

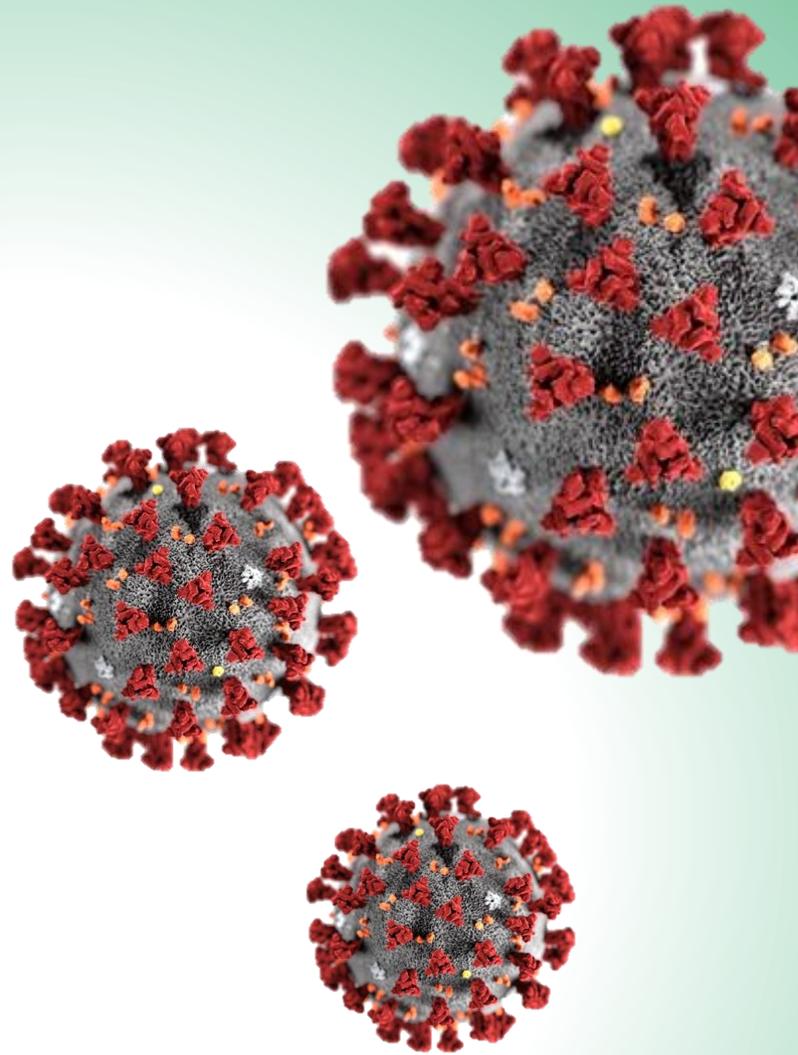


**COVID-19**

# Financial Crime Trend Analysis

# Typologies Brief

Series 2 (October 2020)





COVID-19 Typologies Brief Series 2 is a follow-up to the earlier COVID-19 Brief (July 2020) presented on 21 July 2020 in the Central Banking amidst COVID-19 Webinar Series (Combating Money Laundering during the Pandemic) jointly hosted by the Bangko Sentral ng Pilipinas (BSP) Institute and the International Monetary Fund (IMF) Singapore Regional Training Institute (IMF-STI). A redacted version of said brief was also published in the AMLC website in August 2020.

Series 2 extends the data coverage to 31 August 2020 with comparative year-on-year trends for the months of March to May 2020 (i.e., during the months of the Luzon-wide Enhanced Community Quarantine (ECQ)<sup>1</sup> and Modified ECQ (MECQ)<sup>2</sup>), and the first eight (8) months of the year.

## I. Data coverage and observed trends

Series 2 covers transactions between 1 January and 31 August 2020, which are related or suspected to be related to unlawful activities. The top reasons for filing suspicious transactions are skimming, phishing, unauthorized access, and other similar violations of the Electronic Commerce Act of 2000 with a total estimated value of PHP2.7 billion.

Online sexual exploitation of children (OSEC) and related crimes are also top reasons for STR filing, during the first eight (8) months of 2020, with an estimated value of PHP84.5 million. A major contributor were filings by pawnshops and money service businesses (MSBs). Moreover, it was noted that there were filings in relation to clients' violations of the covered person's (CP) internal policies, such as referral abuse and misuse of incentives. Many account holders have taken advantage of the waived convenience fees in online fund transfers through Instapay and PESONet; and promotional campaigns that encourage cashless transactions. These have triggered the alert systems of some CPs due to unusual transaction behaviors and/or violations of the companies' terms and conditions. Aside from the breach of internal company policies, there are also clients who use their personal accounts to cater to the needs of their immediate community as payment gateways and retail lending services, which are normally accorded by MSBs.

It was also observed that suspicious filings by electronic money issuers (EMIs) surged during the first eight (8) months of 2020 compared to the same periods last year. The filings are related to electronic banking and to purchases using electronic cash cards, unauthorized account access, skimming, and other violations of the Electronic Commerce Act of 2000. This may indicate an increasing trend in the use of the online and e-money space in perpetuating money laundering methods.

## II. Notable typologies and red flags

### 1. *Fraudsters pretending to be affiliated with government units in soliciting COVID-19 donations from victims*

#### Office of the Governor, Laoag City

A certain account, opened on 27 May 2020 under the name of an alleged fraudster, is purportedly being used to solicit donations or funds for COVID-19 relief efforts, using the name of the current governor of Laoag City. The solicited funds were deposited in the bank account of the fraudster. A review of the transactions showed that large cash deposits, totaling PHP622,000, were made into the account. Further, all large deposits were withdrawn on the same day. The alleged fraudster also made frequent balance inquiries in a day. Documents also showed that the alleged fraudster is a TNVS<sup>3</sup> driver with a gross monthly income between PHP20,000 and PHP50,000, which is the only source of funds declared during the onboarding process. An open-source

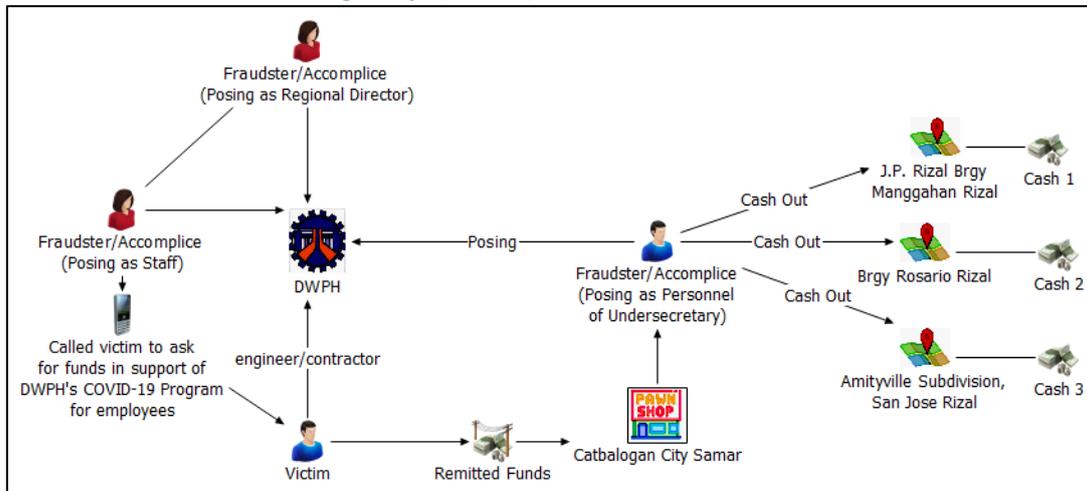
<sup>1</sup> Pursuant to Malacañan Palace's Proclamation No. 929, Declaring a State of Calamity Throughout the Philippines Due to the Corona Virus Diseases 2019 (<https://www.officialgazette.gov.ph/downloads/2020/03mar/20200316-PROC-929-RRD.pdf> accessed 27 May 2020)

<sup>2</sup> Pursuant to Inter-Agency Task Force for the Management of Emerging Infectious Diseases Resolution No.37 Series of 2020 (<https://www.officialgazette.gov.ph/downloads/2020/05may/20200515-IATF-RESOLUTION-NO-37.pdf> accessed on 20 October 2020)

<sup>3</sup> Transport Network Vehicle Service or TNVS is the term used to describe a Public Utility Vehicle accredited with a Transport Network Corporation (TNC), which is granted authority or franchise by the LTRFB to run a public transport service. A TNC is an organization that provides pre-arranged transportation services for compensation using an internet-based technology application or digital platform technology to connect passengers with drivers using their personal vehicle. Example of TNC are Grab Philippines and Angkas. Accessed from <https://ltfrb.gov.ph/wp-content/uploads/2020/06/DO-2017-011-1.pdf> on 8 October 2020.

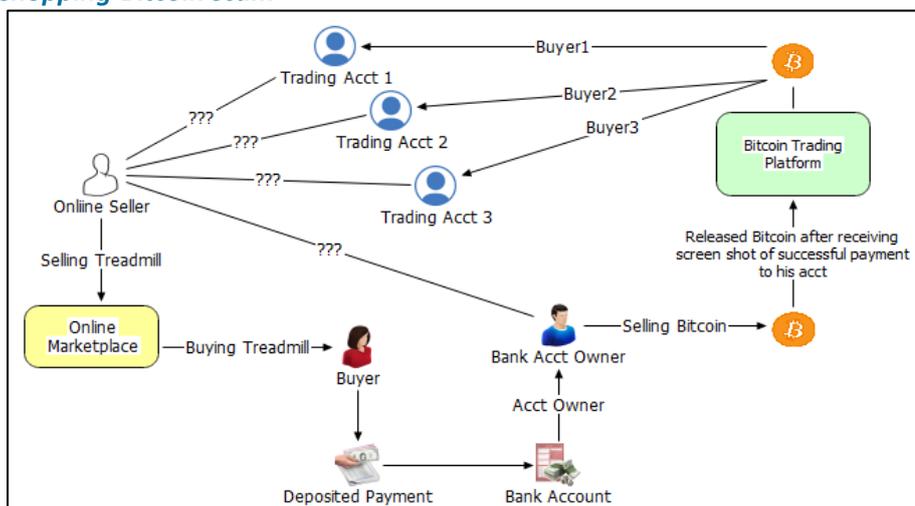
search yielded a social media post of another government agency, regarding an advisory against a similarly named individual (i.e., the alleged fraudster), who was using the name of the agency's executive director to solicit donations supposedly for the Taal Volcano eruption victims and that the donations were being deposited to another bank account of the fraudster.

### Department of Public Works and Highways (DPWH)



Allegedly, the perpetrators are two females and one male, posing as employees of DPWH, while the victim is an engineer/contractor in a regional office of DPWH. On 20 April 2020, the victim received a call from a female, who introduced herself as part of the staff of one of DPWH's regional offices. After telling the victim that the DWPH regional director (DRD) wanted to speak with the victim, the caller passed the phone to another woman, who pretended to be the DRD. The fake DRD informed the victim that the DPWH undersecretary was planning to give subsidies or relief packs to their employees relative to the COVID-19 pandemic. To augment this plan, the victim was told to raise funds, amounting to Php150,000, and to deposit the money directly in the undersecretary's bank account in Manila. Due to time constraints, the victim was advised to send the funds through an MSB instead of a bank. The fake DRD provided the name and the mobile number of the recipient of the funds—a male accomplice, who was introduced as the undersecretary's personnel. The victim sent Php150,000 through the MSB branch in Catbalogan City, Samar and texted the fake male personnel that the money was available for pickup. The victim then received text notifications that the remittances were claimed by the recipient in several branches in the province of Rizal.

### 2. Online shopping-Bitcoin scam





A buyer bought a treadmill from an online marketplace, and the online seller instructed the buyer to deposit the payment in a certain bank account. On 1 June 2020, the buyer made five (5) fund transfers, totaling PhP22,000, but the ordered item was never delivered. The beneficiary bank account owner (Mr. BBAC) denied any relation to the online scammer/seller, emphasizing that he has never sold gadgets/equipment. Mr. BBAC mentioned that at the start of the COVID-19 crisis, he started engaging in Bitcoin trading in a legitimate online peer-to-peer finance platform, where individuals are registered under a username or alias. On 31 May 2020, Mr. BBAC traded Bitcoins with three (3) users. Upon receipt of screenshots of successful payment transfers to his bank account, Mr. BBAC released the Bitcoins to the traders not knowing that the transferred funds were from the buyer. Mr. BBAC submitted all supporting documents, including screenshots from the trades. Details of the ultimate beneficiary/suspect remain unknown.

### **3. Possible fraud – NPO to receive COVID-19 funds from suspected shell company**

A non-profit organization (NPO) opened an account on 15 July 2020 for the purpose of accepting donations. The NPO stated that the account will also be used for operating expenses and funds relating to charitable works. Per the NPO's website, its advocacy is to conduct Bible studies. Aside from account-opening, the NPO also inquired about the documentary requirements if it is expecting to receive a donation of EUR10 million from a company in Hong Kong. The NPO submitted a memorandum of agreement whereby it was stated that the Hong Kong company will be partnering with the NPO in a worldwide corporate social responsibility program on the prevention of the COVID-19 pandemic and improvement of the quality of life and overall health situation in the Philippines, among others. While no actual credit has been made, it was noted that the documents provided were insufficient to support the large amount of funds expected to be received.

### **4. Continuous financial transactions despite business affected by lockdown**

#### **Fish trading**

A female client declared her fishing business as source of funds. Her account was noted to have 170 transactions from 15 November 2019 to 26 May 2020, ranging from PhP50 to PhP1,000,000 with a total value of PhP41 million. The client claimed that the transactions were related to the purchase of fingerlings as her business is fish trading. As noted by the bank, however, the transactions were mostly made during the ECQ, when all commercial flights and sea travel were prohibited. Moreover, the client was unable to present any document to support her claim.

#### **Food court and restaurant**

A corporate client is into the food court and restaurant business, and it was observed that between 21 January and 24 June 2020, there were 90 cash deposits into the client's account, ranging from PhP183,103 to PhP5,411,042, with a total value of PhP140 million. The bank requested documents to support the substantial cash transactions. The client presented cash transmittal slips, but the branch confirmed that these were not enough to support the cash deposits. The bank also observed that the transactions were mostly made during the ECQ, when most restaurants were not allowed to operate.

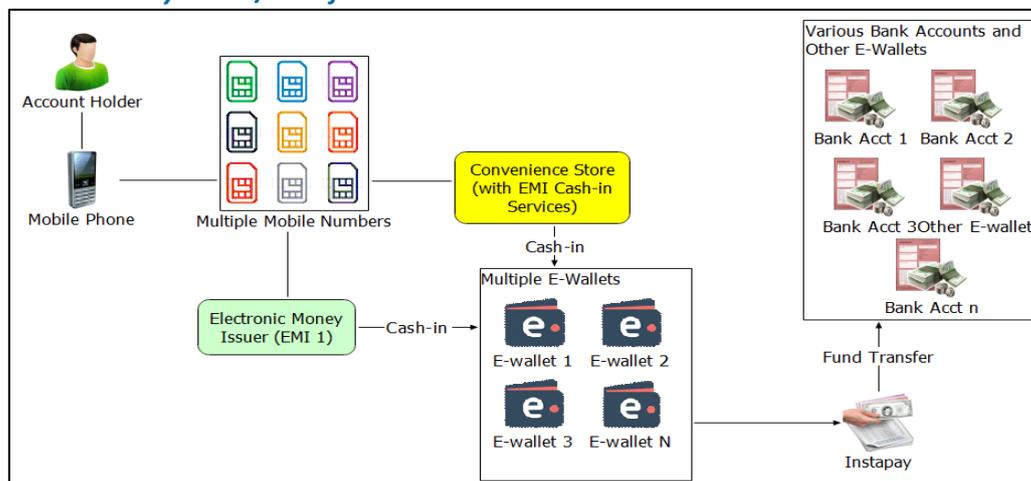
### **5. Receipt of deposit/fund transfer with no underlying legal transaction involving Bitcoin**

The subject opened a passbook with ATM access account in a bank in Biñan, Laguna on 9 January 2020. Purposes of the account are for personal savings and business transactions. Based on the accomplished customer information sheet, the subject earns a monthly income of PhP70,000 as business owner of general merchandise. During account-opening, the subject submitted copies of his driver's license and Department of Trade and Industry (DTI) registration for his business. The subject was assessed as normal risk. The bank's monitoring system, however, triggered an alert due to an inward remittance from a single sender, amounting to PhP55,400 on 12 March 2020. As part of the know-your-customer (KYC) and further due diligence process, the bank exerted effort to contact the subject to verify and to request supporting documents for the alerted transaction. The subject was contacted on 13 May 2020, and he disclosed that the transaction was payment from a customer, who ordered 5,000 pieces of facemasks. Upon checking, said inward remittance was from a verified Bitcoin company. The subject was advised to visit the branch to provide supporting documents, but the client failed to do so, due to the ECQ. The branch asked the subject to e-mail a copy of the voucher and



delivery receipt or any proof of the transaction. The subject submitted a delivery receipt and a voucher, but the documents were deemed unacceptable as they appeared self-serving. The bank also requested the subject to provide a copy of the delivery/courier receipt and screenshots of conversations, regarding the transaction as the subject claimed that the transaction was done through online selling. The bank called the subject almost every day from 13 to 27 May 2020 to follow up the documents but to no avail. The subject is now rejecting the calls, and funds from the subject's account have gone below the maintaining balance.

## 6. Suspected e-money mules/smurfers



From 1 March to 30 May 2020, an EMI reported 2,933 STRs related to suspected money mules or smurfers. These transactions have an estimated value of Php18.89 million transacted in less than four (4) months. Individuals, usually with the same mobile phone, use different mobile numbers to create multiple e-wallet accounts. Once the e-wallet is created, individuals would cash in via convenience stores on separate dates with only a few days apart. Another cash-in method is through another EMI, which is different from the EMI that issued the e-wallet. On the same day of credit to the e-wallets, the funds were subsequently transferred to several bank accounts and/or other e-wallets through Instapay. Transactions were also geographically concentrated in areas in Davao del Sur, Davao del Norte, Pangasinan, Ilocos Norte, Tarlac, Negros Occidental, Siquijor, Laguna, Zamboanga, Quezon City, and Manila. Most account holders' declared occupation was student, while one (1) was an employee of a convenience store.

## 7. Large transactions purportedly received from government units as payment for COVID-19-related products and services

### Food packs

The subject is an owner of a construction and general merchandising business. On 30 July 2020, the subject's personal account received a fund transfer from a third-party account in the amount of Php53 million. According to the subject, this amount is inclusive of the Php21.8 million, which the third-party claimed to be payment received from the Tagaytay City Government for food packs related to the sixth (6th) wave of the COVID-19 ECQ assistance. It was further narrated that the entire Php53 million will be used to finance an alleged joint venture of the subject and a third-party for a real property acquisition.

### Hotel coordination on behalf of Overseas Workers Welfare Administration (OWWA)

The subject opened three (3) bank accounts between August 2019 and June 2020 in different branches with declared source of funds as income from his real estate leasing business. Further, one of the accounts is a joint account with his wife. On 11 June and 10 July 2020, three (3) cash deposits were posted to the three (3) different accounts of the subject with total amounts of Php1.2 million and Php1.05 million, respectively. Per inquiry of the bank, the subject said that they were coordinators for OWWA and partner hotels, where Overseas Filipino Workers (OFW) were being booked for quarantine. The subject further added that they also coordinate with the caterers and disinfection service providers. The subject disclosed that they have no



signed contract with the OWWA and that the funds deposited were payment of the hotels, which would then be used to pay the service providers. Red flags include: (1) the inability to provide acceptable supporting documents for the transactions with OWWA; (2) the nature of the transaction that deviates from the declared source of funds during account-opening, and (3) the amount of transactions that appear to be structured.

#### **8. Large cash deposit allegedly for COVID-19 donations for Marawi residents**

The subject opened a savings account in Iligan City on 25 November 2019 to serve as a settlement account for her insurance account. Per declaration, the subject owns a jewelry shop, but the gross monthly income was not recorded in the system. The subject is the sibling of another bank client, whose account was also opened on 25 November 2019 and who was reported for suspicious transactions due to unconsummated and attempted significant cash deposits from unknown sources. On 7 May 2020, a certain blacklisted individual attempted to deposit PhP4.5 million into the subject's account. Moreover, the blacklisted individual has had transactions in the account of the subject's sibling. The blacklisted individual claimed that the bulk money were donations accumulated due to the ECQ and was intended for the people of Marawi City. The branch, however, denied the deposit due to the lack of supporting documents. A financial review of the subject's account from 25 November 2019 to 22 May 2020 shows 14 cash deposits, ranging from PhP2,000 to PhP246,000, totaling PhP1,473,000. These deposits were declared to be cash assistance from the subject's relatives for living expenses. Funds withdrawn via ATM totaled PhP471,000, and online payments and purchases via EPS<sup>4</sup> totaled PhP195,665. The subject's current account balance is PhP406,782.68.

#### **9. Incentive abuser performing similar MSB functions**

Based on confidential information, the subject is an agent for an EMI. The subject was actively transferring funds from her agent wallet to fund other partner agents outside of her network. Transactions ranged from PhP20,000 to PhP263,000 for the month of April 2020. When the EMI verified the transactions, the subject said that she found a loophole in the system and decided to take the opportunity to continuously fund in other partner agents. The subject was well-informed that agents were not allowed to fund in partner agents outside of their network, but the subject had deviated due to the 1% commission, considering the ECQ imposed in Metro Manila. The subject was then warned not to take advantage of the same scheme. The management of the EMI decided to revoke the commission gained by the subject, and the account wallet was deactivated effective 30 May 2020.

#### **10. Personal account acting as unlicensed MSB**

Suspicious transactions were filed against the subject due to two (2) system alerts on the account. The first alert was due to five cash-outs made within 24 hours on 7 April 2020. The second alert was flagged on 18 May 2020 due to the PhP500,000 cumulative volume of transactions on the account. Upon inspection of the said account, it was noticed that on 3 April 2020, the subject cashed out to various individuals via different EMIs, totaling PhP10,445. The subject cashed in a total of PhP210,000 as of 4 August 2020. A review of the profile showed that the subject is a supervisor in a graphics company. When the subject was interviewed last 17 June 2020, the subject explained that the purpose of creating the account was to have a small prepaid mobile loading and bills payment business during the community quarantine because her company has stopped its operations and she was no longer receiving salary. Moreover, she added that the cash-outs were for her neighbors' social amelioration program (SAP) funds.

#### **11. Unsubstantiated deposits based on declared business and source of funds**

##### **From ready-to-wear (RTW) to lending**

On 18 January 2019, the subject opened a savings account in Pampanga. The subject's declared source of funds was from an RTW business. On 29 April 2020, a representative made a deposit of PhP499,000 to the subject's account at the Juan Luna Branch in Cebu City and another deposit on 14 May 2020 for PhP500,000. The branch called the subject to verify the source of funds. Based on the interview, the subject disclosed that

---

<sup>4</sup> Express Payment System (EPS)



during the ECQ, the subject engaged in a small lending business, which involved mostly cash and unsecured transactions, since most of the malls were not open. She advised the branch that she will forward a copy of her DTI renewal certificate and other records to support the significant deposits. On 29 May 2020, her account was tagged as high risk due to the change in her nature of business and source of funds. Since then, the branch has been unable to contact the client, and after several attempts, the client has yet to provide enough documents to justify the source of funds.

#### **From seafood trading to second-hand car trading**

The subject opened a current account on 30 June 2020 with an initial deposit of PhP25,000 and declared the source of funds as income from a seafood trading business. Due to the pandemic, however, the subject shifted to a freelance agent of second-hand cars. Per result of transactional review covering 1 July to 13 August 2020, notable transactions on the account include: (1) 47 cash deposits ranging from PhP500 to PhP1.37 million, totaling PhP9 million; (2) 130 Instapay remittances, totaling PhP2.47 million; and (3) 11 local check deposits, totaling PhP1.9 million. Per the subject, said deposits and remittances were payments from selling second-hand cars. Subsequently, the subject made check issuances, totaling PhP11 million, payable to a certain company that allegedly owns the second-hand cars. The bank requested the subject to provide deed/s of sale or other proof of transaction, but the subject claimed that he was just a middleman/freelance agent of said transactions and cannot provide any documents. Per open source, said company, who allegedly owns second-hand cars, was selling/leasing disinfection stations.

#### **Politically exposed person engaging in second-hand car trading**

The subject opened a premium checking account on 15 February 2010 with an initial deposit of PhP400,000 and declared salary as a municipal mayor of a northern province as source of funds. It has been noted that during the transactional review covering April to June 2020, the subject had total deposits of PhP4.36 million in cash and PhP3.4 million in checks. Subsequently, these amounts were used to issue checks payable to a certain third-party. Per the bank's telephone conversation with the subject, the deposits were from his buying and selling of used cars and sub-construction business. The subject, however, stated that both businesses have no business documents. Further, the subject allegedly referred to the third-party as business partner. The subject presented copies of deeds of absolute sale for the two vehicles he recently purchased.

### **III. Conclusions and recommendations**

From the initial COVID-19 Brief, aside from the timing of filing and/or transaction, the causal relationship of suspicious report filings and the pandemic cannot be established. Moreover, the AMLC recommended the use of keywords in the narrative when filing STRs for better triaging. In the initial brief, only 185 suspicious reports, mainly attributed to returned checks due to businesses closed by the lockdown, can directly be associated with the pandemic. As more suspicious reports covering the periods of the pandemic, however, were analyzed, typologies related to the pandemic have emerged. Case narratives are explicitly citing COVID-19-related schemes and red flags, such as sending/receiving large funds allegedly for pandemic relief efforts, and continuous receipt of cash transactions, despite business closures due to the lockdown.

Moreover, some CPs have started including identifiable keywords in the narrative. Aside from the use of keywords, PPPP<sup>5</sup> recipients of the initial COVID-19 Brief have also started filing STRs on persons of interest (POIs) identified in the study. As of 31 August 2020, 2,271 suspicious reports have directly mentioned COVID-19 related keywords in the narratives. It should be noted, however, that the trends and typologies discussed in this study are only based on STRs filed by CPs to AMLC. As CPs become more cognizant of these red flags and unusual transaction behaviors coupled with the adjustments in their transaction monitoring tools, the AMLC expects that suspicious filings related to the pandemic will further increase. As more suspicious transactions are reported by CPs, observed trends in the current study may possibly change.

---

<sup>5</sup> AMLC's Public-Private Partnership Program



The vulnerabilities of e-money to smurfing schemes, using money mules and pass-through accounts, are becoming more apparent as two EMLs (the first typology was cited in the initial COVID-19 Brief, while the second typology was discussed in this brief) have reported suspicious transactions exhibiting these schemes. Moreover, this study reiterates the earlier recommendation of the initial COVID-19 Brief that all CPs should be cautious as money launders and perpetrators could be abusing the digitization, such as digital KYC/CDD, which many CPs have adopted during the pandemic. Depository institutions should ensure that proper KYC/CDD is observed and should periodically assess clients' risk rating in view of unusual and suspicious financial transactions. Further, EMLs, MSBs, and other online fund transfer service providers are advised to be vigilant as data showed growth in suspicious and unlawful transactions related to online activities.

The updated study uncovered some notable red flags, which include but are not limited to the following:

1. Large incoming or outgoing transactions for the purpose of COVID-19 relief efforts or other humanitarian causes, which are not strongly supported by valid documentation and proof;
2. Unsubstantiated deposits or fund transfers as alleged payment for products and/or services rendered to government units relating to COVID-19 relief efforts;
3. Continuous or unusual transactions (i.e., cash deposits, cash withdrawals, check issuances, payments to suppliers, etc.) on the accounts maintained by businesses affected by the lockdown;
4. Receipt of large deposits allegedly caused by changes in the nature of employment and/or business vis-à-vis what was declared in the client account information, during on-boarding process, with the change in the nature of employment/business allegedly due to the pandemic;
5. Receipt of large deposits, allegedly for the sale of medical items or donations for COVID-19 relief efforts from unusual senders or channels such as virtual currency companies; and
6. Small-value, fast-moving funds to multiple account holders with immediate cash-outs that have no underlying justification.

