Environmental Scanning: Cybercrime Threats and Perpetrators

September 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cybercrime-related incidents in the country has proliferated brought about by digitalization and the COVID-19 pandemic. The Anti-Money Laundering Council (AMLC) conducted an environmental scanning that aims to determine the extent of cybercrimes specifically on the perpetrators that proliferate such crimes. Environmental scanning using past studies as well as recent news revealed that Nigerian-related crimes are cause for concern due to its increasing prevalence evidenced by the volume and value of suspicious transaction reports (STRs) from year 2009. The year 2020 saw a considerable increase of around 668.2% to 17,178 STRs from the previous year's 2,236. In terms of gross amount, the pandemic period revealed a 261.1% increase to PHP998.6 million of the total transactions from 2019's PHP276.6 million. Conversely, there was a tapering on both counts in year 2021.

A total of 30,967 STRs valued at PHP3,262.1 million filed by various covered persons (CPs) between 1 January 2009 to 31 December 2021 were considered in the study. Banks largely facilitated a 96.2% share (PHP3,139.3 million) for the covered years of 2009 to 2021. This is followed by electronic money issuers (EMIs) and money service businesses (MSBs) at 1.2% (PHP39.8 million) and 0.9% (PHP29.7 million), respectively. Thus, banks, specifically commercial/non-expanded commercial banks, are the main channels for the delivery of big-ticket proceeds likely related to Nigerian-related crimes. For moderate amount transactions, EMIs, MSBs, and pawnshops are generally used.

In terms of international transactions, majority of inflows came from the United States of America (USA) tallied to PHP71.4 million or about 46.7% of the total inward remittances. Outflows, on the other hand, were transmitted primarily to beneficiaries with addresses in Nigeria as it posted PHP28.4 million or 39.5% of the gross amount.

Domestic transactions, on the other hand, were dominated by reports from the National Capital Region (NCR), posting 11,640 or a 37.6% share of the total count and PHP2,162.1 million or a 66.3% share of aggregate peso value. This is followed by Region IV-A (CALABARZON) and Region I (Ilocos Region). In terms of value, a considerable number of the NCR total is due to suspicious activities from Quezon City, amounting to PHP1,211.4 million or a 56.0% share of the PHP2,162 million sum.[1] By count, the city of Las Piñas garnered the maximum quantity at 4,405 STRs or 37.8% of the total.

Submitted STRs are grouped based on the CP's reason for filing the report – either through suspicious circumstances (SC) or predicate crimes (PC). Notably, in line with the increasing link to digitalization and cybercrimes, violations of Electronic Commerce Act of 2000 corner the lion's share of both volume and value at 7,573 (24.5%) and PHP623.4 million (19.1%).

Using specific keywords in the narratives, the top five (5) illegal activities identified in this study in order of value are Others - Unsubstantiated Transactions valued at PHP1,499.6 million (46.0%) of the aggregate, followed by advanced fee fraud at PHP1,086.4 million (33.3%), unauthorized transactions from mostly compromised accounts at PHP308.6 million (9.5%), pass through/money mules at PHP101.3 million (3.1%) and package scam at PHP57.3 million (1.8%). The vulnerabilities of cryptocurrency to money laundering may also be focused on as crypto-related transactions, using keywords such as "crypto," "binance," "bitcoin," and "external wallet" for this study, generated 1,503 STRs with the corresponding value of PHP 132.7 million.

Further, this study identifies typologies based on the significance of the amounts involved and/or frequency of reports on the suspicious activity/scheme as well as significance of the crime involved. These include but not limited to inconsistent transactional activities with the subject's business profile; package, romance, lottery scams with pass-through accounts; deposits from unverified sources; involvement in illegal drugs as well as African drug syndicates; association with bank hacking incidents;

[1] The cities of Parañaque, Makati, Las Piñas, and Manila trail behind Quezon City.

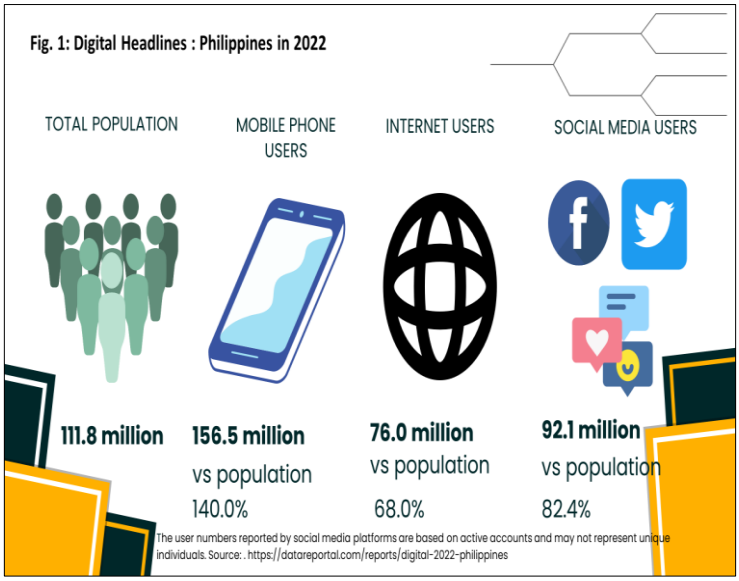
and recruitment of money mules. While these types of crimes have been brought to the attention of the country's law enforcement agencies, the continued proliferation of Nigerian-related crimes call for more stringent monitoring of subjects identified in the STRs.

The study concludes heightened monitoring of Nigerians identified in this study as well as those individuals with financial transactions with the perpetrators. There is a need to increase public awareness of the pervasive as well as emerging threats relative to these types of crimes perpetrated by Nigerian syndicates which are primarily done online. In addition, there are some banks and non-bank financial institutions (including branches) that do not have complete addresses and/or the submitted STR details on the name fields of the subject, account holder and other persons, including addresses of the various name flags, are incomplete. Hence, there is a need to reiterate that CPs should observe proper know-your-customer and customer due diligence procedures. Noting the lag in reporting of the unusual activities from the date of actual transactions, banks and other financial institutions are also encouraged to be more vigilant in tracking and immediately reporting suspicious accounts/transactions especially those with unverifiable identification documents.

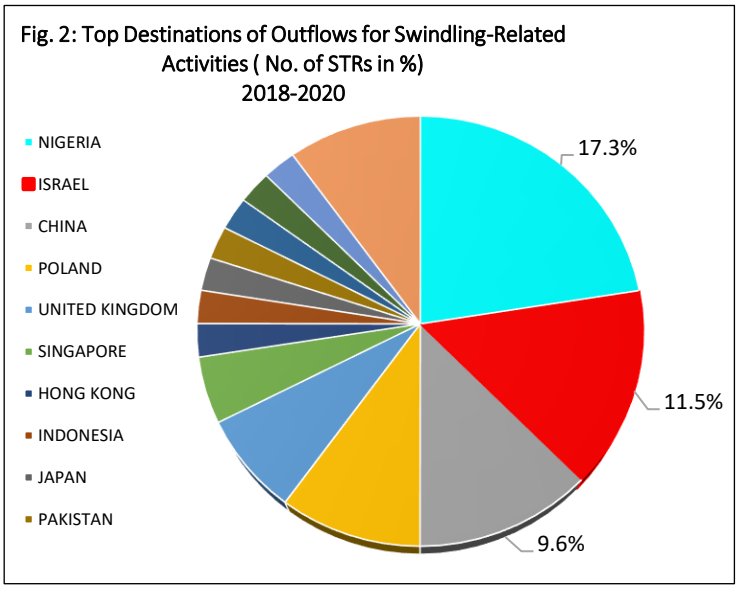
The study recommends the following: 1) encouragement of CPs to submit STRs on the Nigerian subjects and their cohorts; 2) involvement of the Asset Management Group of the AMLC to trace the assets of these scammers and forfeit the same in favor of the government agency both domestic and foreign, designated by the law, as well as, such other claimants as designated by the law, and with the ultimate objective of depriving these criminals of the proceeds of their crimes; and 3) communication of the results of the study to various stakeholders such as internal AMLC groups/divisions, appropriate law enforcement agencies (LEAs), supervising authorities (SAs), private sector participants of the AMLC's Public-Private Partnership Program (PPPPs), and respective financial intelligence units (FIUs) of other jurisdictions with transactional links to the country as identified in the study. A redacted version is also recommended to be posted on the AMLC website.

I. Introduction

The acceleration of digital transformation as well as the COVID-19 pandemic led to the increase in digital vulnerabilities and physical movement restrictions that translated to the proliferation of cybercrimes globally, which does not exempt the Philippines. To support this, Global Digital Report for the year 2022 stated that 5.0 billion (62.5%) of the estimated global population of 7.9 billion are Internet users whereas 5.3 billion (67.1%) are mobile phone users. For the Philippines, there are 156.5 million mobile phone users (140.0%) from the estimated population of 111.8 million as of January 2022, 76.0 million (68.0%) Internet users, and 92.1 million (82.4%) social media users (**Figure 1**).[2]



Relative to this, the Philippine National Police (PNP) cybercrime watch website ranked first online scams or swindling/estafa under Article 315 of the Revised Penal Code as among the country's top-recorded crimes followed by online libel and anti-video voyeurism.[3] While there was no indication of period coverage of the statistics captured from the PNP cybercrime website, it was mentioned that swindling/estafa has the most number of complaints in related news, covering the complaints investigated from 1 January to 30 November 2021.[4]



Concentrating on swindling-related activities, a study[5] by the AMLC revealed that Nigeria (**Figure 2**) emerged as the top destination of

[2] Notes from DataReportal stated that social media platforms are typically based on active user accounts and may not represent unique individuals such that one person may maintain more than one active presence on the same social media platform (i.e., "duplicate" accounts). Thus, figures for social media users may surpass that of the number of internet users, and in some instances may even exceed figures of the gross population. Retrieved from https://datareportal.com/reports/digital-2022-philippines (accessed 17 April 2022).

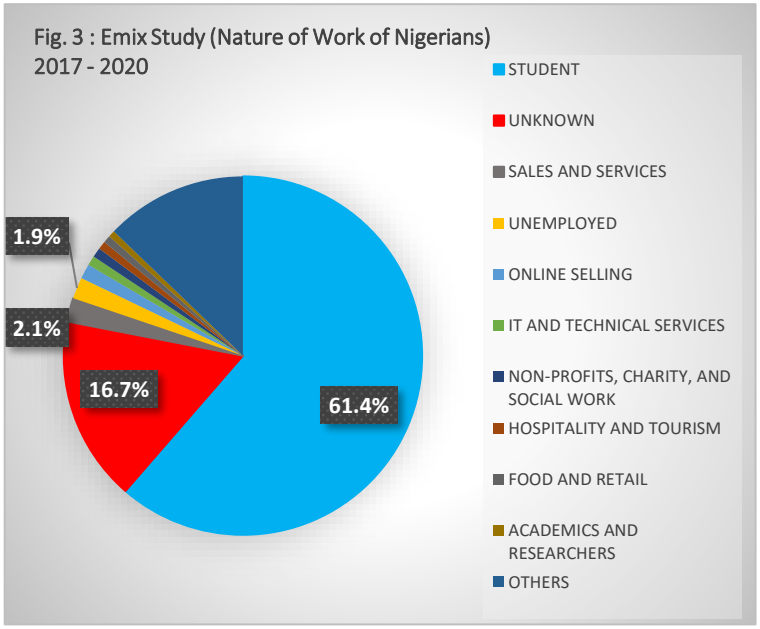
[3] Criminals have taken advantage of the anonymity offered by social media, telecommunication companies, and messaging applications as well as e-mails. Retrieved from https://cybercrimewatch.pnp.gov.ph/ (accessed 13 Jan 2022).

[4] Retrieved from https://journalnews.com.ph/pnp-cybercops-gain-headway-in-anti-cybercrime-drive-in-2021/ (accessed 13 January 2022).

[5] The AMLC's study "*An Assessment of the Philippines' Exposure to External and Internal Threats Based on Suspicious Transaction Reports for 2018 -2020*" is focused on gaining a deeper understanding of the country's risk and exposure to money laundering, terrorism financing and different predicate offenses by gathering information on the generation, movement, and behavior of illicit funds and by evaluating the threats originating within and outside the country's jurisdiction. Retrieved from http://www.amlc.gov.ph/images/PDFs/ASSESSMENT%20OF%20PH%20EXPOSURE%20TO%20EXTERNAL%20AND%20INTERNAL%20THREATS%20BASED%20ON%202018%20TO%202020%20STRS.pdf

funds (frequency-wise) at 17.3%,[6] representing proceeds of different types of fraud—investment scams, romance scams, and counterfeiting of financial documents. This is followed by Israel and China at 11.5% and 9.6%, respectively.

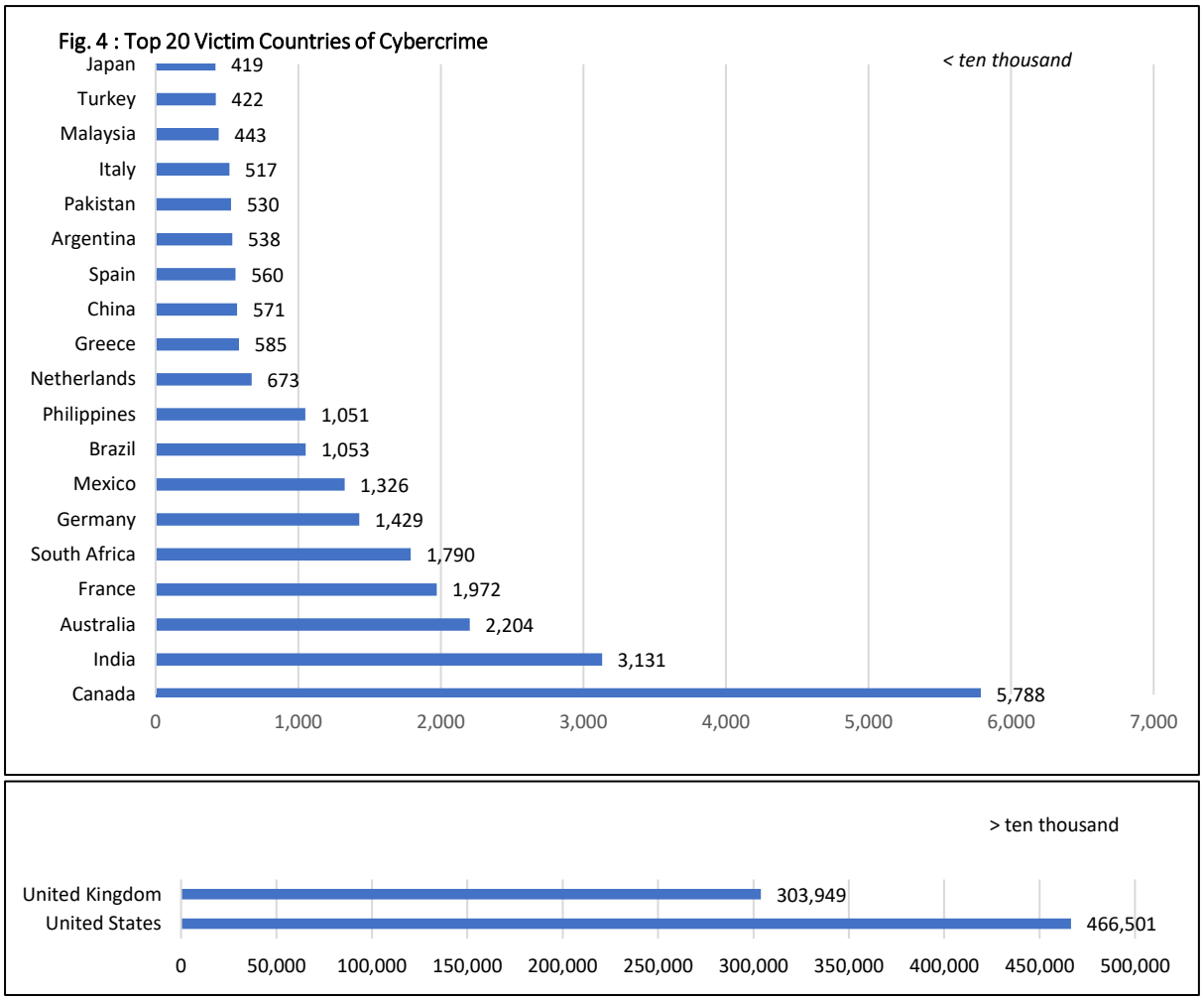
Further, the study by Emix, an EMI, was triggered due to a fraud case on two African individuals from Nigeria and Republic of Cameroon. From the 2,697 Nigerians reviewed and investigated, 55.6% or 1,499 of which were found to be engaging in suspicious transactions. Emix's monitoring covered the period 2017 to 2020, and transactions that found an increase of Nigerian nationalities involved in unlawful activities as well as a significant increase and deviation of transaction amounts over the years. This is quite remarkable, thus the need to monitor these high-risk individuals involved in unlawful activities based on actual cases and complaints. Notably, allowance from parents was the most common source of funds as 61.4% or 920 Nigerians, identified as students, comprised the 1,499 subjects. This is followed by 16.7% that did not indicate any nature of business and categorized as unknown, 2.1% that were under sales and services, and 1.9% that were unemployed (**Figure 3**).



Romance (love) scams are one of the crimes perpetrated online that government agencies, such as the National Bureau of Investigation (NBI) and the Bureau of Customs (BOC), have cautioned the public for a long time.[7] Specifically, news of arrests of Nigerian scammers can be seen in online news, whereas warning signs are discussed at the PNP-ACG website for public awareness.[8] High-profile cases related to Nigerian's involvement in Bank ABC and Bank XYZ hacking, money mules, drug-related transactions as well as syndicates warrant more focus on the crimes committed by these nationals, which will be discussed further in the typology section.

Analytics Insight identified Nigeria at the uppermost of its list of top 10 scamming countries worldwide in July 2021 followed by India, China, and Brazil.[9] Correspondingly, the Federal Bureau of Investigation's (FBI) Internet Crime Report for 2021 ranked the Philippines as 11th globally among countries most affected by Internet crime, the foremost of which are the number of complaints coming from the USA (466,501), United Kingdom (303,949), Canada (5,788), and India (3,131) (**Figure 4**).[10]

[6] This refers to nine (9) STRs out of the total 52 STRs categorized under swindling for the period 2018 to 2020. Retrieved from ibid.
[7] Retrieved from https://www.pna.gov.ph/articles/1013468 ; and https://www.pna.gov.ph/articles/1042140 (accessed on 13 January 2022).
[8] Retrieved from https://www.pressreader.com/philippines/sunstar-pampanga/20211102/281646783360885 (accessed 13 January 2022); https://guardian.ng/news/philippines-to-deport-three-nigerians-for-love-scam-fraud/ and https://www.pna.gov.ph/articles/1078817 (accessed 18 May 2022).
[9] The next six (6) countries consist of Pakistan, Indonesia, Venezuela, South Africa, Philippines, and Romania. Retrieved from https://www.analyticsinsight.net/top-10-scamming-countries-in-the-world-in-2021/ (accessed on 19 April 2022).
[10] This report indicates the top 20 countries by the number of total victims, compared to the United States. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 25 April 2022).



Apparently, Nigerians have caught global attention, and the Philippines is no exception due to subject nationality's involvement in cybercrimes in the country, specifically in scam/fraud-related schemes. These scams identified as romance scams, advance fee scams, inheritance/package scams, among others, are commonly referred to as 'Nigerian 419' scams since the first wave of these schemes came from Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code that outlaws the practice.[11]

The United Nations' Population Division's estimates in 2017 mentioned that around 15 million Nigerians are in diaspora. In the same trend, Pew Research Centre specified that 60 million Nigerians (or half of the adult population) planned to leave Nigeria by 2023, if it is a possibility. According to an analysis by PwC, "Nigerians have emigrated to practically all countries in the world, the topmost destinations of which are USA, United Kingdom, Cameroon, Niger, Ghana, Italy, and Benin, followed by Northern Ireland, Europe, Dubai, and South Africa."[12] The desire to leave is brought about by the need for economic improvement, and Nigerian migrants were able to integrate well in their host societies. These migrants continued to touch base with relatives, thus, establishing transnational networks. Nigerian emigration, however, earned the reputation of being highly criminalized due to the apprehensions of

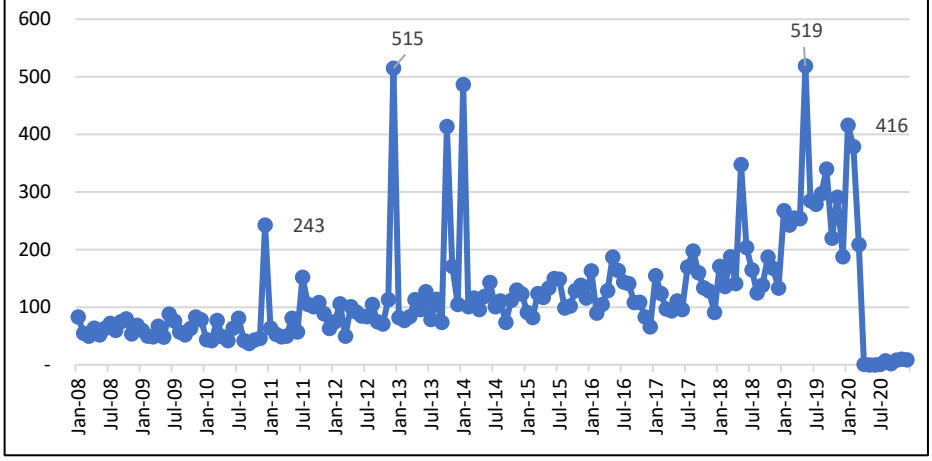
[11] The Nigerian 419 scam dates back to the late 19th century and is comparable to the Spanish Prisoner scam. In this ploy, businessmen were contacted and asked for assistance in smuggling an individual related to a wealthy family out of a prison in Spain in exchange for a hefty reward. However, prior to the promised reward, the victim is asked initially to shell-out a small amount of money (increasingly) to bribe the prison guards. Retrieved from https://pnpacg.ph/main/accomplishments/2-uncategorised/172-common-types-of-internet-fraud-scams (accessed on 10 Jan 2022).

[12] Retrieved from https://www.sunnewsonline.com/why-nigerians-are-emigrating/ (accessed on 17 April 2022).

Nigerians who use counterfeit records, who are involved in illegal agreements, and who participate in criminal activities.[13]

In the Philippines, Nigerians proliferate as students or tourists, the influx of which peaked in December 2012 and May 2019 (**Figure 5**).[14] Noted is the decline in arrivals during the pandemic in 2020 which may be due to the lockdown procedures implemented by the government to mitigate spread of COVID-19. The entire island of Luzon was placed under Enhanced Community Quarantine (ECQ) on March 16, 2020.

Fig. 5 : Visitor Arrivals to the Philippines (Nigerians)



Amid increasing incidence of online scams carried out by Nigerians, both operating within and outside the country and using residents as mules, the AMLC conducted a descriptive analysis of all available information related to Nigerian-associated crimes.

The study seeks to:

1. Assess the prevalence of Nigerian-related crimes in the country;
2. Provide a descriptive analysis of Nigerian-crime related information, using requests for information (RFIs) received and financial intelligence reports (FIRs) disseminated by the AMLC, as well as STRs involving Nigerian-related crimes;
3. Share the result of the study to relevant stakeholders, such as internal AMLC groups/divisions, appropriate LEAs, SAs, private sector participants of the AMLC's PPPP, and respective FIUs of other jurisdictions with transactional links to the country as identified in the study; and
4. Publish a redacted version of the study on the AMLC website.

The first part or the strategic analysis component contains the trends and patterns drawn primarily from observation/analysis of all available data relevant to the study. In addition, part two of the paper contains operational typologies leading to the possible identification of likely perpetrators that is intended for sharing internally and with relevant domestic agencies.

[13] In a study conducted by the International Organization for Migration, 81.0% of respondents indicated their desire to leave their community for economic reasons and move to non-African countries or urban settings within Nigeria. Retrieved from https://migrants-refugees.va/it/wp-content/uploads/sites/3/2021/05/2020-CP-Nigeria.pdf (accessed on 20 April 2021).
[14] Retrieved from http://tourism.gov.ph/tourism_dem_sup_pub.aspx (accessed on 12 April 2022).

II. Scope and Methodology

The study provides a descriptive analysis of STRs filed by various CPs in relation to Nigerian-related crimes. Also included in this report are typologies translated to an operational intelligence report drawn primarily from observation/analysis of all available data which lead to the identification of likely perpetrators. In detail, this research generated the total STRs[15] from the AMLC database in four (4) batches using the following:

1. STRs that contain "Nigeria" or "Nigerian" in the nationality of any name field (account holder or beneficiary or counterparty) or narratives that contain "Nigeria" or "Nigerian;"
2. Related names from RFIs received and FIRs disseminated by the AMLC from 2018 to 2021;
3. Nigerian listings from Emix's investigation performed in September 2020; and
4. Nigerians with travel histories from 2020 to 2021 sourced from the Bureau of Immigration (BI).

The STRs generated in four (4) batches were collated and checked with duplicates eliminated in Excel, using its unique transaction reference number as basis.[16] Likewise in the analysis, other literature sourced online, including news reports and other research or studies conducted in relation to the subject matter, were also considered.

A total of 30,967 STRs filed by various CPs between 1 January 2009 and 31 December 2021 were considered in the study. For a closer look on the submitted STRs, filed reports with Nigerian-related keywords are grouped according to the CP's basis for filing the report—either through suspicious circumstances (SC) or predicate crimes (PC). Of the aggregate number, 20,432 STRs or 66.0% of the entire dataset form part of the SC classification largely due to the SC, "*the amount involved is not commensurate with the business or financial capacity of the client*" (SI3) which registered the highest percentage share of 29.1% or counted at 9,000 STRs. In terms of value, however, the SC *"there is no underlying legal or trade obligation, purpose or economic justification"* (SI1), ranked first with PHP1,562 million (47.9%) value. Filed reports related to PCs, on the other hand, totaled 10,535 (34.0%) and PHP776.7 million (23.8%) in volume and amount, respectively. Notably, in terms of PC, violations of the Electronic Commerce Act of 2000 corner the lion's share of both volume and value at 7,573 (24.5%) and PHP623.4 million (19.1%).

It should be noted that 2,516 generic-coded STRs (ZSTRs) valued at PHP213.1 million form part of the dataset. While STRs with specific codes provide a definite description of the type of transaction (includes withdrawal, deposit, remittance, etc.) in relation to the reported amounts, ZSTRs may be interpreted in various ways subject to the narrative content.[17] Thus, in the analysis of typologies with ZSTRs in this study, closer examination of the STR narrative is done to ensure a more accurate evaluation.

For international transactions, this study considered STRs from 2012 to 2021, since none was captured in earlier periods. These international transactions totaled 1,906 by count and valued at PHP224.9 million. Likewise, inward transfers proved greater in total volume and value at 1,368 STRs or PHP153.0 million as against outward remittances at 538 reports or PHP71.9 million in sum. Likewise, to compare

[15] This study considered including in the dataset the names of the Nigerians identified from the data used in the AMLC's study "An Analysis of the Usefulness of Foreign Currency Declarations in Detecting Possible Cross-Border Transportation of Illicit Funds" between 2015 Q1 and 2021 Q3. The limited number of Nigerians, however, did not have a hit in the AMLC database.

[16] This number should be unique per transaction date per institution as stated in the 2021 AMLC Registration and Reporting Guidelines.

[17] ZSTR, which stands for STR transaction is commonly used for attempted transactions. Some CPs utilize this transaction code when the intent is merely to report business relationship with, or profile of a client or customer and no specific transaction is being reported at the time of filing. In some cases, CPs appear to be using the ZSTR code as a blanket transaction code to cover different transactions with varying dates of several subject, having a common connection (similar beneficiary/counterparty) and perceived to be involved in similar schemes.

across varying currencies, the study utilized the PHP equivalent amount of all foreign currencies present in the reports.

Relevant sections of the STR were also checked for completeness and consistency. Difficulties encountered were lack of uniformity and completeness of the data filed by CPs to the AMLC. For instance, data fields in some of the international transactions, which include but are not limited to the beneficiary and counterparty addresses, are not mandatory to be disclosed to the AMLC. In the absence of said data, the correspondent bank address, currency, nationality, and the narratives were used to determine the illegal money's potential source country or destination. In cases where the above conditions do not apply, the word "UNKNOWN" was used.[18]

For domestic transactions, the indicated branch as reported by the institution is presumed as the transacting branch where the transaction occurred thus, such addresses were used and broadly classified per city/province, and region in the country for easy grouping. There are, however, some banks and non-bank financial institutions (including branches) that do not have complete addresses and/or the submitted STR details on the name fields of the subject, account holder and other person, including addresses of the various name flags, are incomplete. Thus, the subject's domestic address is considered when the institutions did not identify or include the branch location.[19] In cases where the indicated bank branch address refers to two different sites, narrative details are looked into, to know which is the best possible location. If such is not present, the reported address of the account holder was also checked. There are cases where the subject and the accountholder are the same thus, validating the use of the address of the accountholder. Lastly, when the subject's address is not indicated, but the same person appeared in other STRs, the address indicated in other STRs was used. Otherwise, "UNKNOWN" was inputted in the blank field.

The succeeding analysis is guided by the following analytic judgment and confidence level matrix:

Analytic Judgments and Confidence Levels

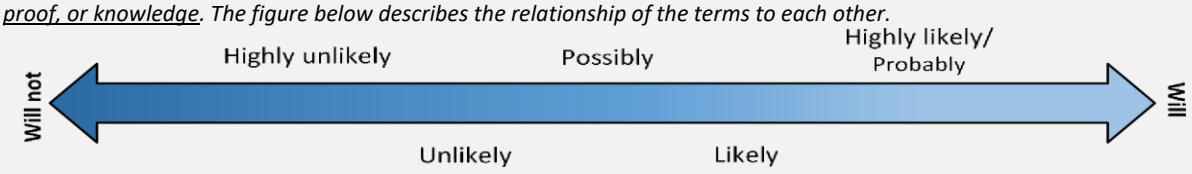
FIU Intelligence Assessments use phrases such as "we judge," "we assess," or "indicates" to convey analytical inferences (conclusions). These assessments are not statements of fact or proof, and do not imply complete knowledge. Analytic judgments are often based on incomplete information of varying quality,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



[18] International remittance transactions where the beneficiary/counterparty addresses are not mandatory to be disclosed to the AMLC are: (1) inward remittances for credit to another account; (2) inward remittances – advise and pay the beneficiary.

[19] Manual matching revealed that 297 or 80.93% of the 367 sample STR have the same subject address and branch locations, thus ensuring that subject addresses may be used in cases of blank branch addresses.

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.

Further, this report should not be interpreted as an assessment of the full amount of proceeds related to Nigerian money laundering or terrorism financing (ML/TF) offenses. The statements herein are not conclusive but are more descriptive of the observation on the gathered STRs from 2009 to 2021. Thus, inferences generated from STRs may need further verification and more in-depth investigation to substantiate likely linkage to certain crimes.

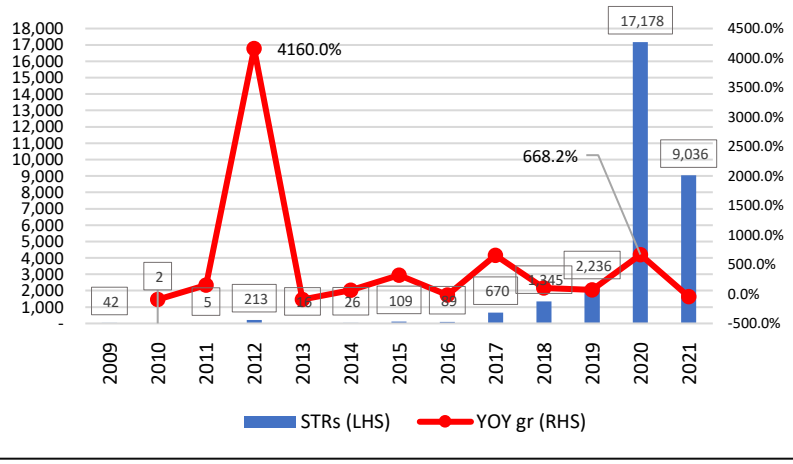
STRATEGIC ANALYSIS REPORT

III. Findings and Results of Analysis

A. Volume and Value of STRs

Total volume of STRs pertaining to Nigerian-related crimes, covering years 2009 to 2021, totaled 30,967 with estimated value of PHP3,262.1 million. In terms of volume, there was a notable jump by 4,160.0% in the number of STRs filed in year 2012 from a mere five (5) in the previous year due to increased unsubstantiated outward transactions to Nigeria in the months of September and December.

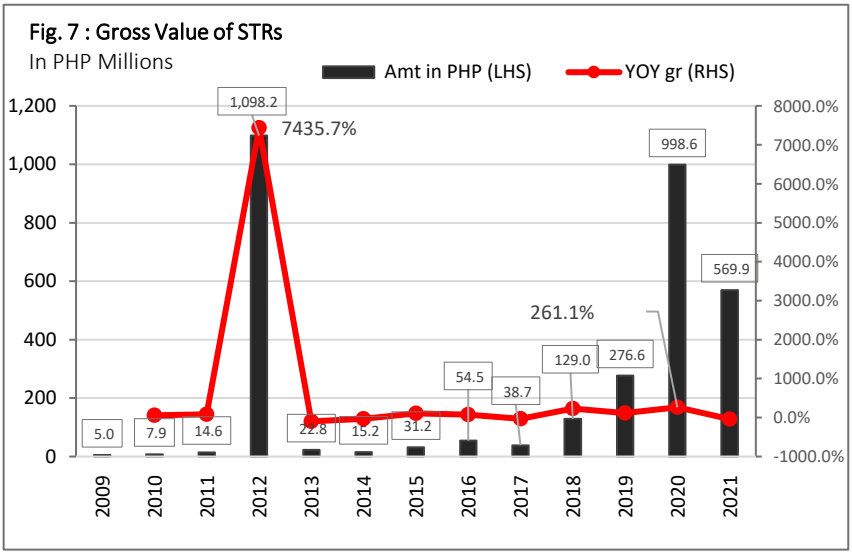
Fig. 6 : Volume of Nigerian Crime-Related STRs
Total Count



The CPs' reports tapered in 2013 but then followed an increasing trend onwards reaching its peak of 17,178 STRs in 2020 registering a 668.2% increase from the previous year's 2,236 transactions. Conversely, there is a significant 47.4% dip to 9,036 in the submitted STRs in 2021 (**Figure 6**).

In the same way, the PHP value of STRs considered in this study follow a fluctuating trend from PHP5.0 million in 2009, which peaked in 2012 at PHP1,098.2 million registering a 7,435.7% increase from prior year's results, largely on account of unjustified outward transactions to Nigeria in September (**Figure 7**). The pandemic period saw a relative 261.1% increase to PHP998.6 million in 2020

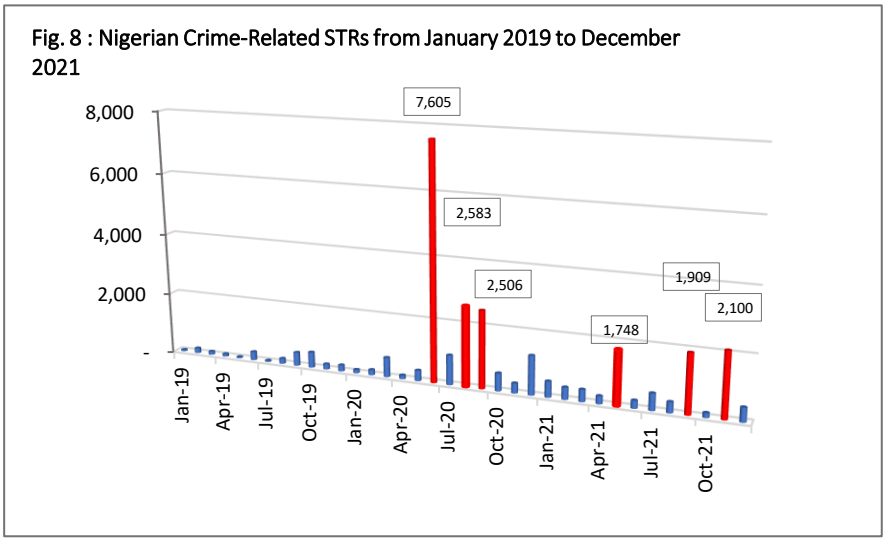
Fig. 7 : Gross Value of STRs
In PHP Millions



from the year 2019's PHP276.6 million and from a gradual pace in 2013. Moreover, the dip in the volume effected a fall in the cumulative value of the STRs to PHP569.9 million in 2021.

Focusing on the trend during the pandemic, it may be safe to assume that there is a significant intensification of crimes during the period as seen in the number of STRs in the months of June (7,605), August (2,583), September (2,506) for year 2020 then May (1,748), September (1,909) and November (2,100) for 2021 (**Figure 8**). Similarly, stringent lockdowns were implemented during the months of March, April, and August of year 2020.[20] For the year 2021, the third lockdown took effect in March and April. [21] While it may be recalled that the influx of tourists halted during the lockdowns, increased Internet usage may have contributed to the proliferation of cybercrimes.[22] Further, STRs involving Nigerian-related crimes may be an indicator of heightened criminal operations of the subject under study in the country.

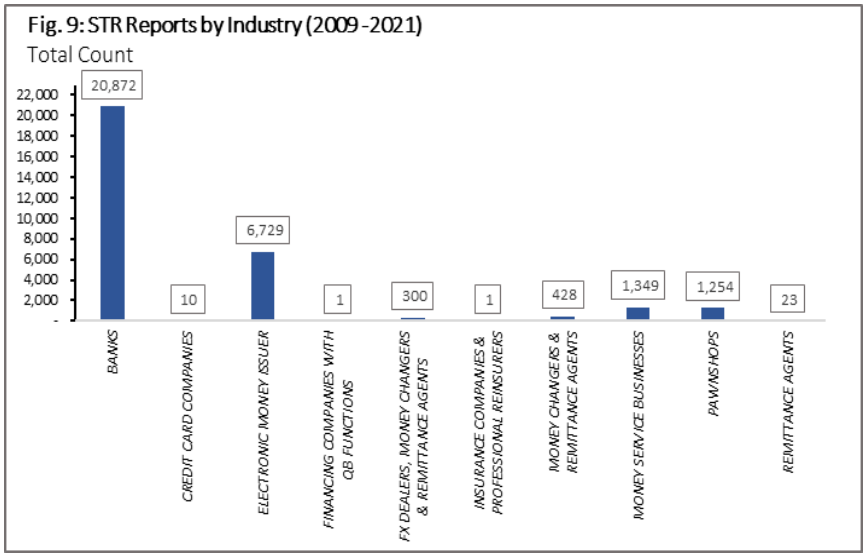
Fig. 8 : Nigerian Crime-Related STRs from January 2019 to December 2021



B. By Industry

The reports from banks[23] for the years 2009 to 2021 cornered a 67.4% (20,872) share of the aggregate 30,967 STRs. This is followed by EMIs at 21.7% (6,729), money service businesses at 4.4% (1,349), and pawnshops at 4.1% (1,254) (**Figures 9** and **10**).

Fig. 9: STR Reports by Industry (2009 -2021)

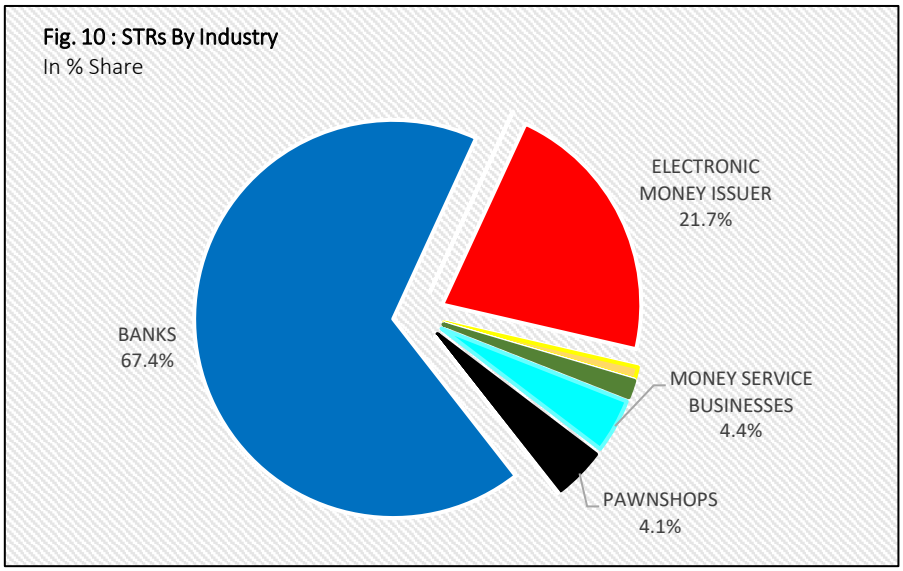


[20] For the year 2020, the first lockdown or enhanced community quarantine (ECQ) was imposed from March 14 to April 30, and the second lockdown transitioned to modified ECQ (MECQ) from August 4 to August 18. Retrieved from https://newsinfo.inquirer.net/1468403/lockdowns-in-ph-a-brief-history (accessed on 21 April 2022).

[21] The third round of ECQ was implemented from March 29 to April 4, 2021. On the day ECQ took effect, there were 71,606 COVID-19 cases, according to the World Health Organization. On April 5, the day after ECQ lapsed, there were 69,164 cases. Retrieved from ibid.

[22] The Philippine National Police (PNP) Anti-Cybercrime Group disclosed on its website the 869 online scam cases from March to September 2020, higher by 37% compared to 633 in the same period in 2019. Retrieved from https://www.pna.gov.ph/articles/1133961 (accessed on 27 April 2022)

[23] Banking sector consists of commercial, commercial/non-expanded commercial banks, private development banks, and savings and mortgage banks.



Tables 1 and 2 likewise, show the volume and PHP value of STRs categorized per supervising authority (SA) and industry classification of the filing CPs. [24]

Table 1: Volume of STR per SA and CPs Industry Classification (2009 – 2021)

Supervising Authority/CPs Industry Classification	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total Volume	Percent to total Volume
BSP															
BANKS	1	2	5	22	16	26	93	78	343	783	2096	13857	3550	20,872	67.4%
ELECTRONIC MONEY ISSUER										73	24	2370	4262	6,729	21.7%
MONEY SERVICE BUSINESSES									12	274	61	116	886	1,349	4.4%
PAWNSHOPS									1	65	18	832	338	1,254	4.0%
MONEY CHANGERS & REMITTANCE AGENTS	41			191					96	100				428	1.4%
FX DEALERS, MONEY CHANGERS & REMITTANCE AGENTS								11	207	45	37			300	1.0%
REMITTANCE AGENTS							10		11	2				23	0.1%
CREDIT CARD COMPANIES							6			2		2		10	0.0%
FINANCING COMPANIES WITH QB FUNCTIONS												1		1	0.0%
IC															
INSURANCE COMPANIES & PROFESSIONAL REINSURERS										1.0				1	0.0%
Grand Total	42	2	5	213	16	26	109	89	670	1,345	2,236	17,178	9,036	30,967	100.0%

Banks contributed largely to the total PHP value with a 96.2% share (PHP3,139.3 million). EMIs followed suit at 1.2% (PHP39.8 million). Likewise, MSBs, pawnshops, and money changers and remittance agents are in third to fifth place as these contributed 0.9% (PHP29.7 million), 0.7% (PHP22.2 million), and 0.6% (PHP18.3 million), respectively, to the total PHP value associated with Nigerian-related crimes (Table 2). The emergence of banks as top filers, both in volume and PHP value, may be due to the banks' capability to facilitate high value transfers, which includes, among others, deposits, withdrawals, and remittances as well as investments. Moreover, banks employ stringent know-your-customer (KYC) procedures as well as enhanced due diligence (EDD) process. The bank-client relationship is also an

[24] The STRs were predominantly filed by BSP-supervised institutions accounting for 99.9 percent (30,166 STRs) for the count, with one STR coming from the Insurance Commission, which has zero monetary value.

advantage as it entails a series of transactions, which can be assessed for any abnormal patterns or behaviors.[25]

Table 2: Value of STR per SA and CPs Industry Classification (2009 – 2021)

Supervising Authority/CPs Industry Classification	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total Value (In PHP Millions)	Percent to Total PHP Value
BSP															
BANKS	0.2	7.9	14.6	1,089.2	22.8	15.2	30.8	53.8	27.5	113.3	273.5	972.8	517.6	3,139.3	96.2%
ELECTRONIC MONEY ISSUER	-	-	-	-	-	-	-	-	-	0.7	0.4	12.5	26.2	39.8	1.2%
MONEY SERVICE BUSINESSES	-	-	-	-	-	-	-	-	0.5	9.5	1.4	2.4	15.9	29.7	0.9%
PAWNSHOPS	-	-	-	-	-	-	-	-	0.2	0.7	0.4	10.8	10.1	22.2	0.7%
MONEY CHANGERS & REMITTANCE AGENTS	4.8	-	-	9.0	-	-	-	-	1.9	2.6	-	-	-	18.3	0.6%
FX DEALERS, MONEY CHANGERS & REMITTANCE AGENTS	-	-	-	-	-	-	-	0.7	8.6	2.1	0.9	-	-	12.3	0.4%
REMITTANCE AGENTS	-	-	-	-	-	-	0.4	-	0.1	0.0	-	-	-	0.5	0.0%
FINANCING COMPANIES WITH QB FUNCTIONS	-	-	-	-	-	-	-	-	-	-	-	0.1	-	0.1	0.0%
CREDIT CARD COMPANIES	-	-	-	-	-	-	0.0	-	-	0.0	-	0.0	-	0.0	0.0%
IC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
INSURANCE COMPANIES & PROFESSIONAL REINSURERS	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0%
Grand Total	**5.0**	**7.9**	**14.6**	**1,098.2**	**22.8**	**15.2**	**31.2**	**54.5**	**38.7**	**129.0**	**276.6**	**998.6**	**569.9**	**3,262.1**	**100.0%**

Further, Tables 1 and 2 show that banks, specifically commercial/non-expanded commercial banks, are the preferred channels in moving high-value proceeds with possible links to Nigerian-related crimes. For small-ticket items, EMIs, MSBs, and pawnshops are generally used.

C. International Transactions

For international remittances, this study considered STRs from 2012 to 2021 since no international transaction pertaining to subject crimes was reported for the three (3)-year period of 2009 to 2011. International remittances[26] for the period under study show the variance between inward and outward flow, with aggregate value of inflow posting 112.9% higher, amounting to PHP153.0 million, compared to the total outflow of PHP71.9 million. Volume of transactions, likewise, follow the same inclination as inflows cornered 71.8% or 1,368 of the total STRs compared to outflows of 28.2% or 538 STRs (Table 3).

Table 3: Total Volume and Value of International Remittance-Related STRs (2009 – 2021)[27]

Reports	Volume	Percent Share to Total Volume	Total Value In PHP Millions	Percent Share to Total Value
STR				
Inflow	1,368	71.8%	153.0	68.0%
Outflow	538	28.2%	71.9	32.0%
Total	**1,906**	**100.0%**	**224.9**	**100.0%**

[25]Lifted from AMLC's published study "An Analysis of Suspicious Transaction Reports with Possible Links to Tax Crimes". Retrieved from http://www.amlc.gov.ph/images/PDFs/2021%20ANALYSIS%20OF%20STRS%20WITH%20POSSIBLE%20LINKS%20TO%20TAX%20CRIMES.pdf

[26] For STRs, the transaction codes RIIR, RIRIA, RIRIC, and RIRIP for inward international remittances; and RORIA, RORIC ,and RORIP for outward international remittances are considered in the assessment

[27] As of the February 2022 run date, STR transactions covering the period 2009 to 2021, no international transactions pertaining to Nigerian-related crimes were reported for the three (3)-year period of 2009 to 2011.

Specifically, total inward transfers were relatively low, except for the years 2020 and 2021, which indicated an influx at 260 and 757 transactions corresponding to PHP20.7 million and PHP54.7 million in sum, respectively. For international outward remittances, the number of STRs peaked at 196 during 2018, slowed down to 15 in 2020 and gained momentum again in 2021 with 60 transactions (**Figure 11**). In terms of value, 2016 outflows were mostly high-value tickets as it registered PHP29 million (peso equivalent) as against the resulting sum for the years 2020 and 2021 at PHP0.5 million and PHP1.0 million, respectively (**Figure 12**).

Fig. 11 : Volume of International Remittances
Total Count

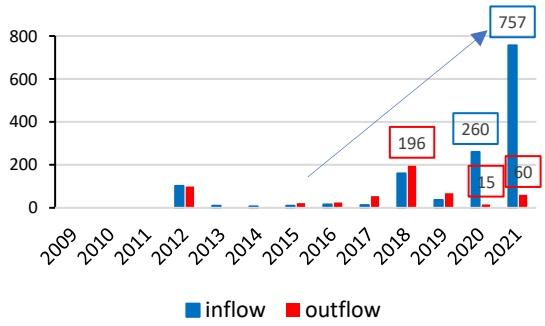
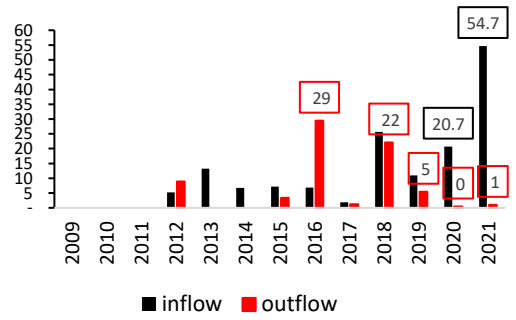


Fig. 12: Value of International Remittances
In PHP Millions



The top 15 sources and recipients of foreign currencies for this study pertaining to Nigerian-associated crimes are identified in **Tables 4** and **5**. Notably, as indicated in **Table 4**, the United States is the top source of foreign currencies brought in the country. Total value of inflows for the seven (7)-year period under consideration reached PHP71.4 million or about 46.7% of the total inward foreign currencies. [28] In terms of count, the USA figured in 762 STRs or 55.7% of the aggregate. Majority of the outward flows were transmitted to the corresponding beneficiaries with addresses in Nigeria as it posted PHP28.4 million or 39.5% of the aggregate outward transfers (**Table 5**).

Table 4: Top 15 Inflow of Remittances

Countries	Volume of Inflows	Percent to Total Volume	Value of Inflows (In PHP Millions)	Percent to Total Value
UNITED STATES	762	55.7%	71.4	46.7%
AUSTRALIA	54	3.9%	5.6	3.6%
SWITZERLAND	8	0.6%	5.5	3.6%
NIGERIA	15	1.1%	5.4	3.5%
SAUDI ARABIA	16	1.2%	5.0	3.3%
JORDAN	1	0.1%	4.4	2.9%
SINGAPORE	16	1.2%	3.9	2.6%
UNITED KINGDOM	97	7.1%	3.2	2.1%
THAILAND	1	0.1%	2.1	1.4%
TAIWAN	21	1.5%	2.1	1.4%
CZECH REPUBLIC	1	0.1%	1.8	1.2%
CANADA	7	0.5%	1.4	0.9%
HONG KONG	10	0.7%	1.4	0.9%
GERMANY	62	4.5%	1.2	0.8%
BAHRAIN	4	0.3%	1.2	0.8%
OTHERS	2876	210%	9.1	5.9%
UNKNOWN	0	0.00%	28.3	18.5%
TOTAL	**1,368**	**100.0%**	**153.0**	**100.0%**

[28] Following the United States, in terms of inflow, are Australia (PHP5.6 million), Switzerland (PHP5.6 million), Nigeria (PHP5.3 million), and Saudi Arabia (PHP5.0 million).

Table 5: Top 15 Outflow of Remittances

Countries	Volume of Outflows	Percent to Total Volume	Value of Outflows (In PHP Millions)	Percent to Total Value
NIGERIA	297	55.2%	28.4	39.5%
UNITED STATES	13	2.4%	24.1	33.5%
CHINA	48	8.9%	9.4	13.1%
INDIA	4	0.7%	3.1	4.3%
CYPRUS	2	0.4%	1.6	2.3%
THAILAND	7	1.3%	1.3	1.8%
GHANA	63	11.7%	0.7	1.0%
SWEDEN	3	0.6%	0.4	0.6%
HONG KONG	8	1.5%	0.4	0.6%
SOUTH AFRICA	6	1.1%	0.3	0.4%
MALI	15	2.8%	0.3	0.4%
UNITED ARAB EMIRATES	5	0.9%	0.2	0.3%
BENIN	22	4.1%	0.2	0.2%
VIETNAM	8	1.5%	0.1	0.2%
HUNGARY	1	0.2%	0.1	0.1%
OTHERS	31	5.8%	0.6	0.9%
UNKNOWN	5	0.9%	0.4	0.6%
TOTAL	**538**	**100.0%**	**71.9**	**100.0%**

D. STRs per Domestic Region

Based on STRs submitted by various CPs covering 2009 to 2021, it was observed that proliferation of Nigerian-related crimes is within the area of the National Capital Region (NCR), both in terms of volume count and aggregate value as it contributed 11,640 or a 37.6% share to the total count, and PHP2,162.1 million or a 66.3% share to the aggregate peso value. Notably, following at a distance are Region IV-A (CALABARZON), Region I (Ilocos Region), Region III (Central Luzon), and Region VII (Central Visayas). Enumerated in Table 6 are the list of domestic regions with the corresponding number and value of STRs for the period under review.[29]

Table 6: Total Volume and Value of STRs per Domestic Region (2009 – 2021)

Domestic Regions	Total Count	Percent to Total Count	Total Value In PHP Millions	Percent to Total Value
NATIONAL CAPITAL REGION (NCR)	11,640	37.6%	2,162.1	66.3%
REGION IV-A (CALABARZON)	4,714	15.2%	217.1	6.7%
REGION I (ILOCOS REGION)	3,286	10.6%	163.7	5.0%
REGION III (CENTRAL LUZON)	1,454	4.7%	154.0	4.7%
REGION VII (CENTRAL VISAYAS)	772	2.5%	146.7	4.5%
REGION II (CAGAYAN VALLEY)	470	1.5%	67.1	2.1%
REGION X (NORTHERN MINDANAO)	277	0.9%	53.4	1.6%
REGION XII (SOCCSKSARGEN)	415	1.3%	43.0	1.3%
REGION VI (WESTERN VISAYAS)	83	0.3%	34.2	1.0%
CORDILLERA ADMINISTRATIVE REGION (CAR)	448	1.4%	24.8	0.8%
REGION VIII (EASTERN VISAYAS)	100	0.3%	9.7	0.3%
REGION XI (DAVAO REGION)	138	0.4%	8.6	0.3%
REGION IX (ZAMBOANGA PENINSULA)	81	0.3%	3.1	0.1%
MIMAROPA REGION	53	0.2%	3.1	0.1%
REGION V (BICOL REGION)	25	0.1%	1.5	0.0%
REGION XIII (CARAGA)	18	0.1%	0.5	0.0%
UNKNOWN	6,993	22.6%	169.6	5.2%
Grand Total	**30,967**	**100.0%**	**3,262.1**	**100.0%**

[29] There is a need for CPs to properly input the specific addresses as STRs identified as Unknown totaled PHP169.6 million, ranking third in terms of value. Likewise, by count it placed second following the NCR at 6,993.

In terms of value, a huge chunk of the NCR aggregate is linked to Nigerian-related reports coming from Quezon City, amounting to PHP1,211.4 million or a 56.0%share (**Figure 13**). Trailing behind are the cities of Parañaque, Makati, Las Piñas, and Manila. By count, the city of Las Piñas garnered the most number at 4,405 STRs or 37.8%of the total (**Figure 14**).

Fig 13 : Total Value of STRs :NCR
In PHP Millions

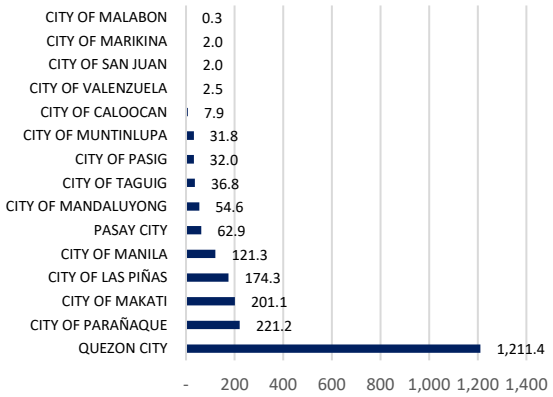
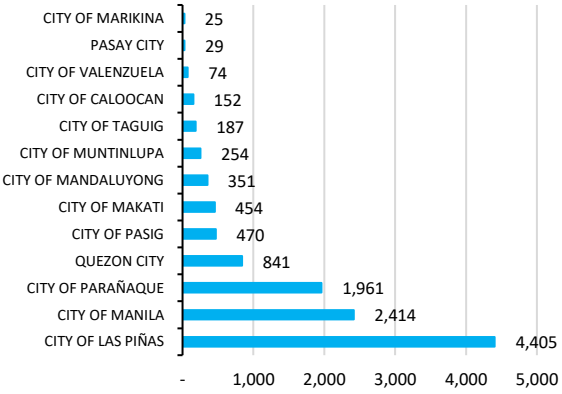


Fig. 14: Total Volume of STRs : NCR



For the period covered by the study, **Figures 15** and **16** below exhibit that the 41 STRs by CPs in 2009 (out of 42 transactions) with the cumulative amount of PHP4.8 million originating from Quezon City followed by the City of Manila in 2010 at PHP7.8 million with one (1) count of STR. Succeeding build-up in the number of STRs, specifically from 2018 onwards, may have been brought about by the awareness of CPs on the need to report as well as the expansion of the scammers' reach. The areas of Las Piñas and Parañaque were active in submitting STRs for the years 2020 and 2021. For 2020, the City of Parañaque posted 1,456 reports, second to Las Piñas in count, but with the highest gross sum of PHP136.4 million compared to the rest of the jurisdictions in the NCR. Notable is the high value STRs filed from Quezon City amounting to PHP1,088.7 million in 2012 greatly contributing to its topping the list by value in the NCR (**Figure 16**).

Fig. 15 : Total Count of STRs : Top Five Cities in NCR (2009-2021)

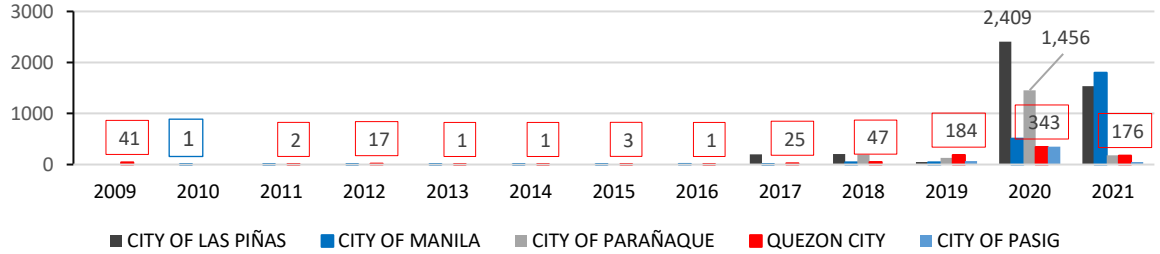
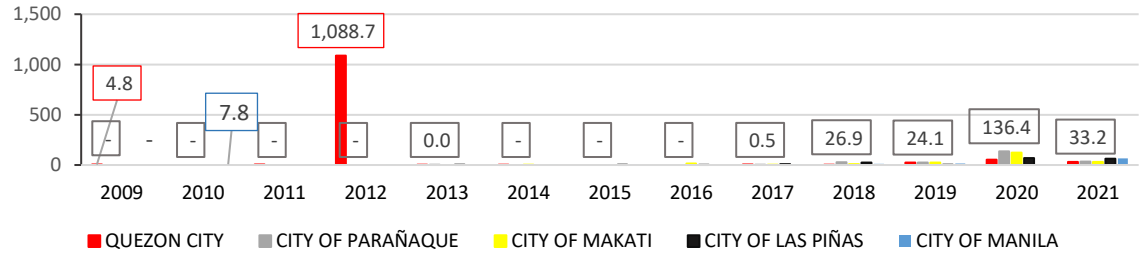
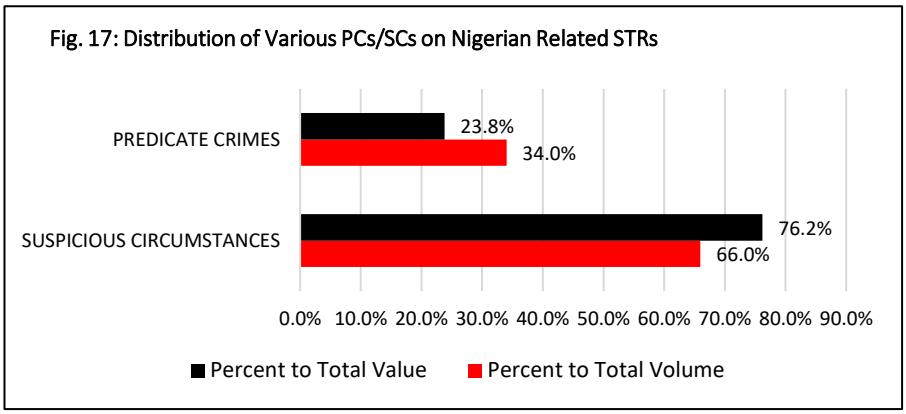


Fig. 16: Total Value of STRs: Top Five Cities in NCR (2009-2021)
In PHP Millions



E. Various PCs and SCs

This section gives an overview of the different SC and PC used by CPs in filing Nigerian-related STRs. It can be drawn from Figure 17 that majority of the STRs fall under the SC category for the period covered, both in volume and PHP value at 20,432 STRs (66.0%) and PHP2,485.4 million (76.2%), respectively. On the other hand, STRs pertaining to various PCs reached 10,535 (34.0%) in terms of number and PHP776.7 million (23.8%) in value.



The table below presents the percentage of SC and PC compared to the total STR volume and aggregate peso value covered in this study:

Table 7: Total Volume and Value of Various PCs/SCs (2009 – 2021)

Various PCs/SCs with Nigerian-Related Keywords	Total Volume	Percent to Total Volume	Total Value (In PHP Millions)	Percent to Total Value
SUSPICIOUS CIRCUMSTANCES	**20,432**	**66.0%**	**2,485.4**	**76.2%**
THE AMOUNT INVOLVED IS NOT COMMENSURATE WITH THE BUSINESS OR FINANCIAL CAPACITY OF THE CLIENT (SI3)	9,000	29.1%	578.2	17.7%
THERE IS NO UNDERLYING LEGAL OR TRADE OBLIGATION, PURPOSE OR ECONOMIC JUSTIFICATION (SI1)	6,865	22.2%	1,562.0	47.9%
THE TRANSACTION IS SIMILAR, ANALOGOUS OR IDENTICAL TO ANY OF THE FOREGOING (SI6)	2,826	9.1%	276.1	8.5%
THERE IS A DEVIATION FROM THE CLIENT'S PROFILE/PAST TRANSACTIONS (SI5)	1,382	4.5%	51.0	1.6%
THE CLIENT IS NOT PROPERLY IDENTIFIED (SI2)	285	0.9%	15.1	0.5%
THE TRANSACTION IS STRUCTURED TO AVOID BEING REPORTED (SI4)	74	0.2%	3.1	0.1%
PREDICATE CRIMES	**10,535**	**34.0%**	**776.7**	**23.8%**
FRAUD-RELATED				
ELECTRONIC COMMERCE ACT OF 2000 (PC11)	7,573	24.5%	623.4	19.1%
SWINDLING(PC09)	1,874	6.1%	96.5	3.0%
FRAUDULENT PRACTICES AND OTHER VIOLATIONS UNDER THE SECURITIES REGULATIONS CODE OF 2000 (PC33)	279	0.9%	29.1	0.9%
CORRUPTION-RELATED	1	-	-	-
GRAFT & CORRUPT PRACTICES (PC03)	1	0.0032%	-	-
DRUG TRAFFICKING & RELATED OFFENSES (PC02)	345	1.1%	5.3	0.2%
VIOLATIONS OF THE ANTI-TRAFFICKING IN PERSONS ACT OF 2003 (PC19)	210	0.7%	12.0	0.4%
VIOLATIONS OF SPECIAL PROTECTION OF CHILDREN AGAINST ABUSE, EXPLOITATION AND DISCRIMINATION ACT (PC32)	167	0.5%	1.3	0.0%
FRAUDS AND ILLEGAL EXACTIONS AND TRANSACTIONS (PC16)	38	0.1%	5.3	0.2%
VIOLATIONS OF THE MIGRANT WORKERS AND OVERSEAS FILIPINOS ACT OF 1995 (PC28)	30	0.1%	1.9	0.1%
FELONIES OR OFFENSES OF A SIMILAR NATURE THAT ARE PUNISHABLE UNDER THE PENAL LAWS OF OTHER COUNTRIES (PC36)	6	0.0194%	1.3220	0.0405%
FINANCING OF TERRORISM (PC14)	5	0.0161%	0.5658	0.0173%
FORGERIES AND COUNTERFEITING (PC18)	4	0.0129%	-	-
JUETENG & MASIAO (PC06)	2	0.0065%	0.0126	0.0004%
ROBBERY & EXTORTION (PC05)	1	0.0032%	0.0182	0.0006%
Grand Total	**30,967**	**100.0%**	**3,262.1**	**100.0%**

From the identified SCs, "*the amount involved is not commensurate with the business or financial capacity of the client*" (SI3) topped the number of filed reports at 9,000 counts or 29.1% of the aggregate volume. This is followed by *"there is no underlying legal or trade obligation, purpose or economic justification"* (SI1), with a 6,865 STRs or a 22.2% share. In terms of value, however, the placing of the two SCs are reversed as SI1 STRs, assumed to have dealt with high-valued amounts, totaling PHP1,562 million (47.9%) against SI3 with PHP578.2 million (17.7%).

In terms of transaction frequency, fraud-related PCs (i.e., Electronic Commerce Act of 2000 violations, swindling and fraudulent practices, and other violations under the Securities Regulation Code (SRC) of 2000) garnered the highest digits of 9,726 STRs. There was a significant number of STRs related to violations of the Electronic Commerce Act of 2000 as it reached 7,573 STRs or 24.5% of the total dataset. Swindling comes next with 1,874 STRs or a 6.1% share and at the third slot is fraudulent practices and other violations under the SRC of 2000 registering 279 transactions (0.9%). Total amount of fraud-related PCs, likewise, follow the same trend for the three PCs with violations of Electronic Commerce Act of 2000, garnering the highest value at PHP623.4 million (19.1%).

Using specific keywords[30] in the narratives, Table 8 below presents the illegal activities identified in the dataset. Apparently, Others - Unsubstantiated Transactions cornered the majority of the activities related to Nigerian-related crimes registering 51.1% or 15,820 STRs of the aggregate volume, valued at PHP1,499.6 million or 46.0% of the PHP3,262.1 gross amount. Triggers to report transactions as suspicious are due to strikingly high frequency and value of the activities and failure to provide supporting documents when asked by the financial institutions.

Table 8: Types of Scams (2009 – 2021)

TYPES OF SCAMS	Total Volume	Percent to Total Volume	Total Value (In PHP Millions)	Percent to Total Value
Others - Unsubstantiated Transactions	**15,820**	**51.1%**	**1,499.6**	**46.0%**
User Triggered The 500K PHP Cumulative Volume System Flag	247	0.8%	42.6	1.3%
Advanced Fee Fraud	**34**	**0.1%**	**1,086.4**	**33.3%**
Unauthorized transactions	**7,491**	**24.2%**	**308.6**	**9.5%**
Pass through account/Money Mule	**996**	**3.2%**	**101.3**	**3.1%**
Package scam	**1,348**	**4.4%**	**57.3**	**1.8%**
Suspect of swindling/estafa	**231**	**0.7%**	**44.8**	**1.4%**
Hacking	**88**	**0.3%**	**33.6**	**1.0%**
Fraud case	**2,170**	**7.0%**	**24.6**	**0.8%**
Phishing	**317**	**1.0%**	**18.1**	**0.6%**
Illegal drugs	**337**	**1.1%**	**13.9**	**0.4%**
Human trafficking	**360**	**1.2%**	**13.2**	**0.4%**
Love/romance scam	**295**	**1.0%**	**11.5**	**0.4%**
Luggage scam	**67**	**0.2%**	**10.5**	**0.3%**
Investment scam	**86**	**0.3%**	**10.4**	**0.3%**
Child exploitation	**460**	**1.5%**	**8.3**	**0.3%**
Release scam	**51**	**0.2%**	**4.7**	**0.1%**

[30] Related keywords "hacking, phishing, lottery, inheritance, drugs, swindling, package, terrorism, and fraud" were used to facilitate identification of illegal activities related to Nigerian-linked crimes.

TYPES OF SCAMS	Total Volume	Percent to Total Volume	Total Value (In PHP Millions)	Percent to Total Value
Structuring	**50**	**0.2%**	**3.9**	**0.1%**
Syndicates	**72**	**0.2%**	**3.0**	**0.1%**
International online syndicate	2	0.0%	0.1	0.0%
African Drug Syndicate	63	0.2%	1.0	0.0%
Nigerian syndicate	7	0.0%	1.9	0.1%
Identity Fraud	**98**	**0.3%**	**2.5**	**0.1%**
Identity Theft	28	0.0904%	0.0527	0.0016%
Multiple Identity	11	0.0355%	1.1919	0.0365%
Fabrication of personal data	56	0.1808%	1.1771	0.0361%
Catfishing	3	0.0097%	0.0475	0.0015%
Illegal recruitment	38	0.1%	2.1	0.1%
Lottery scam	2	0.0065%	1.0	0.0309%
Product scam	38	0.1227%	1.0	0.0301%
Inheritance scam	6	0.0194%	0.7	0.0201%
Terrorism	6	0.0194%	0.6	0.0173%
Automated Teller Machine (ATM) Skimming	481	1.5533%	0.4	0.0114%
Rental property scam	15	0.0484%	0.3625	0.0111%
Sending funds to Dark Service Platform	5	0.0161%	0.0028	-
Sabong/gambling	2	0.0065%	0.0012	-
Subscription scam	2	0.0065%	0.0012	-
Graft and corruption	1	0.0032%	-	-
TOTAL	**30,967**	100.0%	**3,262.1**	100.0%

Further, in terms of value, advanced fee fraud, unauthorized transactions, pass through account or money mules and package scam followed, placing second to fifth (Table 8). Despite the minimal 34 STRs generated by the advanced fee fraud category, the high value of PHP1,086.4 million was brought about by the attempted account opening of a prospective customer who expected to receive funds after payment of some fees. Unauthorized transactions at PHP308.6 million (9.5%) likewise comprise fraudulent transfers as well as withdrawals on compromised accounts. STRs identified as pass through/money mules with total value of PHP101.3 million (3.1%) usually involves Filipinas with Nigerian boyfriends or friends who allow the usage of their accounts. There were instances under pass-through accounts/money mules that accounts belonging to Nigerian nationals were being used by other acquaintances in fraudulent fund transfers. Package scam reports totalled PHP57.3 million (1.8%) and the narrative disclosed that cases were reported by Company P, a remittance agent, and culprits involve a Nigerian student and one Filipina married to a Nigerian.

The vulnerabilities of cryptocurrency to money laundering may be focused on as crypto-related transactions using the keywords "crypto,"[31] "binance,"[32] "bitcoin,"[33] and "external wallet"[34] for this study generated 1,503 STRs with corresponding value of PHP132.7 million (**Table 9**). Of this total, 1,337 STRs or PHP93.5 million pertain to unsubstantiated transactions triggered by a breach of the PHP500,000 cumulative value flag and high volume of activity. Hacking placed second at PHP19.5 million with 42 STRs primarily due to the Bank ABC-hacking incident, the narrative of which discussed the existence of an article pertaining to Bank ABC accounts that were used to buy bitcoin via Bank FIJ. Relative to this, according to a newspaper, an information from a reliable source stated that a Bank FIJ account was used to buy Bitcoin amounting to PHP5 million from the cryptocurrency market on 11 December 2021.[35]

Table 9: Crypto-related Scams (2009 – 2021)

Types of Scams	Volume	Total Value (In PHP Millions)
Others - Unsubstantiated Transactions	1,337	93.5
Hacking	42	19.5
Pass-through account/Money mule	61	12.8
Phishing	3	3.4
Fraud case	15	1.8
Investment scam	32	0.9
Package scam	6	0.5
Suspect of swindling/estafa	1	0.1
Fabrication of personal data	6	0.05
TOTAL	**1,503**	**132.7**

[31] Crypto means hidden. When information is hidden with cryptography, it is encrypted. Retrieved from https://www.bitdegree.org/crypto/tutorials/what-is-cryptocurrency#how-does-cryptocurrency-work (accessed on 3 June 2022).

[32] Binance is an online exchange where users can trade cryptocurrencies as well as provides a crypto wallet for traders to store electronic funds. Retrieved from https://www.investopedia.com/terms/b/binance-exchange.asp (accessed on 3 June 2022).

[33] Bitcoin is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, and thus removing the need for third-party involvement in financial transactions. Retrieved from https://www.investopedia.com/terms/b/bitcoin.asp (accessed on 3 June 2022).

[34] External wallets mean the address(es) of one or more of your external digital asset wallet(s), as the case may be (including but not limited to a Bitcoin Wallet).Retrieved from https://www.lawinsider.com/dictionary/external-wallets (accessed on 3 June 2022).

[35] Apparently, the hacker siphoned money from Bank ABC victims, transferred it to the Bank FIJ account number, using a fictitious name, and immediately bought Bitcoin from it. This was scheduled over the weekend, considering that complaints are processed during office working hours.

IV. Suspicious Activities and Indicators

This section contains typologies and red flag indicators relating to possible ML/TF activities involving likely perpetrators identified in the study. All names of subjects, CPs, and entities mentioned in the succeeding cases are redacted. While these may guide CPs in detecting possible suspicious activities involving Nigerian-related crimes, it should be noted that these cases are solely based on STRs, hence, further intelligence-gathering and investigation are needed to establish likely linkage to Nigerian-related crimes.

Inconsistent Transactional Activities with the Subject's Business Profile

1. Mr. Tee AXY (Mr. AXY) figured in 25 suspicious transactions, amounting to PHP25.9 million as reported by Bank ABC with branches in Quezon City and in Bacoor, Cavite from September 2017 to June 2018.

   Mr. AXY'S transactions allegedly deviated from his profile and seemed structured to avoid being reported. The client's declared source of income at Bank ABC, Quezon City branch (ABC QC) is from importing and exporting of general merchandise, as well as a remittance center identified as Dela Cruz Business, found to be registered under his wife, Mrs. Juana Dela Cruz AXY (Mrs. AXY). When the bank inquired on the sources of deposits, the client claimed that those were proceeds from rentals of his properties which, however, lacked supporting documents. Further, ABC QC filed another batch of 15 suspicious transactions, amounting to PHP3.2 million in November 2017. In June 2018, Bank ABC in Bacoor, Cavite (ABC Cav) branch filed seven (7) suspicious debit and credit transactions on Mr. AXY, aggregating to USD0.4 million with the peso equivalent of PHP22.0 million, which were found to diverge from the subject's declared resources.[36] Notable information revealed by Mr. AXY to ABC Cav branch is the client's engagement in the importation of surplus car parts from Nigeria. In addition, the client divulged moving funds between his accounts with the bank, the rationale of which is yet to be established.

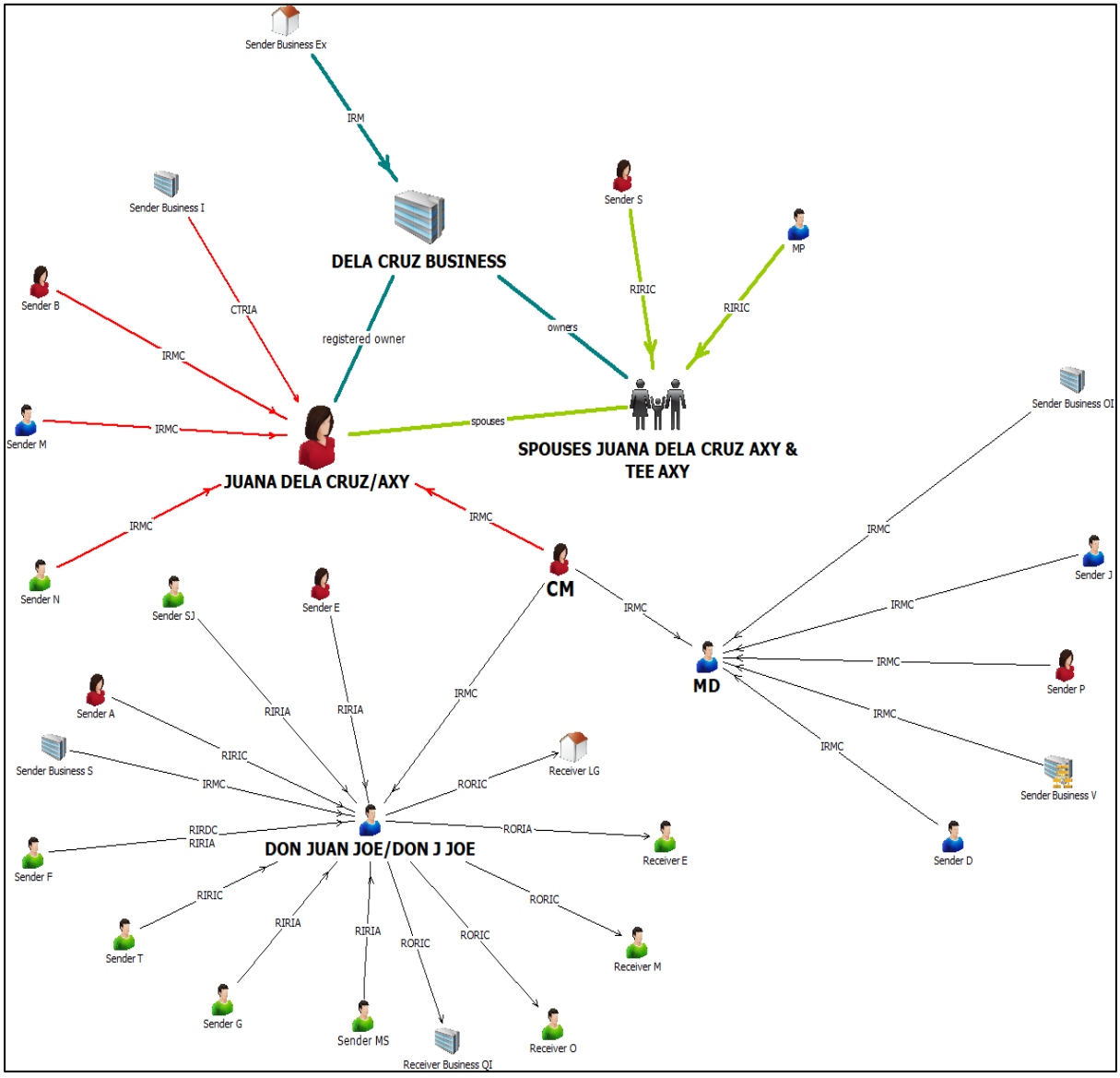
   Mr. AXY's name came to focus from the BI's list of Nigerians with a travel history to the country. The BI's dataset on visitor arrivals revealed that the respective travels of Mr. AXY in and out of the country since September 2008 until end-December 2021 summed to 54 times.[37] Specifically for the period covering the STR data (March 2017 to December 2018), Mr. AXY has travelled on nine (9) occasions to and from Manila to Hong Kong, China, and Korea.[38] This was then checked against the dataset that revealed several STRs filed on the subject on said period.

   Database search on Juana Dela Cruz (aka Juana Dela Cruz AXY [Mrs. AXY]) and Dela Cruz Business revealed 31 covered transaction reports (CTRs) and three (3) STRs with corresponding value of PHP47.1 million. It should be noted that Dela Cruz Business is one of the listed deposit outlets of the Digital Savings[39] account together with a convenience store, local pawnshops, as well as an international remittance company, among others.

[36] The aggregated sum of STRs filed by ABC Bacoor branch have specific transaction codes and are not classified as ZSTRs compared to the ones filed by the ABC branch in Quezon City.
[37] This pertains to the available STR on Mr. AXY from the dataset in this study which is from March 2017 to end-December 2018 to highlight the possible places which might correlate to the deposits made by the subject during that period.
[38] Mr. AXY's travel origin and destinations until year 2021 extended to Ethiopia, Japan, Malaysia, Qatar, Thailand, and United Arab Emirates.
[39] A digital savings account is an online-only account that enables customers to open an account online without need for physical appearance at the branch. All forms and documentary requirements will be submitted via the Digital Savings App.

Transactions with identified beneficiaries and counterparties were selected to determine the possible involvement of other individuals to Mr. AXY. The chart below (**Figure 18**) demonstrates the extent of related transactions to spouses Tee and Juana AXY, which were mostly inward international remittances and an inter-account transfer (same bank) summed at PHP12.1 million.

Fig.18: Transaction Flow of Dela Cruz Business/Mrs. AXY and Mr. Tee AXY



While five (5) individuals and two (2) corporations made substantial transactions with Dela Cruz Business and its owners, a certain Ms. CM from a city in the USA led to suspected pass-through accounts of Mr. MD and Mr. Don Juan Joe (Mr. Joe). Mr. MD had been the recipient of money transfers from three (3) individuals and two (2) businesses valued at PHP13.0 million, one of which resulted to an STR. Mr. Joe, on the other hand, had nine (9) inward and six (6) outward transactions from/to various individuals and corporations with an aggregate amount of PHP21.4 million.

Pass-through Accounts

Mr. Joe, as reported by the Bank O, opened an account on 28 January 2009 and declared a money transfer trade as source of funds. The said Bank O branch filed in December 2011 a report, since it found the transactions of Mr. Joe suspicious. Between 11 and 18 November 2011, subject client received a total amount of PHP3,873.6 million, which was immediately transferred to his other account either on the same day or three (3) days after the remittance transactions were posted, leaving a minimal balance on the source account. While the year 2011 reports showed the same place of residence for Mr. Joe's, succeeding years' bank reports disclosed seven declared places of residence including Shenyang, China.

Mr. MD, on the other hand, received a remittance of USD0.1 million or PHP5.1 million on 25 October 2011 from earlier identified subject, Ms. CM, whose underlying transactions could not be verified. Coincidentally, Ms. CM is apparently a business partner of another Bank O client identified as Mr. Joe. Further, the STR stated that on the same day (25 October 2011), Mr. MD's account was debited for PHP5.0 million and the same amount was credited to the account of Mr. Joe, rendering Mr. MD's transaction as pass-through between Ms. CM and Mr. Joe. Evidently, Mr. MD's declared job as a messenger per bank record is not commensurate with the fund transfers. When asked by the bank, subject declared that he is a business partner of Mr. Joe in operating a remittance business. Mr. MD, however, was again reported in 2012 by Bank O in connection to a complaint filed by a certain principal of a school based abroad regarding a fraudulent wire transfer credited to the subject's account on 3 October 2011.

Package, romance, lottery scams with pass-through accounts

2. Twenty-four individuals and one (1) entity figured in 1,982 STRs with a reported estimated value of PHP300.3 million. The identified individuals had transactional linkages with OBC Corporation and its owner and officer. Said entity, registered with Securities and Exchange Commission, allegedly operates as a bills payment collection agent. Mr. One NDK is the owner of the said company and manages the same with his wife, Ms. CRS Las Casas. also known as Ms. CRS Casas NDK (Mrs. NDK).[40]

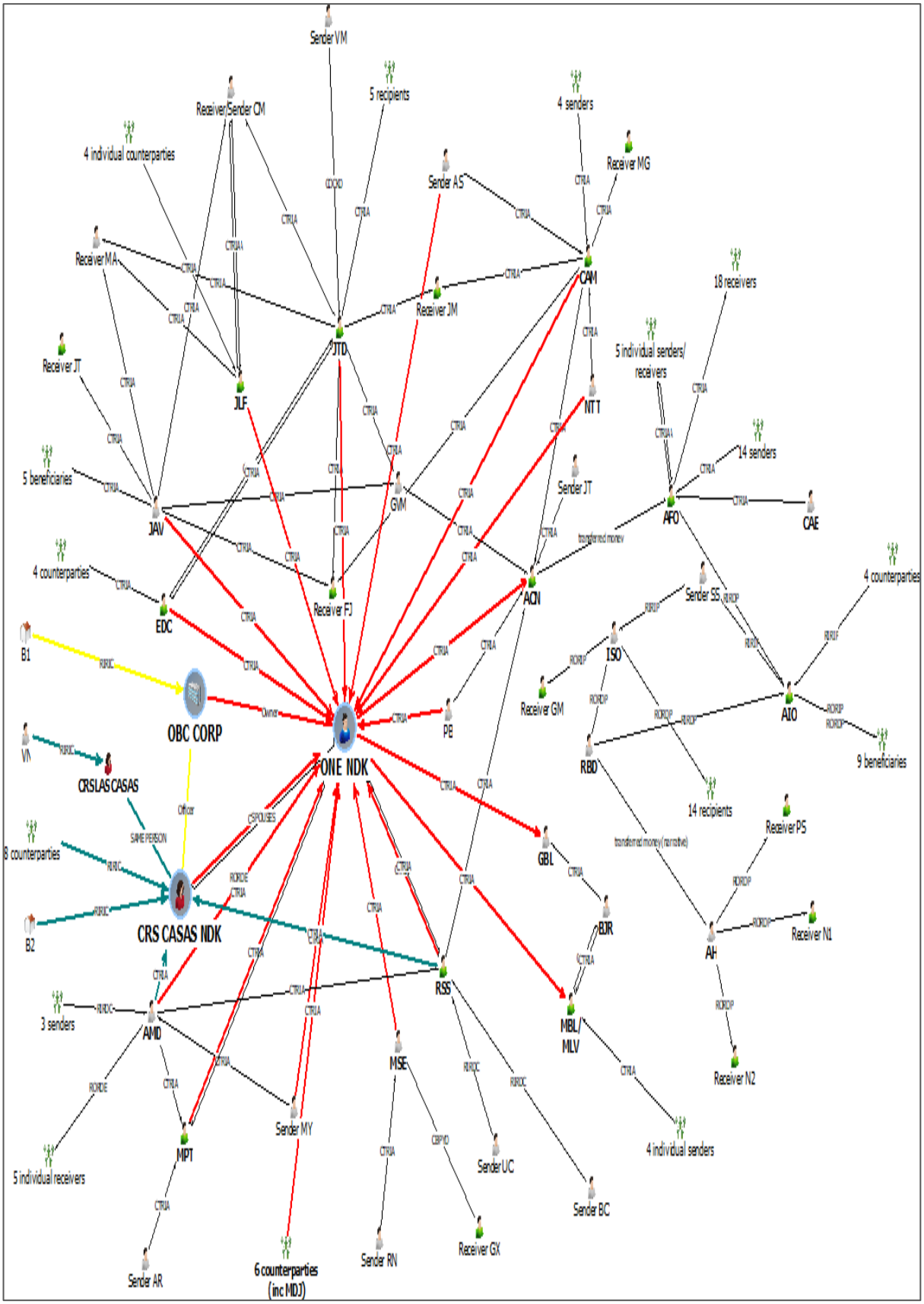
   It should be noted that OBC Corporation, as well as spouses NDK had been previously referred to the AMLC for investigation due to incidents related to romance scams, and swindling/estafa cases, as well as lottery scams. Notably, Mrs. NDK's alleged involvement in lottery scam, as reported by Bank O, concerns the subject's receipt of PHP0.5 million foreign inward telegraphic transfer from a certain VN on 20 October 2017.[41] Moreover, reported inward remittances of Mrs. NDK in various months from 2014 to 2017 originated from Australia, Czech Republic, Singapore, United Kingdom, and USA.

   For easier visualization, the following chart represents the transaction flow between the subjects and the account holders/beneficiaries/counterparties based on transaction reports submitted by CPs for the period 2009 to 2021:

[40] Ms. CRS Casas NDK (likely married name) and Ms. CRS Las Casas are one and the same, and subject names were identified separately to distinguish transactions of each one.

[41] The justification of Ms. CRS Las Casas is that the sender is a cousin of her husband and that there was a misunderstanding which will be clarified. Accordingly, the same sender transferred PHP1.3 million in the first week of November, allegedly intended to assist the NDK couple in house construction. To support this claim, the client submitted a building plan and specifications for the construction.

Fig. 19: Transaction Flow of OBC Corporation and Incorporators/Officers



Relative to **Figure 19,** the web-like feature of the transactions disclosed the interlinkages of the transactions related to OBC Corporation, its owner, and officers as well as the individuals involved. Transactions are largely cash deposits at PHP125.9 million and inter-account transfers (same bank) at PHP104.8 million. Significant is the concentration of the transactions to Mr. NDK and his wife. Moreover, individuals are also subjects of STRs from this dataset and most probably served as pass-through accounts or mules for OBC Corporation and Mr. NDK. Based on the narratives, Mr. NDK received fund transfers from various geographical areas. Most of the source of remittances were allegedly involved in various kinds of scams. Notably, the funds received were immediately disbursed through ATM, over the counter withdrawals or online transfers. Following discussions pertain to individuals identified as having transactional linkages to spouses NDK and OBC Corporation.

Notable high value transactions were those involving Nigerian nationals, Mr. ACN, Mr. AFO, and Mr. CAM. Among the Filipino subjects, high amounts and high counts were those of Ms. AMD, Ms. GBL, and Ms. RSS. While majority of the names identified in this particular case were included in the AMLC FIRs related to subject corporation and its incorporators, additional persons of interest from the dataset sprouted through linkages with Mr. CAN, namely, Mr. ISO, Mr. AIO, and Ms. RBD.

As reported by Company P, Ms. RBD is suspected of swindling by allegedly conspiring with an employee of subject company to disburse the proceeds of an international remittance meant for an individual worth PHP5.3 million sent through a bills payment facility. Correspondingly, Ms. RBD sent domestic remittances in 2017 to Mr. ISO, Mr. AH, and Mr. AIO. Mr. ISO was reported to have sent 39 domestic remittances, totaling PHP0.2 million to four (4) subjects with Nigerian-sounding names and one (1) Filipino among others, mostly coming from Cavite and Laguna.

Latest ZSTR filed by BRID, an EMI, in September 2021 on Mr. ISO revealed that subject was reported due to transactions with different customers and is suspected of involvement in money mule activities. Further, Mr. ISO, was a subject of an ad hoc investigation brought about by the investigation on alleged swindler, Ms. RBD, as cited above. Transactions of Mr. ISO per filed STRs retrieved from 6 January 2017 to 30 May 2018, comprised eight (8) domestic remittances summed at PHP4.2 million sent to seven (7) individuals with Nigerian-sounding names. Worth mentioning is that majority of the beneficiaries' pay-out locations were in Pangasinan. In addition, Mr. ISO received two (2) domestic transfers from Mr. AFO and Ms. RBD summed at PHP45,155 on 23 July and 16 November 2017. Likewise, international remittances were sent to the client from two (2) foreign nationals via money transfer on 20 January 2018 and 1 June 2017, respectively, with an aggregate value of PHP1.2 million, which were mostly processed at Company P's Las Piñas and Pasay City branches.

Deposits in cash, inter-account transfers, as well as withdrawals from various ATMs topped the modes of bank transactions utilized by the individuals related to OBC Corporation. Domestic transactions dominate the aggregate at 94.2%, equivalent to PHP283.0 million. International transactions cornered a minimal 5.8% or PHP17.4 million, which were mostly inflows from victims who were apparently duped into sending remittances, specifically from USA, Singapore, Czech Republic, Australia, and United Kingdom.

Top domestic locations of transacting branches based on peso value were from the National Capital Region, primarily the cities of Las Piñas, Parañaque, Makati, and Mandaluyong; Region III (Central Luzon), specifically in Pampanga; Region IV-A (CALABARZON) from Cavite; Region X (Northern Mindanao) from Misamis Occidental; Region XI (Davao Region) from Davao del Sur; and Region XII (Soccsksargen) from South Cotabato.

Romance and other scams

3. Three (3) Nigerian nationals were subjects of 1,216 STRs valued at PHP14.4 million reported by various CPs (a bank, EMIs, and pawnshops) from 2018 to 2021.

Table 10: STR Transactions[42]

Subject Profile	Transaction Years	Total STRs	STR Filing Years	STRs Total Amount in PHP
PMA	2018-2021	1,212	2020-2021	14,340,499
ROO	2020	1	2020	1,520
STE	2019	3	2020	49,520
Total		1,216		14,391,539

Among the three (3) subjects, Mr. PMA, a Nigerian national and a student at University X, cornered almost the whole reported transactions or 99.6% of the sum. While Mr. ROO and Mr. STE registered minimal amounts, the STRs identified the two (2) along with Mr. PMA and a Mr. PW as the ones who defrauded one (1) female customer.[43] It appears that the female customer has a boyfriend whom she met through Facebook messenger. Her boyfriend, who introduced himself as a resident of the USA, promised to send her gifts and packages. To receive the packages, however, the female customer was purportedly instructed to send money first as payment for customs fees to his alleged boyfriend's friends, who pretended to be employees of the Bureau of Customs. It was noted that Mr. PMA has been receiving numerous remittances from several individuals in which the declared purpose is for budget while the relationship indicated is as a friend. His transactions are considered suspicious since most of his remittances are coming from the elderly and middle-aged women.

Another CP reported a transaction where a client was supposed to send a domestic remittance to Mr. PMA for the clearance of an item shipped from Texas. The branch staff, however, was skeptical with the transaction and reviewed the record of the receiver. It was found out that Mr. PMA is a high-risk client, and said transaction did not proceed as the client/sender had doubts about the money transfer. Also, it was noted that the purpose of the remittance transactions of Mr. PMA varied. One branch said that Mr. PMA has an online business, the senders are his friends, and the purpose of the remittance transaction was for a project. On the other hand, it was reported in another branch that Mr. PMA is a student, and the purpose of remittance was for allowance. Another purpose of the remittances was payment for iPhone products. Most of the transactions of Mr. PMA were processed in Metro Manila branches. Open source and adverse news checking of the branch yielded no negative information on the client and counterparties. Based on the gathered information of the branch, however, the purpose of transactions and relationship with the counterparties were not properly justified.

[42] Figures in actual total due to disparity in values if translated to PHP millions

[43] A CP reported that a female customer went to their branch and claimed that she was defrauded by four individuals: PMA, STE, ROO, and PW. PW's name was not found in the STR database used for the study.

Table 11: Summary of Transaction Types[44]

Transaction Types	2018		2019		2020		2021		TOTAL	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
DEPOSIT - CASH	10	83,500	120	984,050	128	1,859,696	22	310,070	280	3,237,316
ELECTRONIC CASH CARD - LOADING					3	31,357			3	31,357
ELECTRONIC CASH CARD - WITHDRAWAL			3	12,060	1	1,520			4	13,580
INTER-ACCOUNT TRANSFERS (SAME BANK)	6	3,447	19	26,978	29	222,773	34	258,400	88	511,598
INWARD REMITTANCE (DOMESTIC) - ADVISE AND PAY BENEFICIARY			112	1,279,592	532	6,784,455			644	8,064,047
INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING			2	3,100	30	191,170	14	342,200	46	536,470
INWARD REMITTANCE (INTERNATIONAL) - ADVISE AND PAY BENEFICIARY			66	868,009	77	1,050,612			143	1,918,621
OUTWARD REMITTANCE/TT (DOMESTIC) - ADVISE AND PAY BENEFICIARY			4	66,200					4	66,200
RETURNED OUTWARD REMITTANCE/TT (DOMESTIC)			1	850					1	850
STR TRANSACTIONS					1	1,000	2	10,500	3	11,500
TOTAL	**16**	**86,947**	**327**	**3,240,839**	**801**	**10,142,583**	**72**	**921,170**	**1,216**	**14,391,539**

From 2018 to 2021, Mr. PMA's suspicious transactions were mostly deposits, inter-account transfers, as well as inward and outward remittances. Majority of the transactions were inward domestic remittances from various individuals, amounting to PHP8.6 million or equivalent to 60% of the total suspicious transactions. The subject also received international remittances amounting to PHP1.9 million (13% of his suspicious transactions). It was observed that most of the international remittances came from unknown sources while some originated from Hong Kong, Malaysia, Taiwan, United Arab Emirates, United Kingdom, and USA (based on addresses of the correspondent banks). On the other hand, outward domestic remittance transactions were minimal.

Similar to Mr. PMA, Mr. STE is also a Nigerian national and is said to be a student at University X. Mr. STE has been receiving numerous remittances coming from various Filipino individuals, usually middle-aged women working abroad. In addition, the declared purpose and relationship is doubtful. Mr. STE only has minimal suspicious transactions comprising two domestic inward remittances and one electronic cash card withdrawal.

<u>Deposits from unverified sources</u>

4. Thirteen individuals and one (1) business entity appeared in 801 suspicious transactions, amounting to PHP162.3 million reported by various banks, pawnshops, and EMIs. Apparently, said subjects were related parties in the Bank XYZ's hacking case that transpired between 12 and 14 June 2020. The list of names was identified from the AMLC FIR as well as from the narrative of STRs. Additional names included in this study are Mr. NSP, a Nigerian National, and Ms. GBL,[45] a Filipino. Ms. GBL is the purported owner of CGM which was previously identified in the AMLC FIR as having transactions with Ms. KSD. Ms. KSD was one of those identified as persons of interest (POIs) related to the Bank XYZ incident.

   Mr. NSP was cited in 271 suspicious transactions from the dataset amounting to PHP10.1 million. An online news identified NSP as one of the four (4) Nigerian suspects arrested by the NBI in relation

[44] Figures in actual total due to disparity in values if translated to PHP millions
[45] Ms. GBL was also involved in the transactions of OBC Corporation and its officer and owner (Case 2 of this report).

to the Bank XYZ hacking. Based on the STRs, Mr. NSP declared that he is a student with funds sourced from allowance sent by his parents in Nigeria. NSP's accounts were tagged as suspicious due to high aggregated cash inflows and outflows despite being newly opened. Over a 10-month period covering December 2019 to October 2020, volume of NSP's cash deposits totalled 90, valued at PHP4.4 million. Subsequent withdrawals (103 instances), totaling PHP3.5 million and 32 fund transfers to/from various individuals collectively at PHP2.0 million were also recorded on NSP's accounts in the same period.

Mr. NSP reportedly justified that the various cash deposits were from his other Nigerian friends for their enrollment/tuition fees, since the latter do not have accounts yet and are still on the establishment stage as students in the country. Further probing, however, disclosed that some of the counterparties of both debit and credit transactions of Mr. NSP are Filipinos and not purely Nigerians as previously claimed by the subject. The bank noted that the volume and value of NSP's transactions were not commensurate with his financial capacity, but mainly sourced from allowance, and deviate from his profile as student.

Between 2018 and 2021, high-value transactions were also noted on Filipino nationals, Ms. JAV, GBL, and KSD, totaling PHP89.5 million, PHP47.8 million, and PHP8.2 million, respectively. A suspicious alert (ZSTR) was triggered on Ms. JAV's account in Bank XYZ on 7 August 2020, due to receipt of unexplained transfer of PHP30 million on 29 April 2020. Bank XYZ Sucat branch noted the unauthorized additional deposit on the account with various withdrawals and fund transfers online. Also, in the Bank XYZ bank hacking in June 2020, subject's account was involved. Bank records indicated that Ms. JAV is connected, as President, with CRGI, engaged in mining, trading, and construction. In addition, Bank C narrates that the AML management committee approved the filing of an STR on Ms. JAV on 18 December 2020 due to subject's involvement in the Bank XYZ hacking and questionable updating made on her Bank C accounts during the period of the Bank XYZ cyber incident.

Ms. GBL was included as the owner of CGM, which was the subject of freeze order of an AMLA case received on 26 November 2020. The AMLC FIR found that CGM received PHP0.8 million from Ms. KSD on 12 June 2020 credited to its account. This was eventually withdrawn after three (3) days. Ms. GBL, on the other hand had significant transactions with Mr. One NDK, the details of which, was discussed in an earlier case (Case No. 2).

Alleged involvement with the African Drug Syndicate

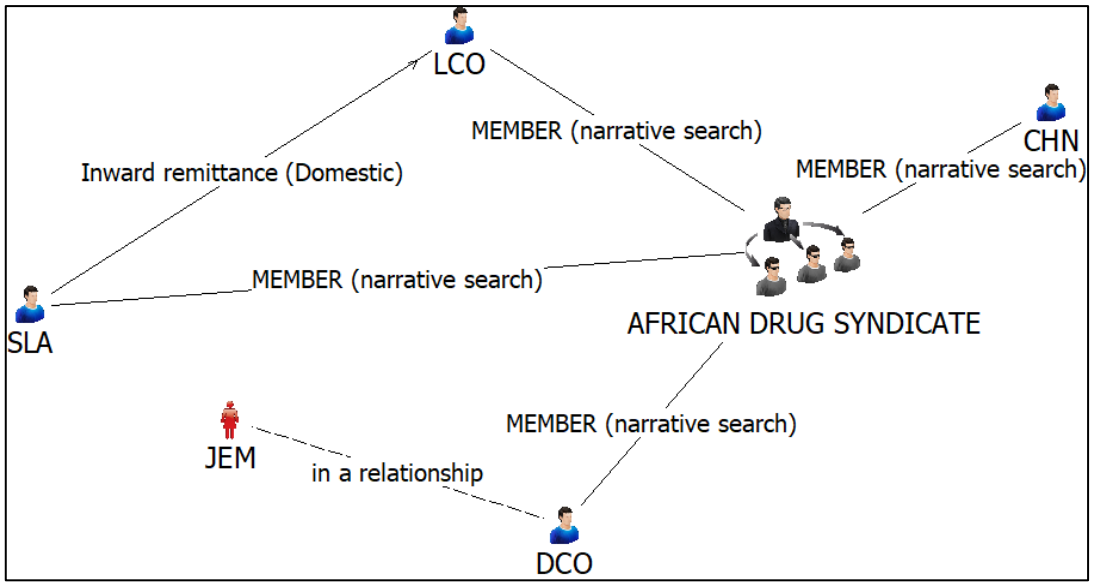
5. Five (5) individuals figured in 158 STRs estimated at PHP3.8 million on alleged involvement in drug-related transactions. The subjects are also tagged as part of the African drug syndicate (ADS). It should be noted that Mr. DCO and SLA were arrested by the Agency X in Cavite province on 8 November 2017 for allegedly supplying "shabu" (crystal meth) to Bicol region.[46] Ms. JEM, meanwhile, is identified as having a relationship with Mr. DCO and is also involved in drug-related transactions.

   Bank information revealed that Mr. DCO is operating a beauty salon. The accounts of Mr. DCO, however, were frozen pursuant to a freeze order dated 22 October 2020 for alleged involvement in illegal drugs. Mr. SLA likewise has had suspicious dealings with Mr. LCO.

   Following this, another ADS member, Mr. CHN, was arrested together with another Nigerian on 10 March 2018. Intelligence reports indicated that subject is engaged in the extensive distribution of shabu in the entire Bicol region and CALABARZON. Figure 20 shows the interrelationship of the suspected individuals who are all members of ADS based on the filed reports of CPs.

[46] Mr. DCO and SLA were high-value targets and included in the government's watch list as drug suppliers in Southern Luzon. Subjects are examining the possibility of expanding operations from Southern Luzon to the Bicol region.

Fig. 20: Transactions Related to ADS



Volume-wise, inward (international) remittances topped the number of ADS-related transactions (45 instances out of 158). In terms of PHP value, outward transfers (international) dominated the share with PHP1.4 million or 38% of the total. Also, 2017 seems to be the active year for the group both in terms of volume and corresponding peso-equivalent owed to the contributions of Mr. DCO and Mr. LCO during the period. Reported transactions tapered off in the succeeding years.

Alleged association with bank hacking incident

6. Eleven (11) individuals and three (3) entities figured in 56 STRs valued at PHP24.7 million on alleged involvement in the 2021 Bank ABC bank hacking incident.[47] Mr. CPN is one (1) of the five (5) suspects arrested by the NBI as the ones behind the unauthorized transfer of money of more than 700 Bank ABC customers in January 2022 bound to Bank FIJ accounts. The NBI informant revealed that while a Filipino offered phishing websites to perpetrators and used e-mails to send links of phishing websites to victims, the Nigerians provided devices to anyone looking for options to cash out illegally obtained funds. In addition, two (2) more Filipinos served as the web developers tasked to scout for vulnerabilities of bank websites.

   Based on a news article, alleged cybercriminals were able to access the victims' Bank ABC accounts, despite the latter not clicking any suspicious links. Clients of Bank ABC were surprised to receive emails, as well as text communications, notifying them of the bank transfer. Also, there were instances when the hackers were able to get past the one-time PIN (OTP) security feature of the bank.

   Moreover, an AMLC FIR identified that the Bank FIJ accounts of four (4) Filipinos DE, LPD, RTC, and DMT, with corresponding STR value of PHP7.7 million, were found to be recipients of funds from Bank ABC and apparently were used by a certain "J Scammer" who is not an account holder of Bank FIJ.[48]

[47] Analysis comprised STRs with related keywords "Bank ABC hacking," Bank ABC cyber," as well as those names that figured in a 2022 FIR of the AMLC, which are all included in the study's dataset.
[48] Findings from the AMLC FIR detailing the Bank FIJ account numbers of DE, RTC, and LPC as being used by a certain "J Scammer". Likewise, the account number of Ms. DMT uses the alias JMU.

Mr. GKR generated the highest number of STRs from the dataset related to this case valued at PHP9.3 million. The STRs narrated that the subject's account was identified as one (1) of the recipients of funds from the hacked Bank ABC accounts as well as the first to third level beneficiary of the earlier mentioned DE and RTC accounts. Also, Mr. GKR was previously asked for supporting documents to establish the legitimacy of the various online bank transactions given the declared source of fund as a medical student. The subject disclosed involvement with cryptocurrency exchange trading.

Notably, Bank ABC-related hacking transactions from the dataset prominently occurred in 2021 and were found to be mostly inter-account transfers valued at PHP22.3 million with 41 counts, which is anticipated considering the scheme done in this case. Deposit in cash follows behind at PHP1.5 million.

Table 12: Aggregate Transaction Volume & Value[49]

Transaction Types	2018		2021	
	Volume	Value	Volume	Value
DEPOSIT - CASH			3	1,508,260
ELECTRONIC CASH CARD - WITHDRAWAL	1	200	2	189,000
INTER-ACCOUNT TRANSFERS (SAME BANK)			41	22,260,300
INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING			2	712,241
INWARD REMITTANCE (INTERNATIONAL) - ADVISE			3	30,096
OUTWARD REMITTANCE/TT (DOMESTIC) - CREDIT TO BENEFICIARY'S ACCOUNT			4	9,470
Total	**1**	**200**	**55**	**24,709,367**

Recruitment of money mules

7. Money mules are recruited via face-to-face, online job scams, social media networks, and romance scams. Some were duped into believing that such is a legitimate transaction and were attracted with the lucrative return.

For instance, Ms. RS is a sari-sari store owner who was recruited by a certain Mr. O into what the subject thought was a legitimate money scheme. Apparently, Mr. O promised Ms. RS a portion for every bank transaction. Mr. O is a Nigerian national who was arrested in 2019 for allegedly operating a multimillion online scam.[50] It should be noted though that Ms. RS collaborated with the authorities on the entrapment operation for Mr. O in Trece Martires City on 16 November 2019.

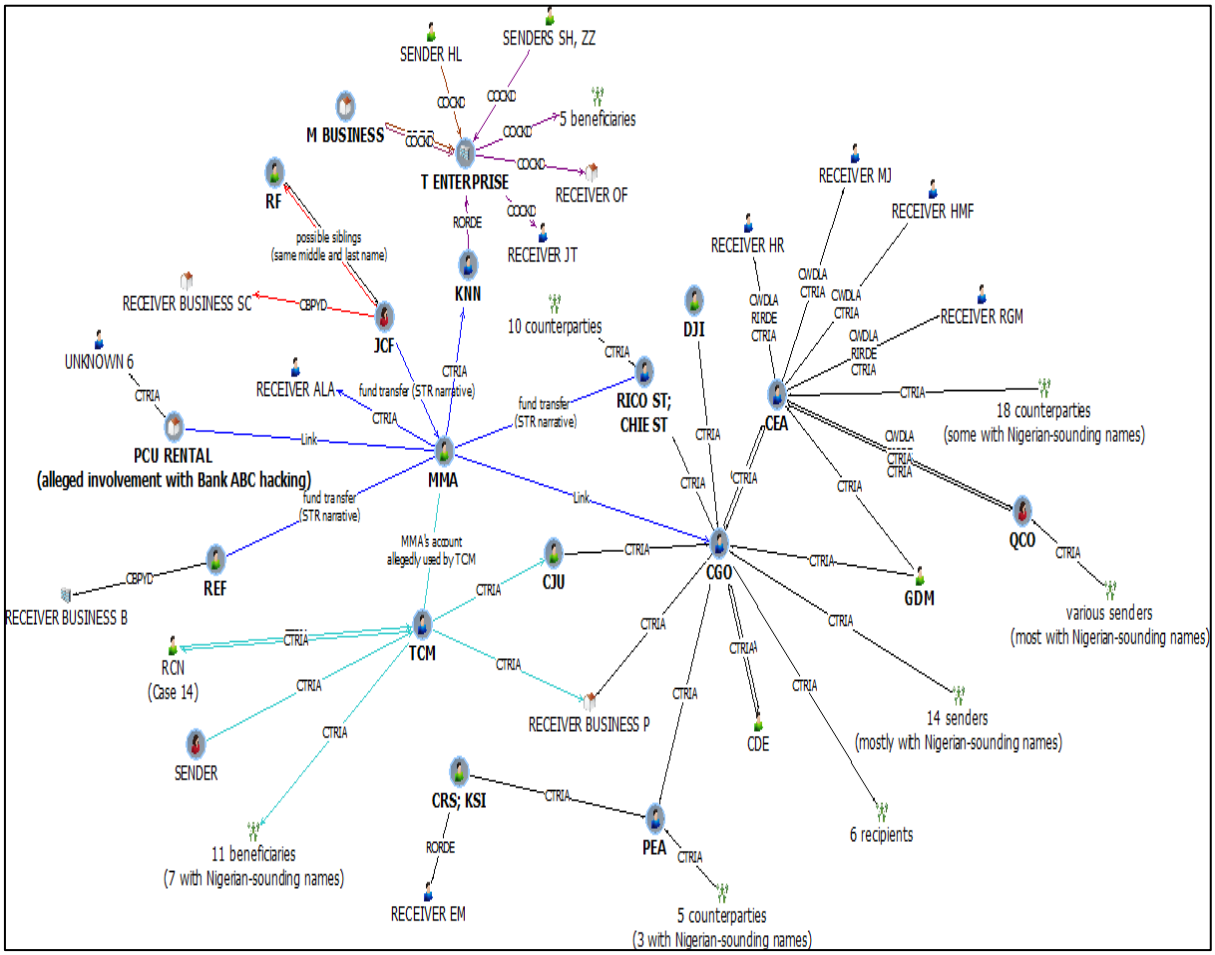
Ms. RS figured in 83 transactions valued at PHP3.6 million for a six (6)-month period in 2019. Notably, all transactions were purely cash-based (i.e., cash deposits, and withdrawals via ATM, and over-the-counter). This tends to obscure the audit trail as identifying the ultimate source (deposits) and destination (withdrawals) of funds becomes challenging.

For the second case, 16 individuals and three (3) entities figured in 1,295 STRs, estimated at PHP178.8 million. The link chart (**Figure 21**) below revealed the intricate connections of alleged money mule, Ms. JCF, to alleged scammer, Ms. MMA, who has transactional linkages with Mr. TCM and Mr. CGO leading to other individuals as well as entities involved in other scams.

[49] Figures in actual total due to disparity in values if translated to PHP millions

[50] Mr. O entered the Philippines using a student visa in 2015 and is involved in a love/romance scam, swindling around PHP8 million from a "senior citizen" and a business woman from Cagayan Valley.

Fig. 21: Link Analysis of the STRs on JCF, MMA, TCM and linkages



In detail, a suspicious transaction report filed by Bank FIJ on Ms. JCF[51] led to suspected scammer, Ms. MMA, whose account was interlinked by transactions with several other individuals as well as entities – starting with that of alleged Nigerian friend, Mr. TCM.[52]

Upon the bank's review, Ms. MMA opened an account under Bank FIJ on 24 July 2021 and she informed that the money and transactions were those of a Nigerian friend, Mr. TCM. The rationale is that Mr. TCM could not open a bank account due to his nationality, thus, Ms. MMA's Bank FIJ account was utilized. This is questionable as a digital account was opened by Mr. TCM at Bank FIJ Cubao branch on 6 August 2021, and he also has accounts at Bank ABC, Pangasinan branch.

According to the STR, funds were received and disbursed mostly online via Instapay fund transfers and cash-ins to partner banks as well as ATM cash deposits. Alerted transactions on Ms. MMA's accounts were transfers to PCU Rental (involved with Bank ABC hacking from Case 6), KNN, Rico ST (linked to Chie ST); RF; and CGO.

Mr. TCM is a student and a client of the DP Spa where Ms. MMA works. Open-source search revealed that a certain TCM is at present a medical student at University A. From the said LinkedIn account, the subject person was a pharmacy intern at HS Hospital in Urdaneta, Pangasinan from May 2018

[51] Transaction review on the account of Ms. JCF revealed that the purpose of opening is for online fund transfers and US Instapay transactions. Also, subject had a credit transaction from Ms. MMA amounting to PHP0.2 million on 9 August 1991.
[52] Linked in account disclosed that TCM is a medical student from University A (June 2020 to present).

to June 2020. Coincidentally, filed STR of Emix with transaction date 18 September 2018 identified Mr. TCM's address as in Pangasinan. A transaction on 29 June 2020, however, identified the subject's address as located in Parañaque with proximity to the location of his declared job at a hospital in Manila (as a clinical pharmacist), covering the period August 2019 to June 2020. Emix further informed in another STR that after the conduct of complete validation and investigation, Mr. TCM perpetrated an identity fraud, recognized as having the same face of a previously confirmed fraudster.

The STR dataset used in the study revealed the following subjects with transactional linkages with Ms. JCF, Ms. MMA, and Mr. TCM (Figure 21). Based on the dataset related to this case, Ms. QCO garnered the most number with 641 STRs, totaling PHP35.2 million. Ms. QCO's transactions ranged from PHP500 to PHP0.5 million, which she declared as coming from her online business of selling shoes and dresses. There were no documents to support Ms. QCO's claim, and her account was closed as of the CP's reporting date of May 2021.

T Enterprise figured in 34 transactions in 2019, totaling PHP91.8 million. Entity reportedly submitted a Department of Trade and Industry (DTI) certificate to Bank ABC, Cebu branch upon account opening. The entity is engaged in retail and wholesale of China wares under the sole proprietorship of Ms. ML. Bank's review of T Enterprise's account revealed that the aforementioned transactions made in a span of five (5) days (covering 5 to 9 July 2019) were deemed as not commensurate with the declared source of funds.

Package scam

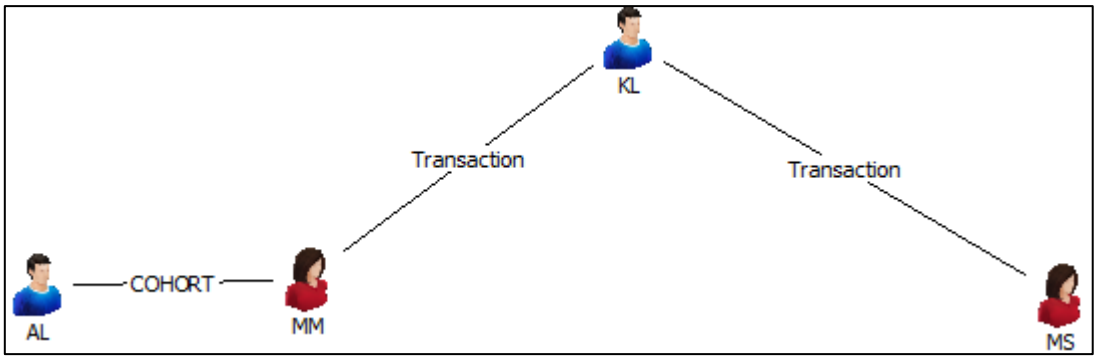
8. Mr. KL, a Nigerian national, is included in the list of customers provided by a covered person (an EMI), on possible involvement in suspicious activities through the use of mobtels (mobile telephone). Mr. KL's account posted significant deviations on transaction amounts over the years. He had one (1) transaction involving mobtels (electronic cash card/gift card/debit card – withdrawal), amounting to PHP2,298. Mr. KL also received a total of PHP0.2 million in 2018 pertaining to six (6) remittance transactions from a certain MS. Moreover, Mr. KL received 104 remittance transactions from Ms. MM, amounting to PHP3.7 million.

   Ms. MM received transactions coming from various individuals who are possibly victims of their deceitful acts where the declared purpose was mainly for business while relationship to sender is either a client or a friend. The CP specified that Ms. MM had a total of 104 outward remittances, amounting to PHP3.7 million and 78 inward remittances, amounting to PHP2.7 million.

   In addition, Ms. MM is apparently a cohort of Mr. AL. A customer of said pawnshop requested pertinent documents, concerning Mr. AL and Ms. MM who are allegedly involved in swindling activities. Said customer went to a branch of the pawnshop to send remittances with aggregate amount of PHP78,000 to Mr. AL, where the purpose was payment for a package and the stated relationship to the receiver as "company representative of EG," a global courier. The remittances were released on the same day in one of the pawnshop's authorized agents and the declared purpose was payment, while the relationship indicated was as "a friend." In the pawnshop's conduct of due diligence, it was learned from the customer (sender) that the foregoing remittances were payment for her anticipated package coming from her son-in-law. Purportedly, the customer received a call from a representative of EG informing that her package has arrived in the airport, but she needs to pay PHP78,000 for its release to be coursed through a certain Mr. AL who is referred to as an agent. The fraudulent act was only discovered when the customer's daughter informed her that there is no package being sent by her husband (the victim's son-in-law). Moreover, the customer tried to communicate with the alleged agent, who, unfortunately, can no longer be contacted. Relative to this, a copy of the CCTV footage and other necessary documents of Mr. AL

and Ms. MM were requested, and said incident was also reported for blotter at the PNP. The pawnshop deemed the transactions of Mr. AL and Ms. MM suspicious due to the swindling complaint filed by the package scam victim.

Fig. 22: KL Transaction



Package Scams & Pass through-Accounts

9. Six (6) individuals were subjects of STRs involving package scam. Upon verification of the reporting entities, subject individuals mentioned allowing their accounts to be used by their Nigerian boyfriend/friend/partner. Details of the transactions are enumerated below:

   a. Mrs. APM's transactions are not commensurate with the declared source of income. In addition, the branch received several complaints from other branches indicating Mrs. APM's involvement in a scam. One of the complainants said that he/she paid the customer's account intended for shipping and processing fee of a package they are expecting to receive overseas. Mrs. APM initially claimed that her ATM card was stolen. She later, however, admitted that she lent her account to a Nigerian friend with a promise of payment. Mrs. APM does not have any supporting documents to validate her claim.

   b. Ms. GLL has 17 cash deposit transactions, totaling PHP0.4 million and one (1) remittance transaction, amounting to PHP24,056.4. Based on the CP's interview with Ms. GLL, it was found that the client gave her ATM card to her Nigerian boyfriend, and she had no idea of the transactions in her account. Hence, the underlying legal or trade obligation, purpose, or economic justification of the transactions cannot be ascertained. In addition, the CP received a complaint involving the account of Ms. GLL on scam allegations, where a victim purportedly received a telephone call that a certain package shall be sent to him/her and that someone from the customs office will call the victim for further instructions. Ms. GLL's account was closed in 2018.

   c. Ms. JB's account with Bank O was the subject of multiple complaints demanding refunds for the tracking fees solicited for fictitious packages. The messages of the alleged victims were sent via the Facebook page of Ms. JB. The client then went to the bank's branch to report said incidents and disclosed that her account was being used by her Nigerian partner who apparently sends e-mails to various individuals advising them of a tracking fee that needs to be paid for the delivery of an expensive valuable from London. She declared that she was aware of that and has allowed her partner to gain full control of her account, including her ATM as well as online banking account. Ms. JB received deposits, totaling PHP3.1 million, from 5 June 2020 to 21 January 2021 and these funds were subsequently withdrawn either via ATM withdrawals or inter-bank transfers, leaving the account with minimal balance. The branch's open-source verification shows that the client is engaged in online selling of ready-to-wear items. Verification was done due to inconsistent volume of transactions with client's profile.

d. A client went to a bank's branch and reported a possible fraud transaction involving Ms. PDL's account. The client mentioned that he deposited PHP14,500 to the account of Ms. PDL for payment of tax for the shipment of a package. The victim allegedly received the instruction through text message from Ms. JO. Review of the transactions disclosed that funds were immediately withdrawn on the same day through ATM. Further review revealed that the account received 34 cash deposits, amounting to PHP0.8 million and 11 inward Instapay transactions, totaling PHP0.1 million from various remitters, which were withdrawn immediately on the same day of credit. Ms. PDL disclosed that she is not aware of the transactions and added that she gave the ATM card to her Nigerian ex-boyfriend in exchange for a certain amount of money which was not disclosed.

e. Ms. RLG's branch of account (BOA) received information from another branch informing that its client made a deposit of PHP0.1 million in favor of Ms. RLG's account allegedly as payment of customs fee for a package, amounting to USD2.5 million. Though there is no formal complaint from the client, the scheme appears to be an online fraud related to package scam. Ms. RLG disclosed that her Nigerian partner had used her ATM account in the past, but said partner is already in custody of the PNP. The branch also noted that the transactions are not consistent with the purpose of her account-opening. Review of the account noted three (3) cash deposits, amounting to PHP0.3 million, including the PHP0.1 million mentioned earlier. It is worth mentioning that Ms. RLG voluntarily closed her account during a branch visit.

f. Review of Ms. RAP's account showed that her transactions are not commensurate with her declared source of funds as a part-time helper at her sister's store. The branch noted 30 interbranch credit and debit transactions summed at PHP0.4 million, covering 30 August 2017 to 7 September 2017. Ms. RAP disclosed that her account is being used by her boyfriend, a foreign individual of Nigerian South African descent, who is using the name EC. The account of Ms. RAP is suspected of being used in a fraudulent activity, where a potential victim is instructed to deposit a certain amount in return for a package.

<u>Deposits from unverified sources</u>

10. Between 6 December 2019 and 6 November 2020, NFN figured in 27 STRs, pertaining to inter-account transfers under Bank O. Said STRs amounted to PHP0.5 million, of which 30.7% or PHP0.2 million were outward transfers to four (4) other Bank O accounts and 69.3% or PHP0.4 million were inward transfers to NFN's savings account.

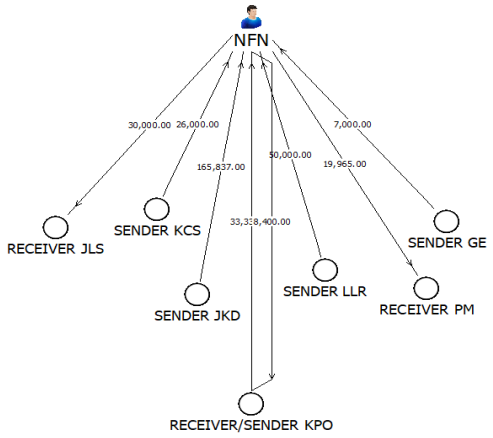
    On 11 December 2020, Bank O received a report from Bank D, regarding a confirmed phishing incident that resulted to several unauthorized fund transfers involving a Bank O savings account belonging to Ms. JKD. Upon review of Ms. JKD's transaction history, 13 online fund transfers to NFN's savings account were found. Said online fund transfers were completed between 10 July 2020 and 6 November 2020, and had values ranging from PHP5,000 to PHP50,000.

    Bank O's examination of NFN's savings account revealed several inward transactions consisting of cash deposits, online payments, and fund transfers, ranging from PHP5,000 to PHP72,943, which were deemed to be inconsistent with his declared profile and source of funds. NFN's transaction

history likewise showed outward transactions consisting of withdrawals made over the counter and via ATMs, and transfers to other deposit accounts.

Based on Bank O's records, NFN is a 23-year-old unmarried Nigerian citizen who relies on monthly allowances of PHP10,000 as his source of funds, which were not substantiated. Upon further inquiry, NFN told his BOA that the funds credited to his account came from his parents. He denied connections with or knowledge of Ms. JKD but admitted sharing his account number to his family and friends.

Fig. 23: Network of NFN
06 December 2019 – 06 November 2020



Possible pass-through accounts

11. Mr. TGO was the subject of 23 STRs filed by Bank O on 13 December 2018 due to unusually frequent transactions associated with his account. Based on the STR narratives, Mr. TGO's account recorded 97 transactions with an aggregate amount of PHP2.9 million, in just a span of 35 days, covering 5 November 2018 to 10 December 2018. These transactions comprised 17 cash deposits, totaling PHP1.1 million; 23 online fund transfers, totaling PHP0.4 million; 10 over-the-counter withdrawals, totaling PHP1.1 million; and 37 ATM withdrawals, totaling PHP0.3 million. In contrast, however, the 23 STRs found on the AMLC database summed up to PHP0.4 million only and indicated Mr. TGO as both the account holder and beneficiary of said inter-account transfers.

    During the probing process, Mr. TGO claimed that most of the fund inflows were given by his uncle as his allowance and for the payment of his tuition fee. Mr. TGO, however, did not disclose the name and profile of his supposed uncle. In addition, Mr. TGO admitted that his unnamed friends were also using his account to receive funds in their favor. The account behavior is indicative of a pass-through pattern, where the total fund inflows stood at PHP1.5 million and fund outflows at PHP1.4 million.

    Meanwhile, two other CPs filed STRs on Mr. TGO on the basis of an AML investigation being conducted on Nigerian students and Mr. TGO's outward transfers were deemed as not commensurate with his declared profile. Said CPs are Emix and AD, Inc. Specific to the report of AD, Inc., it stated that the client sends large amounts of money without familial relationship or an underlying legal trade obligation. Further, no supporting documents were presented to establish legitimacy of relations.

Drug-related transactions

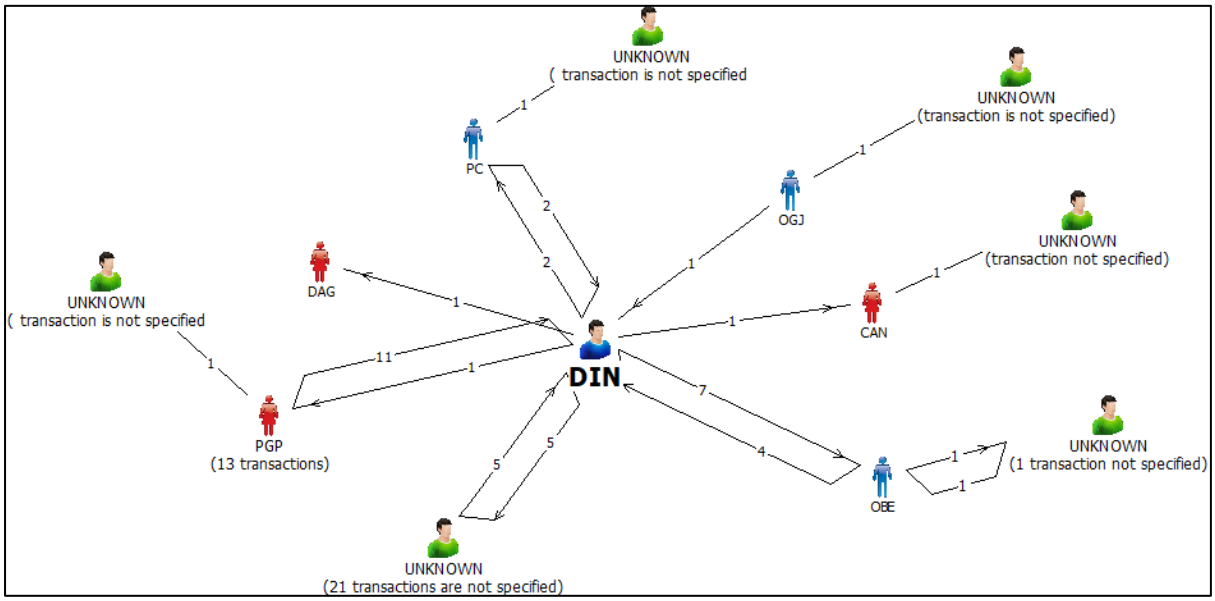
12. Mr. DIN and four other individuals had been the subject of 68 related STRs filed by Bank O, Bank TM[53] and Emix with the estimated value of PHP0.5 million. Most of the transactions pertain to Mr. DIN. Notably, subject individuals were mostly from Dagupan, Pangasinan except for Mr. OGJ, who is from Las Piñas, Metro Manila. Most of the transactions were cash deposits followed by inter-account transfers (same bank). Money transfers were in small denominations ranging from PHP150

[53] Filing CPs are Bank O and Bank TM's branches in Pangasinan.

to PHP42,000. Moreover, **Figure 24** presents the transactions of Mr. DIN and other related subjects to individuals, who are either recipients or senders of funds, including the number of transactions.[54]

Data from the BI disclosed that Mr. DIN entered the Philippines from Istanbul, Turkey in 2016 to seek admission at the University K which, coincidentally, is in Pangasinan. Total travels of Mr. DIN to and from Manila are six (6) (i.e., Turkey, Ethiopia, and Thailand). Correspondingly, another subject with eight (8) travels to and from Turkey and Manila between 2020 and 2021 is Mr. OGJ.

Fig. 24: Network of Mr. DIN



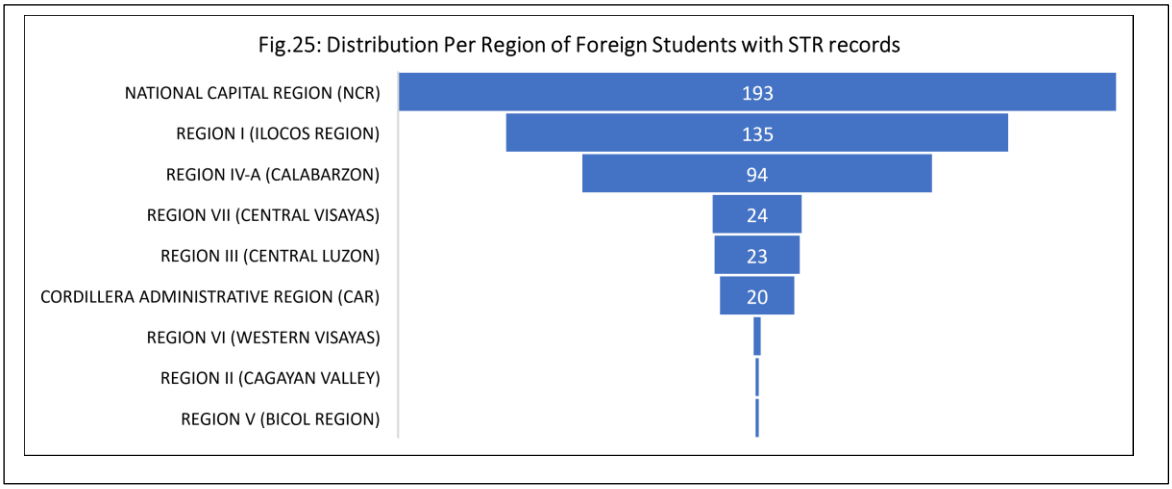
13. The following cases involve two (2) Filipinas' accounts which were probably being used/borrowed by their Nigerian boyfriends. For the first case, Ms. CCB was reported by Bank ABC from Nueva Ecija branch since the 24 cash deposit transactions made to her account were deemed as not commensurate with the subject individual's declared source of income. Upon verification, Ms. CCB reasoned that said funds came from her Nigerian partner's salary on the projects he made as an information technologist. Further confirmation led the bank to the Facebook page of the police station wherein Ms. CCB[55] and her Nigerian partner, named JLB, were caught for violation of RA 9165 (Comprehensive Dangerous Drugs Act of 2002). Moreover, the posted FB article mentioned that client is the number one personality in the drug watch list as well as a notorious drug pusher in Nueva Ecija.

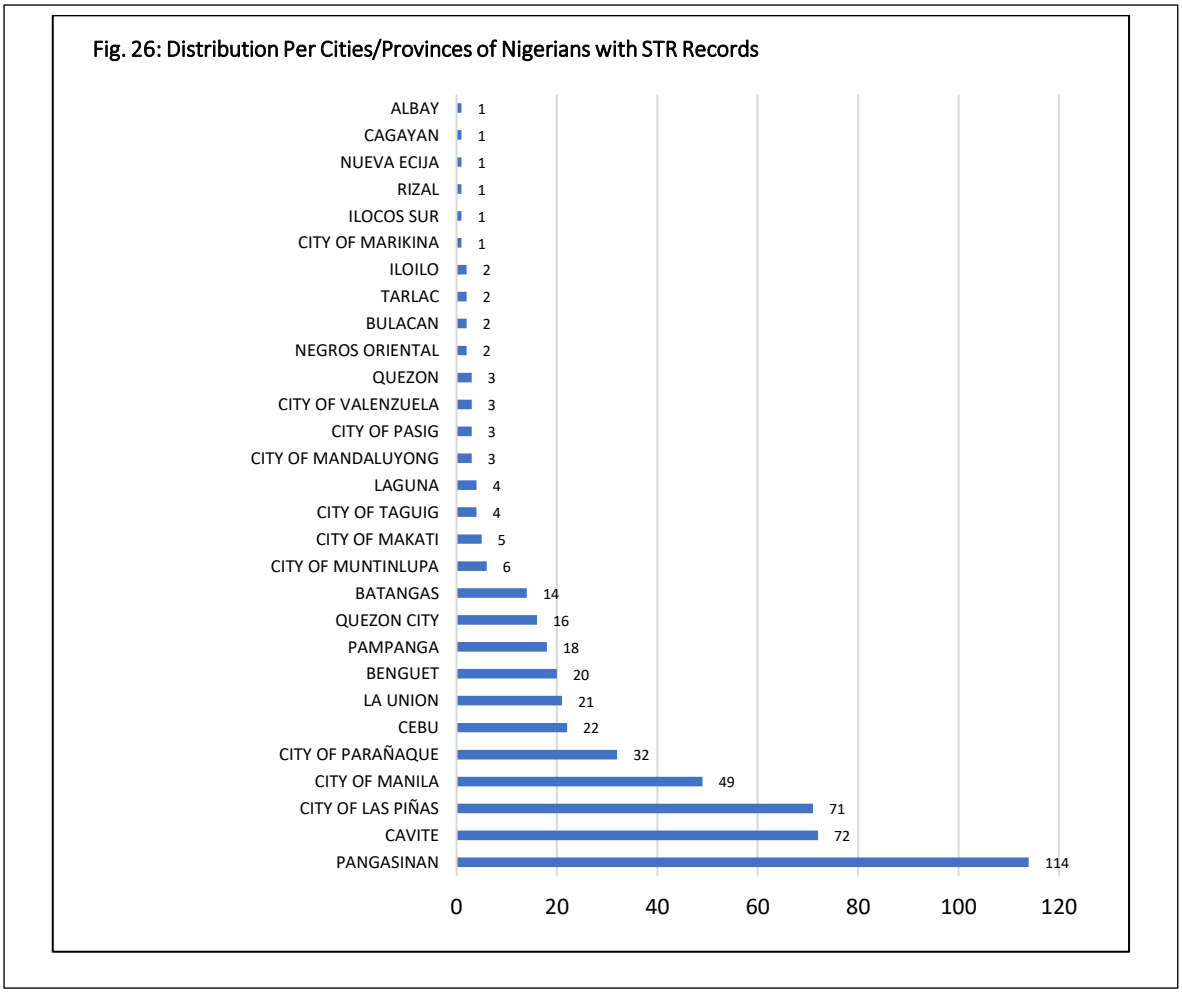
The second Filipina, Ms. RBR,[56] was recognized as the female nabbed in a buy-bust operation along Makati City together with a Nigerian partner. Ms. RBR, known for her alias "BX," and the Nigerian partner named LCU alias "NX," both residents of Cavite, were nabbed and seized from them were 400 grams of alleged crystal meth worth PHP2.7 million; a Toyota Altis; and two (2) mobile phones. Said incident indicated that the suspects will be charged for violations of RA 9165 or the Comprehensive Dangerous Drugs Act of 2002.

[54] Unknown beneficiary/counterparty were limited to one (1) representative to simply indicate the presence of unknown co-transactors, which is 45.6% or 31 out of the 68 STRs.
[55] An STR stated that Ms. CBB was identified as a confirmed match via full name and photo on said Facebook post in 2019.
[56] Bank O, Cavite branch, confirmed that client is one and the same person.

Various PCs: Swindling (romance/love scam, custom fees scam, poor investment) and illegal drugs

14. Around 502 Nigerians who entered the country and identified/registered themselves as students were scattered in nine (9) regions in the country, the topmost of which includes the NCR (193), Ilocos Region (135), CALABARZON (94), Central Visayas (24) and Central Luzon (23). Specifically, per cities/provinces, the chief areas are Pangasinan (114), Cavite (72), City of Las Piñas (71), City of Manila (49) and Parañaque (32) (**Figures 25** and **26**).[57]





[57] The list of names was lifted from the dataset, using the narrative search as well as filtering names of students from the Emix study, where nature of work of customers is one of the required personal information during registration. Eight (8) of the 508 have registered addresses in Nigeria.

Moreover, from the student dataset, 29 individuals were enrolled in 19 schools or universities in the country based on the details of the STR narratives, BI's remarks, as well as open source (Table 13).

Table 13: Schools/Universities of the Students

Schools/Universitites	Number of Students
University X	6
University X, Las Piñas	5
University X, Laguna	1
University S	2
University D	2
University H	2
University AD	2
University AU	1
University M	1
University F	1
LZ School	1
University Y	1
University L	1
University N	1
University PT	1
University C	1
PA School	1
University DC	1
University T	1
University U	2
University V	1
Grand Total	**29**

For this paper, detailed analysis of STRs involving Nigerian subjects from three (3) schools/universities, focusing on Pangasinan, Cavite, and Las Piñas. These were selected based on the area with the highest number of students. This is under the assumption that these students will rent/live in the areas near their schools/universities.

Figure 27 shows the dispersion of Nigerian students to various areas, mostly in Luzon, and principally in Pangasinan, Cavite, and Las Piñas. The top locations showed three (3) universities from Pangasinan namely PA School, University Y, and LZ School; one (1) from Cavite (University S), and one (1) from Las Piñas City (University X). Notable were the alleged involvement of the students themselves or their conspirators in various predicate crimes, mostly swindling (romance/love scam, custom fees scam, poor investment) and illegal drugs.[58] KYC records show that source of income were allowance from parents, support from relatives, and online businesses. Some even stated that their accounts were being used by other Nigerian students.

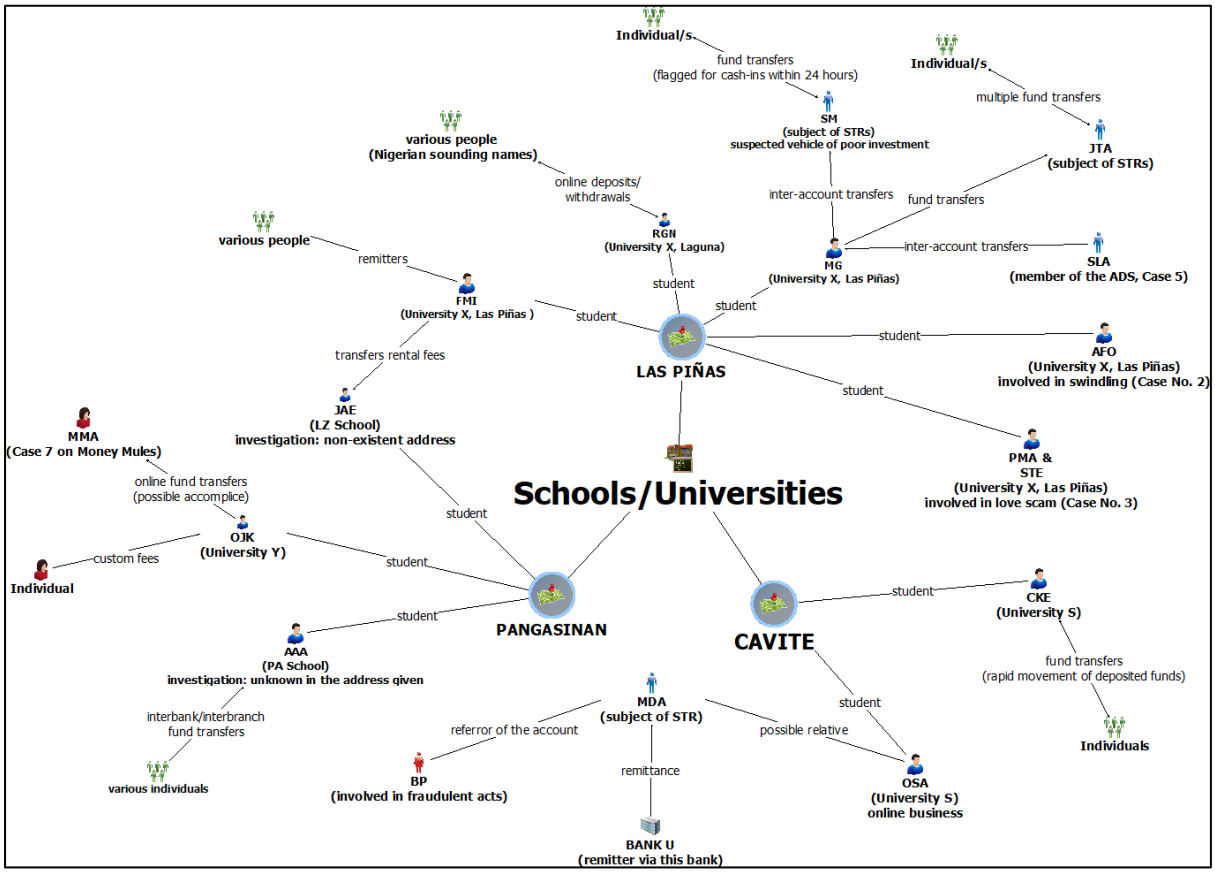
While these students may have legally passed the temporary visa requirements of a foreign student from the Department of Foreign Affairs, extension may be requested through the BI.[59] Further to this, one of BI's specific function is the accreditation of schools and learning institutions that can officially accept and enroll foreign students.[60] This is in accordance with the Department of Education and Commission of Higher Education guidelines. The school then has the responsibility of establishing a foreign student unit as well as submit to BI a monthly periodic report on foreigners enrolled in their school; and students who transferred, who were dropped from the rolls, who are with derogatory reports, or who went missing. Also, Section 10 of Republic Act No. 562, as amended, or the Alien Registration Act of 1950, mandates all registered aliens to report in person to the BI within the first 60 days of every calendar year.[61] Considering that the BI has the power to accredit and revoke the accreditation of the schools to accept foreign students, the BI can use that to strictly monitor that schools/universities submit their monthly status report pertaining to foreign students specifically on any derogatory record that may occur.

a. **Province of Pangasinan:** Five (5) individuals were reported to be enrolled in schools/universities in Pangasinan, which were narrowed down to three (3) since the other two (2) have been discussed in

[58] Mr. MG is the beneficiary of transactions involving Mr. SLA, a known ADS member.
[59] Temporary student visas are given for a period of six (6) months, while for extension of periods of stay, the student will have to report to BI and secure the extension of stay and pay the corresponding immigration fees. Retrieved from https://dfa.gov.ph/guidelines-requirements (accessed on 11 August 2022).
[60] https://immigration.gov.ph/the-bureau/functions (accessed on 11 August 2022).
[61] Retrieved from https://immigration.gov.ph/images/AnnualReport/AnnualReportGuidelines2022.pdf (accessed 11 August 2022).

earlier cases in this paper.[62] These are identified as Mr. JAE (LZ School), Mr. AAA (PA School), and Mr. OJK (University Y).

Fig. 27: Selected Areas and Schools/Universities



Mr. JAE has reportedly been living in the Philippines for a year. While his school is in Pangasinan, he prefers to live in Pampanga and merely takes a bus to go to his school in Dagupan. Bank BS, Pampanga branch conducted EDD on the client due to various interbank transfers done via mobile wallet. The client allegedly failed to provide supporting documents for the 100 notable online transfers made thru the said fund transfer facility. Specifically for transaction dates covering 2019 to 2020, client figured in 109 STRs which are largely domestic inward remittances, amounting to PHP0.4 million. There were five (5) inter-account transfers (same bank), amounting to PHP37,172, which apparently came from Mr. FMI who is from University X, Las Piñas branch.

Mr. JAE's sources of income are allowance from parents as well as the share in house rentals and food of friends staying at his apartment (one is Mr. FMI). The client failed to provide supporting documents for his claims. Considering that Mr. FMI is enrolled at University X, Las Piñas and his declared addresses did not include the address of Mr. JAE in Pangasinan gave rise to the suspicion. Further, background investigation on 23 November 2020 disclosed that the given address of Mr. JAE is non-existent.[63]

[62]DIN (University K) was the major subject in Case 12 related to illegal drugs, while Ms. KSI (MVF) was discussed in Case 7.2 JCF, et al., pertaining to money mules.

[63] The STR stated that given street address is a dead-end street, where house numbers have two (2) digits, and long-term residents are not aware of an individual named JAE.

Table 14: Pangasinan Area STRs[64]

Subject Names	Transaction Dates	Total STRs	Transaction Types	Total Amount in PHP
JAE	2019	1	ELECTRONIC CASH CARD WITHDRAWALS	15
	2020	5	INTER-ACCOUNT TRANSFERS (SAME BANK)	37,172
	2020	103	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	368,981
OJK	2018	1	ELECTRONIC CASH CARD WITHDRAWALS	50
	2021	1	INTER-ACCOUNT TRANSFERS (SAME BANK)	36,000
AAA	2020 - 2021	3	DEPOSIT - CASH	137,100
	2019	1	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	1,254,354
TOTAL		**115**		**1,833,672**

Mr. AAA was reported by the bank since a certain JD alleged that she was defrauded by Mr. AAA in the amount of PHP12,000, representing payment for custom fees. Based on the STR narrative, Mr. AAA's account received two (2) interbank deposits of PHP40,000 at Bank B-Tayug branch on 8 January 2021 and 59 inward remittances credited from 26 November 2019 to 18 February 2021, ranging from PHP1,000 to PHP50,000 and aggregated to PHP1.25 million. The client's claim of allowance from parents in Nigeria failed to substantiate the transfers and the account was closed on 30 March 2021. The bank visited the given address of the client, but the lessor denied having a tenant named AAA.

Mr. OJK, on the other hand, was the one sending funds to an alleged scammer Ms. MMA (Case 7 on Money Mules). Based on the STR narrative, the total credited amount to Mr. OJK's account amounted to PHP18.8 million with the corresponding debit of PHP18.8 million, covering 24 August 2020 to 14 September 2021. Credits to Mr. OJK's account were immediately transferred to other accounts or withdrawn through ATM. The client claimed that aside from allowance from his parents, most of the fund transfers were transactions from cryptocurrency trading. Moreover, according to CP's October 2021 STR, it sought to temporarily freeze Mr. OJK's account in preparation for account closure.

b. **Province of Cavite: University S**. Identified students from this university fared in 34 STRs with estimated value of PHP2.7 million. The first student, Mr. CKE, with address in Cavite was reported by Bank ABC in Cavite due to the amount of deposited funds coupled with rapid movement of funds. The branch further noted a cash deposit, amounting to PHP0.4 million that was immediately withdrawn in tranches thru ATM in a span of two (2) days. As per branch evaluation, client's transactions are not commensurate with the declared source of funds as student in University S. Mr. CKE apparently took up Engineering from the said university based on the thesis of a certain individual with a similar name. Notably, the receiver of funds cannot be identified from the filed reports thus, the limitation in the analysis of the involved persons.

[64] Figures in actual total due to disparity in values if translated to PHP Millions.

Table 15: STRs of Individuals from University S[65]

Subject Names	Transaction Dates	Total STRs	Transaction Types	Total Amount in PHP
CKE	2019 - 2020	5	DEPOSIT - CASH	544,720
	2020	22	ATM WITHDRAWALS	420,000
	2016	1	ATM WITHDRAWALS	19,540
OSA	2019	1	ATM WITHDRAWALS	6,020
	2021	1	INTER-ACCOUNT TRANSFERS (SAME BANK)	235,300
MDA	2021	1	DEPOSIT - CASH	390,000
	2019	3	STR TRANSACTIONS	0
	2015	1	UNKNOWN	1,043,128
MLM; MDA	2019	1	STR TRANSACTIONS	0
TOTAL		36		2,658,708

Another identified student, Mr. OSA, a walk-in client of Bank C of Bacoor branch was the subject of an STR on the grounds that the amount of funds involved is not commensurate with the business or financial capacity of the client. Mr. OSA declared that he is a student at University S and has a business named H Enterprise which is engaged in the selling of electronic parts gadgets and other electronic products in an e-commerce platform.[66] Apparently, Mr. OSA declared that monthly credits from online shopping business is about PHP25,000, yet records show average credits reaching PHP0.1 million. Moreover, Mr. OSA had transactions with an individual who was the subject of an STR – MDA.

Mr. MDA, a likely relative of Mr. OSA (similar last names), figured in a 2015 STR filed by Bank ABC, Bacoor branch due to a recall request on an alleged fraudulent remittance, amounting to USD23,644.1, which was reported by the scammed sender. The client failed to present supporting documents to justify the remittance from a financial services company based abroad. The USD savings account of Mr. MDA was opened with initial deposit of USD542. Based on the client's initial KYC submission, subject is a manager for PMGA Business, while upon KYC updating, client declared that he has a business under the name CED. Open-source search on CED revealed a closely corresponding name to a business located in Cavite which, however, failed to appear via business name search on the DTI website.

Further, Mr. MDA was again the subject of an STR due to his linkage to a certain Mrs. PB, recipient of a fraudulent payment. Mr. MDA served as the referrer of the latter's account. The EDD conducted revealed additional details such as: 1) subject is a permanent resident of the country having married a presumed Filipino wife; 2) wife is working at a pharmaceuticals company earning PHP0.1 million; 3) according to the client, he can earn PHP0.5 million a day from his money exchange and remittance business, as well as a consultancy firm; 4) purported other businesses of the subject are GT, UW outlet, and PPL that was converted to a travel agency. Mr. MDA, however, failed to provide supporting documents for the businesses he claims to own. Aside from this, there were inconsistencies with his submitted financial income statement as well as certificate of employment. The CP deemed that Mr. MDA's transactions are not commensurate with his business or financial capacity.

[65] Figures in actual total due to disparity in values if translated to PHP millions

[66] E-commerce platform search for online sellers proved nil for the name of this business entity.

c. **City of Las Piñas: University X.** Filed suspicious reports on subject individuals who declared University X as place of education totaled 377, valued at PHP15 million.

Table 16: STRs of Individuals from University X, Las Piñas[67]

Subject Names	Transaction Dates	Total STRs	Transaction Types	Total Amount in PHP
RGN	2019-2020	60	DEPOSIT - CASH	3,196,461
	2019-2020	17	INTER-ACCOUNT TRANSFERS (SAME BANK)	147,705
	2019-2020	15	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	217,480
	2019-2020	4	OUTWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	96,850
	2019-2020	184	WITHDRAWALS - ATM	4,089,700
	2019-2020	1	WITHDRAWALS - OTC	12,857
OKS	2019	1	ELECTRONIC CASH CARD - WITHDRAWAL	50
JM	2019	1	ELECTRONIC CASH CARD - WITHDRAWAL	10,020
SOO	2019	1	INTER-ACCOUNT TRANSFERS (SAME BANK)	19,720
FMI	2019	6	INWARD REMITTANCE (DOMESTIC) - CREDIT TO BENEFICIARY'S ACCOUNT	600,000
	2020	4	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	200,000
	2020	11	DEPOSIT - CASH	992,400
MG	2018; 2020	15	DEPOSIT - CASH	2,782,020
	2018-2019	2	ELECTRONIC CASH CARD - WITHDRAWAL	1,749
	2017;2020	5	INTER-ACCOUNT TRANSFERS (SAME BANK)	76,850
	2020	22	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	553,219
JTA	2020	26	DEPOSIT - CASH	1,587,100
	2020	15	INWARD REMITTANCE (DOMESTIC) CREDIT TO BENEFICIARY ACCOUNT VIA ELECTRONIC BANKING	241,957
SM	2019	6	DEPOSIT - CASH	200,200
TOTAL		**396**		**15,026,338**

It should be noted that three (3) other individuals linked to University X were not included in the list since subjects were already discussed in other parts of the paper, namely Mr. PMA and Mr. STE (Case No. 3: Love Scam), and Mr. AFO (Case 2: Swindling/OBC Corporation).

Mr. RGN figured in 281 STRs with estimated value of PHP7.8 million, which largely relates to ATM withdrawals and cash deposits. The subject is reportedly a student with declared monthly remittance of PHP0.3 million. Subject's account generated an alert due to high frequency of activities, while its end of day balance amounts to PHP50,000. Also, the subject's transactions varied with the nature of the client's declared source of funds. Upon bank verification, the client claimed that the transactions are remittances from his parents for school allowances and personal expenses. He further claimed that some credits were from relatives of his friends that reside here in the Philippines for their expenses. Mr. RGN, however, failed to provide supporting documents to substantiate his claims.

While Mr. RGN is purportedly enrolled in University X, Laguna, his addresses, based on the transactions from 2019 to 2020, were in Las Piñas and Laguna. Majority of the STRs were submitted by Bank O and Bank P, both located in Las Piñas. Also, for Bank P, Mr. RGN's justification for the fund

[67] Figures in actual total due to disparity in values if translated to PHP Millions.

transfers to his account were support from his cousins – KCI, DCT, and IA. Said cousins all have Bank O accounts with declared addresses in Angeles City, Pampanga, Silang, Cavite, and Batangas City.[68] Three (3) individuals were beneficiaries of Mr. RGN with addresses in Quezon City, Benguet, and Manila, respectively.

Mr. FMI was reported by three (3) banks located in Las Piñas since the transfers/remittances are not commensurate with the declared source of funds (remittances from parents in Nigeria). Generated alert from the AML system of Bank ABC was categorized under single beneficiary with multiple remitter/remittance scenario. Upon verification with the client, remittances are intended for MG, which according to Mr. FMI is not known to him personally. The client failed to provide proof for the bank transactions.

In connection with the above, Mr. MG was profiled as a Maritime Transportation student from University X, Las Piñas based on customer confirmation record of Bank ABC in Las Piñas. Apparently, the bank noted 14 transactions, amounting to PHP2.8 million, which upon the review of the account in 2018, was found to have no underlying purpose and deviates from the profile of Mr. MG. The client further claimed that he acted as middleman for other Nigerian students whose parents used his account to deposit funds to pay for tuition fees and other expenses. The client, however, failed to provide supporting documents for his claim. Moreover, customer had a reported transaction with a certain SLA[69] who is involved with ADS (Case 5 of this study). Two (2) other beneficiaries, Mr. JTA and Mr. SM, were beneficiaries of transfers from Mr. MG which are also subjects of STRs captured in the dataset. Mr. JTA received multiple domestic transfers from local banks which deviated from the client's source of funds. Mr. SM's account, on the one hand, was flagged for five (5) cash-ins within 24 hours that reached the PHP0.5 million cumulative volume on 3 May 2019. Further, the bank disclosed that the account received a total of PHP0.3 million via LM on 15 June 2019, which were converted to bitcoin and subsequently sent to an e-mail address.[70] Apparently, the bitcoin user was placed under internal watchlist due to a suspicion that the account was used as a vehicle for pooled investment. Further review revealed that the user is a student and that the declared allowance as source of income is inconsistent with the amounts received.

V. Conclusion and Recommendation

The notable rise in reported Nigerian-related crimes in the country should evidently be given attention. Aside from the significant amount, this study revealed that these unlawful transactions had been in existence in the country since 2009 and has proliferated up to the present.

In terms of international transactions, majority of the inflows came from the USA, whereas outflows were transmitted primarily to beneficiaries with addresses in Nigeria. The NCR, meanwhile, dominated the total number and value of STRs, specifically Quezon City in terms of value and Las Piñas City by count.

The pandemic served as precursor to signal the convenience and importance of digitizing the mode of transactions. What is glaring is that the increased use of online services during the pandemic also intensified the risks of cybercrimes. For this study, while banks ranked first as the preferred method for transferring funds, the year 2021 yielded higher reporting volume of EMIs, suggesting the increased use of this financial channel as it provides anonymity to the perpetrators. In addition,

[68] Filed report stated that identified deposits/transfers from these cousins were withdrawn from various ATMs on the same day and/or the next.
[69] The STR disclosed that Mr. SLA's account is subject of a freeze order in relation to the account of Mr. MG.
[70] Relationship of Mr. SM with the user of subject e-mail address has yet to be established.

there are some banks and non-bank financial institutions (including branches) that do not have complete addresses and/or the submitted STR details on the name fields of the subject, account holder or other person, including addresses of the various name flags, are incomplete. Hence, there is a need to reiterate that CPS should observe proper know-your-customer and customer due diligence procedures. Noting the lag in reporting of certain unusual activities from the date of actual transactions, banks and other financial institutions are also encouraged to be more vigilant in tracking and immediately reporting suspicious transactions and accounts especially those with unverifiable identification documents.

Using specific keywords in the narratives, the top five illegal activities identified in this study in order of value are Others - Unsubstantiated Transaction valued at PHP1,499.6 million (46.0%) of the aggregate, followed by advanced fee fraud at PHP1,086.4 million (33.3%), unauthorized transactions from mostly compromised accounts at PHP308.6 million (9.5%), pass through/money mules at PHP101.3 million (3.1%), and package scam at PHP57.3 million (1.8%). Moreover, the vulnerabilities of cryptocurrency to money laundering may be focused on as crypto-related transactions, using the keywords "crypto," "binance," "bitcoin," and "external wallet" for this study generated 1,503 STRs with the corresponding value of PHP132.7 million.

The study further identified some significant typologies and red flags which include, but are not limited, to inconsistent transactional activities with the subject's business profile; package, romance, lottery scams with pass-through accounts; deposits from unverified sources; involvement in illegal drugs as well as African drug syndicates; association with bank hacking incidents; and recruitment of money mules. While these types of crimes have been brought to the attention of the country's law enforcement agencies, the continued proliferation of Nigerian-related crimes call for more stringent monitoring of subjects identified in the STRs.

The study recommends the following: 1) encouragement of CPs to submit STRs on the Nigerian subjects and their cohorts; 2) involvement of the Asset Management Group of the AMLC to trace the assets of these scammers and forfeit the same in favor of the government agency both domestic and foreign, as well as such other claimants, as designated by the law, with the ultimate objective of depriving these criminals of the proceeds of their crimes; and 3) communication of the results of the study to various stakeholders such as internal AMLC groups/divisions, appropriate LEAs, SAs, private sector participants of the AMLC's PPPP, and respective FIUs of other jurisdictions with transactional links to the country as identified in the study. A redacted version is also recommended to be posted on the AMLC website.

REFERENCES:

Anti-Money Laundering Council. ***An Analysis of Suspicious Transaction Reports with Possible Links to Tax Crimes.*** 2021. Anti-Money Laundering Council website. Retrieved from http://www.amlc.gov.ph/images/PDFs/2021%20ANALYSIS%20OF%20STRS%20WITH%20POSSIBLE%20LINKS%20TO%20TAX%20CRIMES.pdf (accessed on 27 April 2022).

Bergonia, T. ***Lockdowns in PH: A brief history.*** (03 August 2021). Inquirer.net. Retrieved from https://newsinfo.inquirer.net/1468403/lockdowns-in-ph-a-brief-history (accessed on 21 April 2022).

Bureau of Immigration. ***Annual Report Guidelines 2022***. Retrieved from https://immigration.gov.ph/images/AnnualReport/AnnualReportGuidelines2022.pdf (accessed 11 August 2022).

Bureau of Immigration. ***The Bureau Functions***. Bureau of Immigration. Retrieved from https://immigration.gov.ph/the-bureau/functions (accessed on 11 August 2022).

Chowdry, M. ***Top Ten Scamming Countries in the World in 2021***. (24 June 2021). Retrieved from https://www.analyticsinsight.net/top-10-scamming-countries-in-the-world-in-2021/ (accessed 19 April 2022).

Cudis, C. ***Public warned of increasing financial cybercrimes amid pandemic***. (17 March 2021). Philippine News Agency. Retrieved from https://www.pna.gov.ph/articles/1133961 (accessed on 27 April 2022).

Dalison, A. (10 January 2022). ***PNP cybercops gain headway in anti-cybercrime drive in 2021.*** Journal News Online. Retrieved from https://journalnews.com.ph/pnp-cybercops-gain-headway-in-anti-cybercrime-drive-in-2021/, (accessed 13 Jan 2022).

DataReportal***. Digital 2022: Global Digital Overview.*** 2022. DataReportal website. Retrieved from https://datareportal.com/reports/digital-2022-philippines (accessed 17 April 2022).

Department of Foreign Affairs**.** ***Visa Guidelines / Requirements*****.** Retrieved from https://dfa.gov.ph/guidelines-requirements (accessed on 11 August 2022).

Digital 2022: The Philippines. 2022. DataReportal. Retrieved from https://datareportal.com/reports/digital-2022-philippines (accessed 17 April 2022).

External Wallets definition n.d. Law Insider. Retrieved from https://www.lawinsider.com/dictionary/external-wallets (accessed on 3 June 2022).

Federal Bureau of Investigation. ***Internet Crime Report 2021.*** n.d. Internet Crime Complaint Center, Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed 25 April 2022).

Frankerfield, J. ***Bitcoin (BTC)***. (12 May 2022). Investopedia. Retrieved from https://www.investopedia.com/terms/b/bitcoin.asp (accessed on 3 June 2022).

Lena, P. ***NBI warns of 'love scam' via internet.*** (20 July 2018). Philippine News Agency. Retrieved from https://www.pna.gov.ph/articles/1042140 (accessed 13 Jan 2022).

Migration Profile: Nigeria. n.d. Migrants & Refugees. Retrieved from https://migrants-refugees.va/it/wp-content/uploads/sites/3/2021/05/2020-CP-Nigeria.pdf (accessed 20 April 2022).

Panaligan, R. ***Cyber-related crimes on the rise during pandemic — DOJ***. (12 July 2020). Manila Bulletin online. Retrieved from https://mb.com.ph/2020/07/12/cyber-related-crimes-on-the-rise-during-pandemic-doj/, (accessed on 25 April 2022).

Patino, F. ***BOC warns public against online love scam.*** (21 October 2017). Philippine News Agency. Retrieved from https://www.pna.gov.ph/articles/1013468, (accessed 13 Jan 2022).

Peters, K. ***Binance Exchange***. (08 July 2021). Investopedia. Retrieved from https://www.investopedia.com/terms/b/binance-exchange.asp (accessed on 3 June 2022).

Philippine National Police Anti-Cybercrime Group (ACG). ***Common Types of Internet Fraud Scams.*** n.d. PNP-ACG Website. Retrieved from https://pnpacg.ph/main/accomplishments/2-uncategorised/172-common-types-of-internet-fraud-scams (accessed 10 Jan 2022).

Philippine National Police. ***PNP Reported Cybercrime Statistics.*** n.d.Retrieved from https://cybercrimewatch.pnp.gov.ph/, (accessed 13 Jan 2022).

PNP cautions public vs. online 'love scam'. Sun Star Pampanga. Retrieved from https://www.pressreader.com/philippines/sunstar-pampanga/20211102/281646783360885, (accessed 13 Jan 2022).

Visitor Arrivals to the Philippines. n.d. Department of Tourism. Retrieved from http://tourism.gov.ph/tourism_dem_sup_pub.aspx, (accessed 12 April 2022).

What is Cryptocurrency: Your Complete Crypto ABC. n.d. (21 November 2022). Bitdegree.org. Retrieved from https://www.bitdegree.org/crypto/tutorials/what-is-cryptocurrency#how-does-cryptocurrency-work (accessed on 3 June 2022).

Why Nigerians are emigrating. n.d. The Sun Nigeria. Retrieved from https://www.sunnewsonline.com/why-nigerians-are-emigrating/ (accessed 17 April 2022).