned "an identified female," while the other six (6) reports stated "unidentified female."

No. of International Remittance Transactions (Inward/Outward) per Country

Table 4

COUNTRY	NO. OF STRS	% AS TO THE TOTAL NUMBER OF STRs	PHP AMOUNT (in millions)	% AS TO THE TOTAL AMOUNT
UNITED STATES OF AMERICA	37	27.21%	41.38	44.1%
UNKNOWN	12	8.82%	9.86	10.5%
KOREA[11]	11	8.09%	0.38	0.4%
UNITED ARAB EMIRATES	11	8.09%	3.30	3.5%
HONG KONG	8	5.88%	8.75	9.3%
SINGAPORE	8	5.88%	3.15	3.4%
VIETNAM	5	3.68%	1.83	1.9%
ITALY	4	2.94%	0.14	0.1%
SOUTH KOREA	4	2.94%	0.93	1.0%
UNITED KINGDOM	4	2.94%	4.03	4.3%
CANADA	3	2.21%	0.12	0.1%
CHINA	3	2.21%	1.32	1.4%
NORWAY	3	2.21%	0.04	0.0%
QATAR	3	2.21%	0.00	0.0%
FRANCE	2	1.47%	0.09	0.1%
MALAYSIA	2	1.47%	0.05	0.0%
SAUDI ARABIA	2	1.47%	0.99	1.1%
THAILAND	2	1.47%	0.57	0.6%
TURKEY	2	1.47%	11.37	12.1%
AUSTRALIA	1	0.74%	0.07	0.1%
GERMANY	1	0.74%	1.17	1.2%
INDONESIA	1	0.74%	0.58	0.6%
ISRAEL	1	0.74%	0.64	0.7%
KUWAIT	1	0.74%	0.98	1.0%
MEXICO	1	0.74%	0.36	0.4%
ROMANIA	1	0.74%	0.00	0.0%
SOUTH AFRICA	1	0.74%	0.15	0.2%
SPAIN	1	0.74%	1.54	1.6%
TAIWAN	1	0.74%	0.07	0.1%
TOTAL	136	100.00%	93.85	100.0%

[11] Only indicated in the address is the country "Korea." There are no additional details.

Domestic Transactions

Top locations of domestic transactions include the National Capital Region, CALABARZON,[12] Central Luzon, Central Visayas, Ilocos Region, Davao Region, and Western Visayas, accounting for 50.45% or 25,417 STRs in count. There is, however, a considerable number of transactions totaling 22,482 or 44.62% of total count with unknown location (i.e., the branch name of the CP was not indicated; there are multiple addresses and/or the subject's address is blank; or location cannot be determined). On the other hand, Region VII (Central Visayas) has the largest amount in terms of peso value with PHP15,320.8 million or 94% of the total. This, however, includes an unconsummated transaction reported by a CP branch located in said region, involving an attempt to deposit to an account a bogus EUR250 million bank draft equivalent to PHP15,205.8 million.

Number of Domestic Transactions per Region
Table 5

REGION	NO. OF STRS	% AS TO THE TOTAL NUMBER OF STRs	PHP AMOUNT (in millions)	% AS TO THE TOTAL AMOUNT
UNKNOWN	22,482	44.62%	489.7	3%
NATIONAL CAPITAL REGION (NCR)	12,876	25.56%	280.1	2%
REGION IV-A (CALABARZON)	4,907	9.74%	83.9	1%
REGION III (CENTRAL LUZON)	3,516	6.98%	44.8	0%
REGION VII (CENTRAL VISAYAS)	2,229	4.42%	15,320.8	94%
REGION I (ILOCOS REGION)	730	1.45%	5.4	0%
REGION XI (DAVAO REGION)	641	1.27%	9.5	0%
REGION VI (WESTERN VISAYAS)	518	1.03%	5.9	0%
REGION XII (SOCCSKSARGEN)	411	0.82%	4.2	0%
CORDILLERA ADMINISTRATIVE REGION (CAR)	355	0.70%	20.6	0%
REGION V (BICOL REGION)	347	0.69%	3.0	0%
REGION II (CAGAYAN VALLEY)	326	0.65%	5.2	0%
REGION X (NORTHERN MINDANAO)	325	0.65%	2.4	0%
REGION VIII (EASTERN VISAYAS)	180	0.36%	4.2	0%
MIMAROPA REGION	165	0.33%	2.4	0%
REGION XIII (CARAGA)	150	0.30%	0.9	0%
REGION IX (ZAMBOANGA PENINSULA)	137	0.27%	1.9	0%
AUTONOMOUS REGION IN MUSLIM MINDANAO (ARMM)	90	0.18%	0.9	0%
TOTAL	50,385	100.00%	16,285.7	100%

B. TYPOLOGIES and SUSPICIOUS INDICATORS

The following typologies/suspicious indicators include the actual names, locations, and surrounding suspicious circumstances of the subjects identified in the STRs filed by various CPs. Typologies are identified based on the number of reports on the suspicious activity/transactions,

[12] CALABARZON refers to the region comprising the following five (5) provinces: Batangas, Cavite, Laguna, Quezon, and Rizal.

as well as the significance of the amounts involved in the transaction reported. It should be noted that these cases are solely based on gathered STRs, hence, further intelligence-gathering and investigation are needed to substantiate the likely linkage to phishing/hacking.

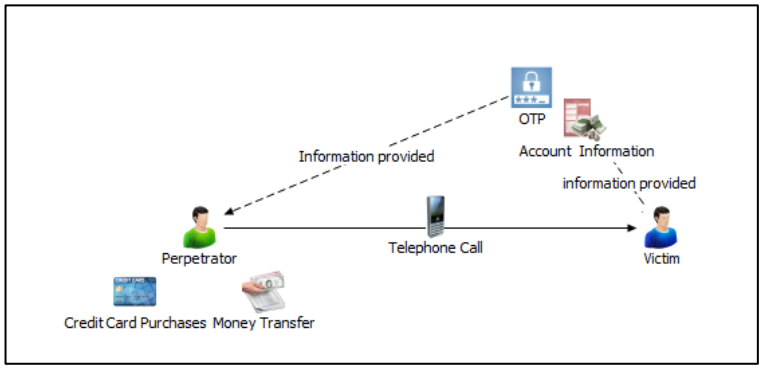
1. Account holders receiving calls from people pretending to be employees of banks to gather information (examples of vishing)

    a. The client received a call from someone pretending to be a Bank A employee inquiring on a transaction made on an e-commerce platform. The caller advised the client that she would be sending a new user ID and password to access the client's Bank A account. The client reported that he did not receive said SMS and the alleged Bank A employee can no longer be contacted. It was noted that the alleged Bank A employee knew the client's information even his last balance and that a one-time password (OTP) used to amend the client's mobile and e-mail address information was confirmed to have been shared to the caller, resulting in several transactions without notification to the actual account holder.

    The total amount scammed was PHP1.6 million, involving 157 transactions.

    b. The client became aware that his account was compromised because he received a call from an alleged Bank B employee, informing him that there were various transactions recorded on his account. The alleged Bank B employee (caller) said that the bank will send an OTP, which the client should provide to the caller in order to secure his account. The client allegedly provided the OTP as instructed by the caller. Based on the review of the client's accounts, there were various transactions that included a debit from his dollar account, where the nature of transaction is dollar conversion to peso via mobile application. The converted amount was credited to his peso account followed by three (3) debit transactions from the same account totaling PHP663,000.00, which were all credited to the account of one person (the likely perpetrator).

Illustration of Account Holders Receiving Calls from People Pretending to be from Banks
Figure 3



2. Disclosing information to a third party via call (another example of vishing)

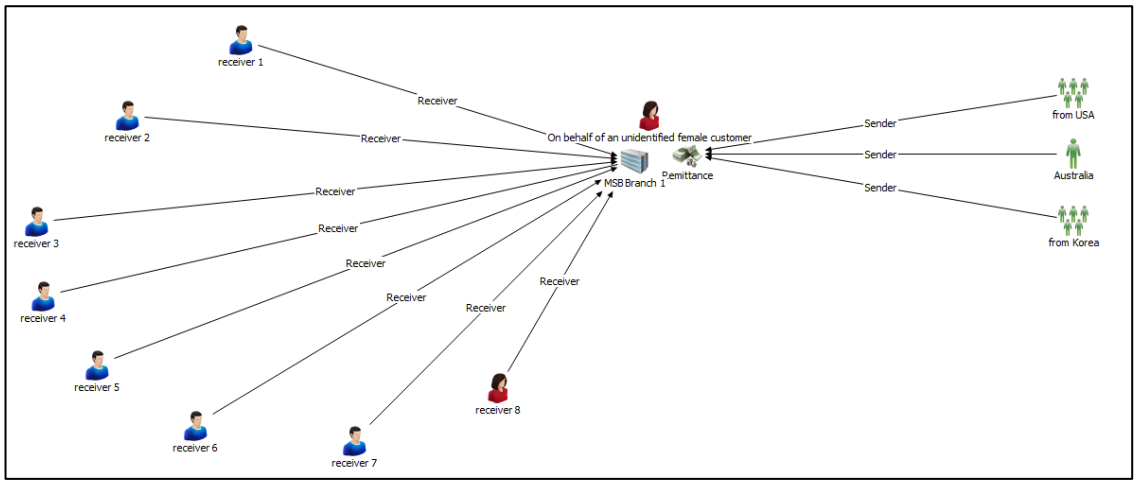
   A client reported various unauthorized online transactions. The investigation revealed that the online transactions were not within the transaction history of the client. The client, however, admitted to disclosing her account details to a third party over a call prior to the unauthorized transactions, which caused her account to be compromised. This involved 81 credit card purchases/availment, amounting to PHP125,108.00.

3. International inward remittances received on behalf of a person by a group of people possibly related to each other

   A group of individuals were reported as potentially engaged in an illegal activity. These alleged customers were receiving remittances on behalf of an unidentified[13] female customer. Various senders of this group were foreign males from the USA, Korea, and Australia, in which the declared relationship (as family) was quite questionable. Most of the transactions were claimed simultaneously on the same day at MSB A Branch in a province in Central Luzon, while other transactions were collected using the MSB A Service App. It was also noted that these customers have suspicious e-mail addresses in their records and are apparently related to each other because of their similar family names, residential location, and occupation. According to the report, these individuals are potentially linked to hacking and blackmailing activities.

Illustration of a Group of People Receiving Remittance on behalf of Another Person

Figure 4

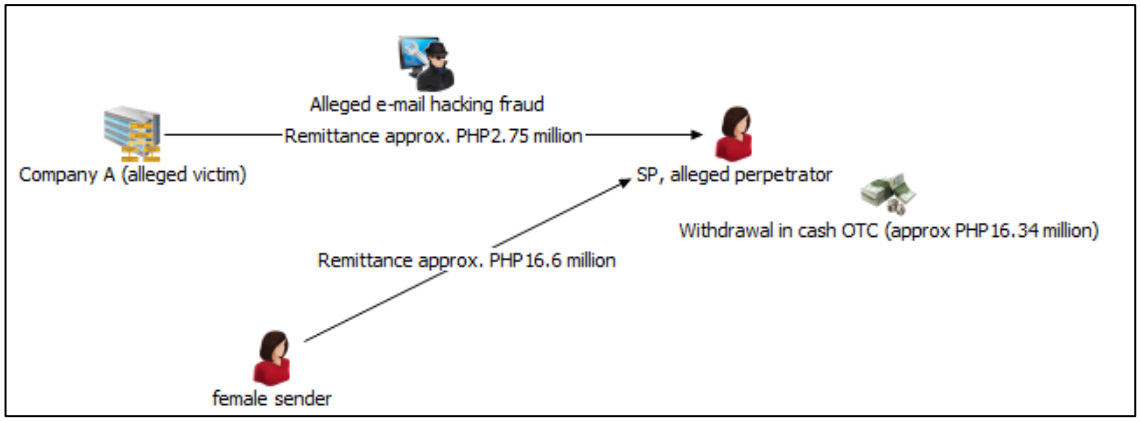


[13] (Or identified). Five (5) out of 19 transactions mentioned "an identified" female customer though majority of the transactions indicated "unidentified" female customer.

4. Client's withdrawal in cash, leaving no audit trail

   A customer's account was a subject of an investigation because of a remittance cancellation due to an alleged e-mail hacking. Said remittance came from a company and was allowed to be credited to the customer's DBA account, SP 1, as the client previously provided documents, such as a condominium reservation agreement and price table, and a franchise agreement with an accredited remittance partner. Apart from these, there were three (3) remittances from a female sender, totaling PHP16.6 million credited to the customer's DBA account. Correspondingly, cash withdrawals ranging from PHP90,000 to PHP5 million or totaling PHP16.34 million were likewise transacted. The client claimed that the female sender is her friend, and the remittances were intended for financial aid on the proposed franchise of an MSB B outlet and for the purchase of two (2) condominium units. Her transactions and business papers, however, revealed that no other transactions pertained to her remittance agent business or trading. Given this information, her transactions were reported on the basis of the recalled remittance allegedly due to e-mail hacking fraud and questionable remittances with significant amounts that were all withdrawn over the counter in cash, leaving no audit trail.

Illustration of the Client Withdrawing in Cash OTC
Figure 5



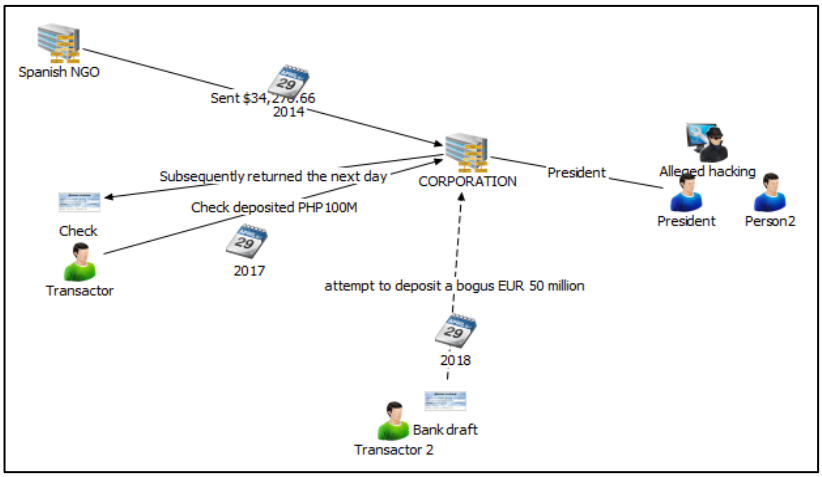
5. Suspicious Indicators: Not commensurate with the financial capacity of the client

   a. A CP received a report from Bank C regarding unauthorized fund transfers, involving the account of their client, Ms. B, due to a confirmed phishing incident. The funds credited to her account were either subsequently withdrawn via ATM or transferred to other accounts. Historical review of the account showed inflows in cash deposits and online transfers (unknown senders/recipients for remittance transactions) that ranged from PHP300.00 to PHP100,000.00, which are beyond the declared profile of the client. The client merely declared an online business and a grocery store (unregistered business) as sources of funds with a monthly income of PHP50,000.00.

b. A bank noted three (3) material transactions of a construction company, Company B, that were deemed not commensurate with its business or financial capacity. The transactions consist of an inward remittance of USD34,276.66 (EUR24,914) from a Spanish Non-Governmental Organization (NGO); a check deposit of PHP100 million that was subsequently returned the next banking day; and an attempt to deposit a bogus EUR50 million bank draft, purportedly issued by a Foreign Bank. It was also disclosed that the inward remittance of USD34,276.66 is the subject of a complaint due to an alleged fraud. The complainant claimed that this was supposedly for the account of a domestic NGO. Online search revealed that a case of estafa was filed against Company B and its president, Mr. X. Mr. X along with another individual was arrested by the National Bureau of Investigation for allegedly stealing PHP6 million from the Typhoon Yolanda aid. Both were accused of hacking into the e-mail addresses of a domestic NGO and a Spanish NGO so that the money was not deposited into the bank account of the domestic NGO but the account of the construction company.

Illustration of the Transaction of a Corporation

Figure 6



c. The client works as a team leader and "code stockist" of Marketing Company A. Based on the review of the client's account, there were 138 cash deposits, 356 Internet fund transfer credits, 11 international and domestic inward remittances, and 143 bills payment credits. Said credits were payments from members and referrals. The client's customers buy codes for the activation of their Marketing Company A account to become an official member. Based on the report of the CP, Marketing Company A's business model looks like a pyramid scheme as the company does not have products to sell as the business relies on the recruitment of people. There were two (2) ways to earn: (1) through captcha encode (This does not require a software installation and is mostly used by websites to prevent hackers and spammers from immediately doing a particular action, using script or bots. Criminals prefer bots to hack passwords in various accounts and spam comments in blogs); and (2) by inviting people. The volume of the transactions noted are suggestive that the account is being used as a conduit to

facilitate the seemingly pyramiding activity of the company. Likewise, said transactions were grossly not commensurate with the client's declared economic profile.

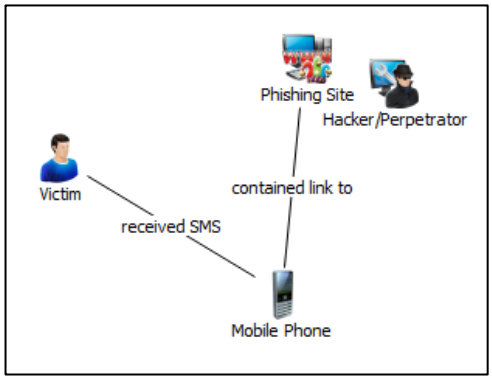
These involved 648 transactions, amounting to PHP771,054.00.

d. The Bank received a report against the client, Mr. Y, regarding unauthorized fund transfers due to a confirmed phishing incident, involving a savings account owned by a Bank D client. Review of the Bank D client's account disclosed that there were 13 online fund transfers, ranging from PHP2,500 to PHP50,000 to the savings account of Mr. Y. Examination of the account of Mr. Y showed several transaction inflows composed of cash deposits, online payments, and fund transfers that are not consistent with the declared profile and source of funds of the customer, while transaction outflows consist of withdrawals via OTC and ATM, and transfers to other deposit accounts. Upon inquiry on the source of funds credited to his account, Mr. Y claimed that they were from his parents. He also denied connections with or knowledge of the Bank D client and admitted sharing his account number to his family and friends.

6. Suspicious Indicator: No underlying legal or trade obligation, purpose, or economic justification

a. This pertains to a case of SMS Phishing. The customer reported that they received an SMS pretending to be from EMI 2 that contained a link to a phishing site. After the customer clicked the link, the account was subsequently accessed without authorization. The perpetrator successfully logged in and transferred funds from the user's account.

Illustration of SMS Phishing
Figure 7



b. The CP received an e-mail from a complainant, informing that he was a victim of an e-mail hacking and that the CP's client, Ms. C, was the alleged recipient of the funds. Based on the customer information record, Ms. C is a direct seller of a cosmetic products company. The branch could not contact the client through her given contact numbers, thus the CP deemed that the client's transactions have no underlying legal or trade obligation, purpose, or economic justification and are not commensurate to the

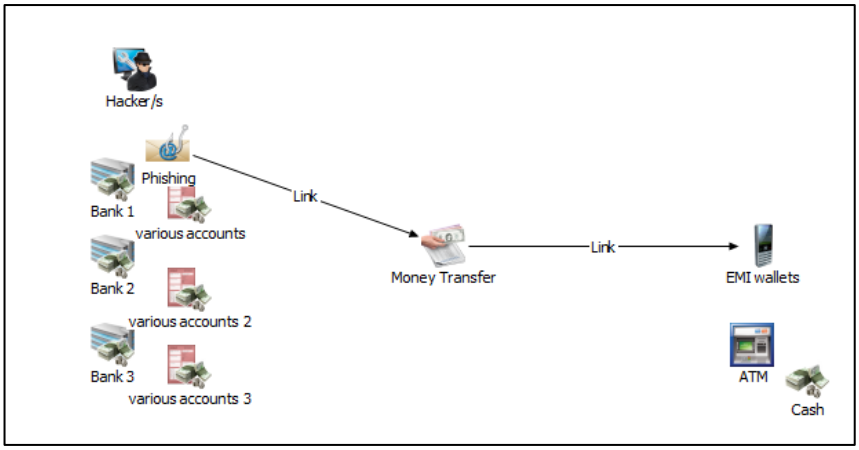
declared business or financial capacity. Ms. C has three (3) cash deposits, amounting to PHP276,641. A generic-coded STR (ZSTR) was likewise filed against Ms. C.

7. Account takeover, involving electronic money issuer (EMI) wallets

   a. Perpetrators are the owners of the EMI 1A wallets

   EMI 1 reported 8,847 transactions in 2019, following its investigation of complaints raised by some banks involving account takeover, where some bank accounts maintained by these banks were compromised and proceeds of the activities were transferred to various EMI 1A wallets. Said transfers were subsequently debited via ATM withdrawals, fund transfers, cash outs, and send money transfers. The accounts were compromised through hacking, using phishing methods to capture details necessary for transactions. The balances of these accounts were transferred to EMI 1A wallets, using the banks' online banking application.

Illustration of Account Takeover involving EMI
Figure 8



   b. Victims/perpetrators are the owners of EMI 1 wallets

   In 2021, EMI 1 reported 13,116 transactions, involving various EMI 1A customers who are victims of account takeover. These include incidents of EMI 1A customers falling victim to phishing through calls, SMS, e-mails, phishing links, fake EMI 1A pages, other fake pages via social media platform chat or through an e-commerce platform app, lost/stolen phones, and other unknown means initiated by perpetrators. Proceeds of funds were coursed through banks and non-bank financial institutions under various modes, such as send money, buy load, online payment, bills payment, web pay, ATM withdrawal, scan to pay, via EMI 1A padala,[14] and other means. The reported customers

[14] This is a service provided to users to send money to non-EMI 1 users.

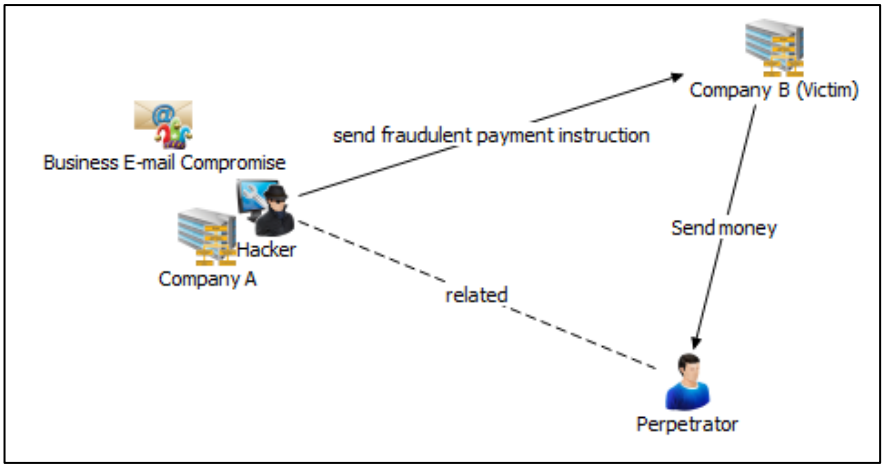
are the alleged fraudsters as they are the recipients of funds or their used mobile telephones were registered under identified fraudster devices.

8. Business e-mail compromise

Based on ACG-Cyber Security Bulletin No. 107: Business E-mail Compromise Attack, "business e-mail compromise is a form of phishing attack, where the cybercriminal impersonates an executive and attempts to get an employee, customer, or vendor to transfer funds or sensitive information."[15]

There are noted transactions involving this type of phishing where perpetrators hack the e-mail accounts of victims to send fraudulent payment instructions. These involve transactions, such as check deposits, outward international remittances, outward domestic remittances, and STR transactions. The client involved is the recipient or sender of the fraudulent payment.

Illustration of a Business E-mail Compromise
Figure 9



Internet e-mail hacking (another case of business e-mail compromise)

A perpetrator hacked the e-mail account of the victim's agent who is based in Hong Kong and e-mailed the victim with the instruction to send payment to the account of an alleged director of the agent's company, Ms. D. The purpose of the deposit was not known although the victim is the owner of Company C, a cargo/freight forwarders company based in the Philippines. The victim's company and the agent's company are business counterparts in carrying cargo shipment from the point of origin to point of destination. After several days, the agent responded through e-mail to the victim's secretary that they never sent a request to deposit funds or, much more, to pay a client for them. This prompted the victim to re-visit the depository branch, and she found out that the account

[15] https://acg.pnp.gov.ph/main/cyber-security-bulletin/228-acg-cyber-security-bulletin-no-107-business-email-compromise-attack.html. Accessed on 13 October 2022.

of Ms. D is in the Philippines. The victim then realized that she had communicated with an e-mail hacker and that she was deceived to pay a large amount for a fraudulent transaction. Historical review of the movement of the cited account disclosed that the questionable funds were subsequently withdrawn via ATM and OTC.

9. Hacking of user account in social media platform

    a. Reports were submitted regarding the client, Ms. E, where her account was used to illegally transfer funds by hacking the social media user account of a male victim and defrauding the victim's wife to remit PHP130,000 via a convenience store. This involved six (6) STRs and were reported by two (2) CPs.

    b. The CP received a complaint on the alleged involvement of their client, Ms. F, in an online scam conducted by hacking a social media account. Said client worked as a risk enforcement/marketing officer of a company. Per CP's review of the statement of account, most of the transactions are salary credits, but there were two (2) online transfers, amounting to PHP28,000 and PHP50,000 that were noted to deviate from and not within the pattern of client's past transactions. The client is no longer connected with her employer and cannot be contacted to verify the true origin of the funds and purpose of the transaction.

V. CONCLUSION AND RECOMMENDATION

The STRs involving phishing/hacking showed a generally increasing trend, except for the year 2020 when a slight drop in STRs was noted. Majority of the STRs filed are for the following reasons: swindling (65%) and violations of the Electronic Commerce Act of 2000 (23%). Other suspicious indicators, such as the amount involved is not commensurate with the business or financial capacity of the client, are also among the reasons used by CPs. For common transactions used, majority are inter-account transfers, electronic cash card loading, credit card purchases/availment, and electronic cash card withdrawal.

It should also be noted that majority of the STRs or 99.73% are domestic transactions, while only 0.27% are international remittance transactions. Majority or 50.45% of the total domestic transactions are reported from the National Capital Region, CALABARZON, Central Luzon, Central Visayas, Ilocos Region, Davao Region, and Western Visayas, while 44.62% of the transactions' locations are unknown or cannot be determined based on available data. For international remittances, 27.21% of the transactions were from or sent to the USA.

Typologies/suspicious indicators noted in the STR sample include but are not limited to the following:

1. Transaction is not commensurate with the business or financial capacity of the client;
2. There is no underlying legal or trade obligation, purpose, or economic justification;
3. Account holders receiving calls from people pretending to be employees of banks or third-party callers to gather information on the client's account;
4. A group of people possibly related to each other receiving international inward remittance transactions on behalf of another person; and

5. Client withdrawing in cash, leaving no audit trail.

The typologies also include different types of phishing/hacking, such as vishing, SMS phishing, business e-mail compromise, and hacking of user accounts in social media platforms, among others. In addition, it was also observed in some of the typologies that proceeds of these crimes were mostly transferred through banks and non-bank financial institutions, such as electronic money issuers and money service businesses.

With the increasing trend of STRs involving phishing/hacking, it is important for CPs to be cautious as perpetrators could be maximizing the use of technology in the facilitation of said crimes. Hence, it is recommended to share this brief with relevant AMLC units and external stakeholders,[16] such as appropriate LEAs, SAs, AMLC PPPP partners, and other FIUs with transactional links to the Philippines to increase awareness of the presence of phishing/hacking domestically. In addition, a redacted version of the study is recommended to be posted on the AMLC website.

[16] It is recommended to provide the redacted version of the study to external stakeholders.