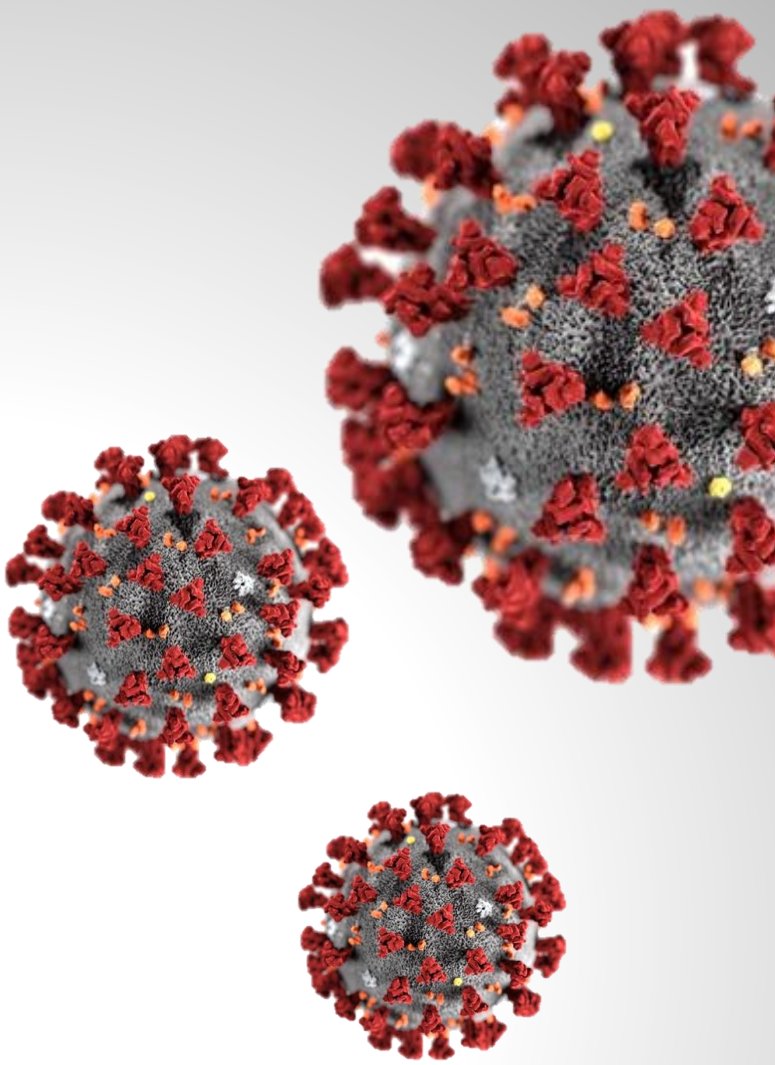
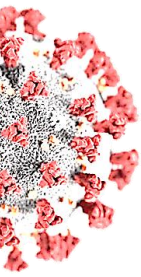
AMLC
Anti-Money Laundering Council



COVID-19
Financial Crime Trend Analysis
Typologies Brief

July 2020

secretariat@amlc.gov.ph



The Coronavirus Disease 2019 (COVID-19) pandemic is disrupting global economic activities and providing opportunities for offenders to exploit the fears of the general public and the loopholes in the financial system. Thus, the Anti-Money Laundering Council (AMLC) Secretariat is issuing a COVID-19 Financial Crime Trend Analysis to inform relevant stakeholders on pervasive and emerging money laundering and terrorism financing (ML/TF) threats posed by this global pandemic.

Discussions analyze the financial crime trends and typologies observed from various sources, primarily from suspicious transaction reports (STRs) approaching and during the months of the Luzon-wide Enhanced Community Quarantine (ECQ).[1] Requests for information received by the AMLC, local news reports/pronouncements, and related posts from various websites during the ECQ were also considered.

I. Data coverage and observed trends

The typologies brief covers transactions between 1 January 2020 and 24 April 2020[2] that are related or suspected to be related to unlawful activities. The top reasons for filing these transactions were likely fraud-related, such as possible money mule or pass-through accounts; and unauthorized transactions (i.e. phishing, card-skimming, and other violations of the Electronic Commerce Act of 2000), with a combined estimated value of PHP341 million.

Online sexual exploitation of children (Violations of the Anti-Child Pornography Act of 2009) is also one of the top reasons of STR filing, with an estimated value of PHP11.93 million. This observation is supported by various open-source warnings on the adverse effects of the pandemic on children's welfare. The Philippine Commission on Human Rights cited that "the lockdown situation due to the ECQ is making the already grim situation of child safety in the Internet worse. With the widening availability of Internet connection in the Philippines, and with the ECQ prompting children to spend more time online, sexual predators can find it easier to prey on children."[3]

The economic impact of the pandemic, reflected in the ECQ sample as returned checks due to insufficient funds and/or business closures because of the lockdown, accounts for 2% of the sample with an estimated value of PHP148 million.

Social media listening yielded many results on product scams, which may fall under swindling/estafa. The ECQ sample yields an estimated value of PHP6.2 million, mostly involving fake or bogus selling and overpricing of medical items, such as surgical masks, thermal scanners, and alcohol, among others.

II. Prevalent and notable typologies

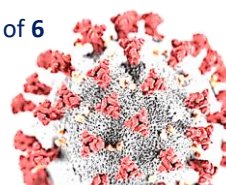
1. Possible bulk-cash smuggling, using cruise ships

One notable attempted transaction was reported due to a deviation from the client's usual activity. The client requested its bank to pick up bulk foreign currency cash from a cruise ship docked at a Philippine port via a deposit pick-up arrangement (DPA). The amount was intended to be deposited in its foreign currency account maintained in the local bank. This kind of transaction is usually done via telegraphic transfer from a bank abroad, but because of COVID-19 concerns, the client requested the funds to be picked up by its bank under the DPA. The amount involved, however, is above the average daily foreign currency volume of the client. Further, the client could not present any document as proof of source.

2. Using money mule or pass-through accounts

During the ECQ period, more than 13,000 transactions were flagged as suspected pass-through or money mule accounts with a total estimated value of PHP197 million. Majority of the transactions were reported

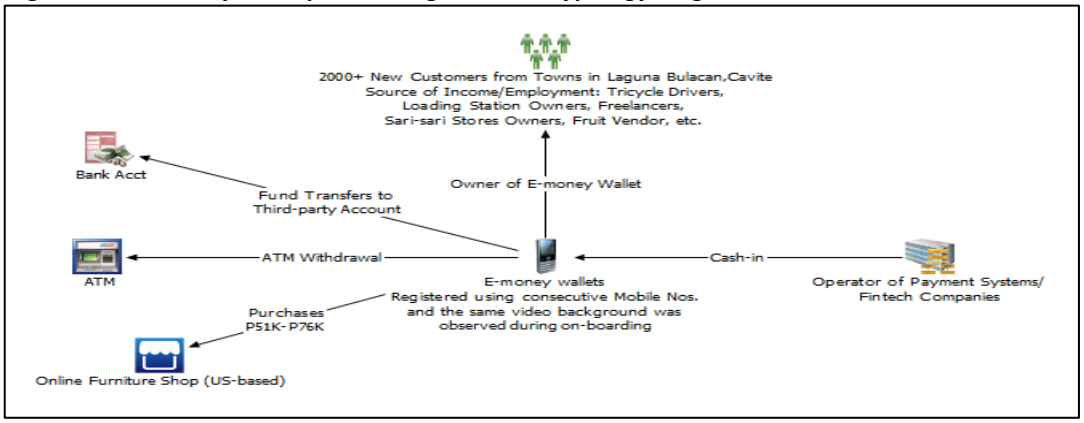
[1] Pursuant to Malacañan Palace's Proclamation No. 929, Declaring a State of Calamity Throughout the Philippines Due to the Corona Virus Diseases 2019 (https://www.officialgazette.gov.ph/downloads/2020/03mar/20200316-PROC-929-RRD.pdf accessed 27 May 2020)
[2] For purposes of this brief, these transactions will comprise the ECQ sample.
[3] http://chr.gov.ph/child-rights-advocates-urge-govt-public-dont-forget-child-victims-of-online-sexual-abuse-exploitation-amid-pandemic/ accessed on 23 May 2020



by an electronic money issuer (EMI), citing possible abuse of its digital know-your-customer/customer due diligence (KYC/CDD) process to create suspected pass-through accounts. Although these were filed within the ECQ period, transactions may cover a wider period (e.g. three [3] to six [6] months).

a. Abusing digital KYC/CDD to create pass-through accounts

Figure 1. EMI money mule/pass-through account typology diagram



More than 2,000 newly on-boarded e-money customers made multiple high-value transfers, totaling PHP180 million to third-party bank accounts. These transfers were transacted in less than six months. Majority of the customers were on-boarded from July 2019 to February 2020. Most were identified to be residents of various provinces in Luzon. These account holders were profiled as tricycle drivers, loading station owners, freelancers, sari-sari store owners, fruit vendors, and private employees, who declared business proceeds and salaries as source of funds. Suspicious indicators involving these accounts are as follows: (a) concerns surrounding high-value deposits from unidentified sources that were received in one day via certain financial technology (fintech) or payment system companies; (b) activities that appear excessive, considering the customers' profiles; (c) layering concerns as evidenced by the rapid movement of funds through subsequent cash withdrawals and transfers to a third-party account; (d) majority of the customers' KYC videos that had similar backgrounds; and (e) consecutive mobile numbers that were registered in succession. Other notable activities observed are online purchases from an online furniture shop abroad.

b. Bank account buying

Two individuals were caught buying bank accounts for PHP500 in an entrapment operation by the National Bureau of Investigation (NBI). According to the perpetrators, they would use the bank accounts to receive funds from their fraudulent activities, so that their identities would not be known or traced by proper authorities. NBI also confiscated a laptop with a stolen database, containing e-mail addresses and contact numbers of account holders of a certain bank. This information would allegedly be used by the arrested individuals in their phishing activities.

3. Swindling/estafa (various product scams)

Confidential information cites overpricing and unauthorized selling of medical items, such as alcohol, medical masks, and thermal scanners. Moreover, other fake or bogus sellers took the crisis as an opportunity to scam victims into buying essential items. Most often, offenders will post items for sale in their social media account/s. After receiving the advance payment from the buyer/victim, the seller/offender cuts off communication and blocks the buyer/victim in social media. Majority of these transactions involve local buyers and sellers. While violators are found to be in various cities and provinces in the country, heavy concentration is observed in the National Capital Region (NCR).

4. Emergency fraud and donation scams

Using the ECQ sample, the following emergency fraud and donation scam typologies were observed:

a. Emergency fraud schemes through hacking

A perpetrator hacks a social media or e-mail account. Using the hacked account, the perpetrator sends messages to the account owner's family and friends, asking for monetary assistance with purposes including medical expenses, payment of debts, and personal finance, among others. Unaware that the message is from a hacker, the victim sends funds, thinking that the beneficiary is the real account owner, that is, the victim's family or friend. The hacker usually instructs the victim to remit the purported monetary assistance through e-money wallets or money service businesses (MSBs).

b. Donation scams (social media influencer)

Perpetrators set up a faux donation campaign in social media platforms to solicit funds from the public. During the ECQ, a purported social media influencer became popular for his social media challenge, where he posts his alleged donations to COVID-19 relief efforts and encourages the upper class to donate. Based on information gathered from different sources, this person uses fictitious identities to deceive people and has been allegedly charged with various estafa cases over the years.

5. Possible terrorism financing (TF) activities linked to COVID-19

During the ECQ, a group allegedly staged a protest rally, demanding the release of relief goods (food support), which they claimed that they have not received from their local government unit (LGU). Said protest rally was purportedly organized and premeditated by two (2) left-leaning organizations (LLOs) and other allied personalities. Their purpose was to alienate the government from the marginalized community and to use chaos and disorder to portray the government as incapable of governing during the COVID-19 crisis.

As the crowds became unruly, protesters were arrested and charged with criminal offenses, including violation of ECQ rules; and resistance and disobedience to lawful order. The accused were temporarily released from jail after making bail. Their counsel claimed to have solicited the money for bail via social media, asking donors to deposit donations in two (2) bank accounts and through web-based donation/shopping platforms.

The LGU denied the allegation that there was no food support distributed to this group. Further, the arrested protesters appeared to be non-residents of the concerned LGU, and they were identified as members of the two (2) LLOs associated with a communist group (CG) and its armed-wing group (AWG). The bank accounts used to solicit funds were also identified to be common depository bank accounts used by their allies and LLOs of CG and AWG for their fundraising activities.

6. Unauthorized purchases or account access

Unauthorized transactions (e.g. various cases of card-skimming and phishing), and other financial cybercrimes (violations of the Electronic Commerce Act of 2000) have an estimated value of PHP144.2 million, based on the ECQ sample. Most of these transactions were submitted by universal/commercial banks and EMIs.

a. One-time password (OTP) phishing via fake social media customer care

The victim sought assistance from an EMI via its customer care's social media account because the victim could not log in the EMI account. After sending a message, the victim received a call from an alleged customer service representative (CSR) of the EMI. The CSR offered assistance and asked the victim's personal identification number and OTP. After providing the details, the victim discovered that funds were transferred from the victim's savings account that was linked to the victim's EMI account. This was immediately followed by three more fund transfers in favor of two other EMI wallets unknown to the victim.

b. OTP e-mail phishing, transfer of funds from bank to EMI

During the ECQ, moving small-value funds became easier as payment system operators waived transaction fees, making online fund transfers more convenient. As observed from the sample, there were reported unauthorized transactions of transferring funds from bank accounts to various e-wallet channels. Based on confidential information, a client received an e-mail about an account information update. The client updated the records by using the link sent through the said e-mail, thinking that the link was from the bank's website. The client also provided the OTP, not knowing that it was already for the authorization to debit the client's savings account. Thereafter, the client received a notification that transfers, which the client did not intend to authorize, were successfully executed. This prompted the client to report the unrecognized transactions. The ultimate beneficiary of said transfers is an unknown e-wallet.

7. Various extortion schemes

a. "Sextortion" or blackmail attacks

During the ECQ period, there were confidential information involving victims, who received e-mails or SMS messages from unknown perpetrators. These perpetrators state that they know the victims' passwords and/or that they have access to the victims' private videos or photos. This scheme, which often involves deposits through virtual wallets or remittances through MSBs, intends to extort money from victims. In some cases, the attack is random, and the perpetrator is merely intimidating the victim. In other cases, the perpetrator initially befriends the victim and eventually asks for salacious videos or photos. Once the victim gives in, the perpetrator would demand money in exchange for not exposing the victim's photos or videos publicly. As observed in the ECQ sample, sextortion or blackmail transactions were often small in value and are coursed through non-banks like MSBs, EMIs, and pawnshops. The total estimated value is PHP413,172.

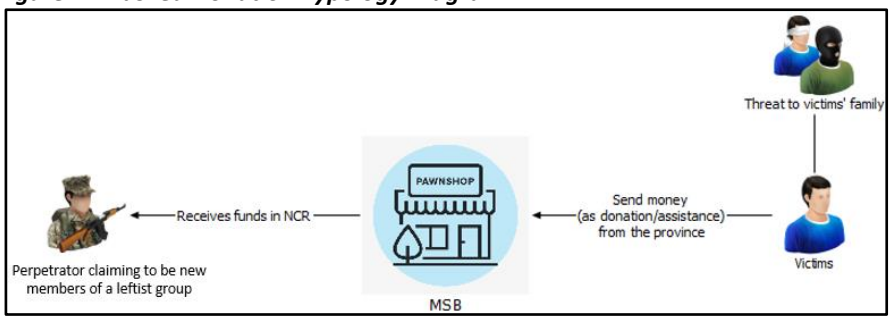
Table 1. Transactions related to sextortion or blackmail

	No. of Transactions	%Share to Total	Estimated Peso Value
Electronic Money Issuer	37	82.22%	354,519.32
Money Service Businesses/Pawnshop	8	17.78%	58,652.77
Total	**45**	**100.00%**	**413,172.09**

b. Extortion masked as donation

Another type is extortion money disguised as a donation or financial assistance for a friend. Perpetrators claiming to be new members of a leftist group would threaten the safety of the victims' family and would instruct the victim to send funds in exchange for the safety of the family. Victims are usually located in provinces outside NCR. To avoid endangering lives, victims would comply and send money through MSBs, declaring the purpose of the transactions as a donation or financial assistance. The alleged offender would then withdraw the funds in NCR.

Figure 2. Masked Donation Typology Diagram



8. *Online sexual exploitation of children (OSEC)*

An estimated value of PHP11.9 million related to OSEC were observed from the ECQ sample. Typical to child exploitation cases, none of the transactions were coursed through banks. More than 99% were transacted and reported by MSBs, and the rest were through pawnshops and EMIs.

Table 2. Transactions related to OSEC

	No. of Transactions	%Share to Total	Estimated Peso Value
Electronic Money Issuers	1	0.03%	3,000.00
Money Service Businesses	3,389	99.21%	11,629,568.35
Pawnshops	26	0.76%	293,063.45
Total	**3,416**	**100.00%**	**11,925,631.80**

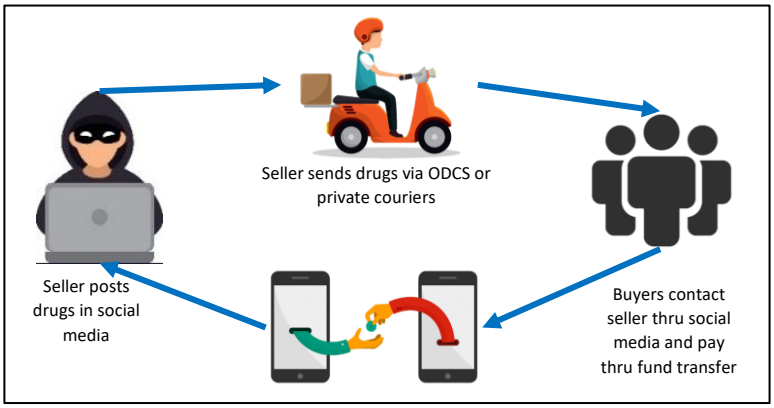
Forty-two (42) domestic remittances came from Cebu, Cavite, Cagayan, Bulacan, Tarlac, Pampanga, Leyte, Negros Occidental, and Quezon City. International remittances to the Philippines, on the other hand, came from the United States of America, Australia, Canada, Saudi Arabia, United Kingdom, Kuwait, and Hong Kong.

Confidential information recounts that a foreign national, who was a pensioner residing in a metropolitan area in the Philippines, was sending local remittances to various individuals. The declared purposes of the transactions included transportation, allowance, food expense, rental, budget, medicine, and salary. The sender declared varied relationships with the recipients, such as boyfriend, friend, uncle, or brother. In other instances, recipients were declared as helper or caregiver. Transaction alerts were triggered by the volume and frequency of the remittances, which reached 200 counts; and by the characteristics of the recipients, who were Filipinos, usually female, and residents of Bohol, Cebu, Samar, Leyte, Davao City, Rizal, Negros Occidental, Negros Oriental, Bulacan, Misamis Occidental, Misamis Oriental, Agusan del Norte, Compostela Valley, Laguna, Cavite, Cagayan de Oro, Biliran, Surigao del Sur, Pampanga, and Metro Manila. Majority of the transactions were between PHP140 and PHP30,000. Eight (8) female individuals received over 10 transactions each with a total count of 159 remittances equivalent to PHP664,355. Suspicious indicators cited were (1) numerous remittances sent to different local individuals, who were usually female, with unjustified and unsupported purpose and relationship; and (2) the usual destinations known to be closely related to OSEC.

9. *Drug trafficking via on-demand courier services (ODCS)*

The crisis did not hinder drug syndicates in their operations. Selling illegal drugs are blatantly advertised in social media accounts. Modes of payment may be through cash-on-delivery (COD), through EMI, or through other fund transfer services. Delivery is made by ODCS or private couriers, pretending to be carrying medical or food items.[4]

Figure 3. Drug trafficking (ECQ) typology diagram



According to the National Capital Region Police Office (NCRPO) chief, an estimated PHP171 million-worth of drugs (approximately 25.2 million kilograms) were confiscated from 15 March to 10 May 2020. This is compared to the less than five (5) kilograms confiscated during the same

[4] https://philnews.ph/2020/05/11/more-shabu-confiscated-in-2020-despite-strict-quarantine-protocols/ accessed on 15 May 2020

period last year. Most of these arrests happened in road checkpoints. Despite several news reports on this modus, there were no suspicious transactions filed by covered persons (CPs) involving this modus in the ECQ sample.

III. Conclusion and recommendation

Except for the timing of the transactions, a direct correlation between the rising suspicious reports and COVID-19 cases or the ECQ has not been established. Report filing of CPs significantly increased starting March 2020 with more than 104,138 suspicious reports from 1 March to 24 April 2020. Of these transactions, however, 59% have transactions dates that do not fall under or near the ECQ period. Only 41% were considered part of the ECQ sample, and even a smaller subset of only 185 suspicious reports contained COVID-19 related keywords.

From the current sample, it seems that transactions related to the pandemic and lockdown may be minimal. There is a possibility, however, that some suspicious reports related to the pandemic were not labeled by the CPs and were not identified in the study. Thus, for better triaging of COVID-19 related financial crimes, CPs may use suggested keywords when reporting these transactions such as "COVID-19," "ECQ," "pandemic," "lockdown," "MECQ," "GCQ," "quarantine," "Wuhan," and other relevant terminologies. Moreover, some unlawful activities during ECQ have elements of or are analogous to swindling/estafa and violations of Electronic Commerce Act of 2000. To enhance surveillance efforts, additional keywords may be used in describing scheme types, which may relate to COVID-19 or the community quarantine, such as "donation scam," "product scam," "overpricing scam," "fake product scam," "bogus or fake seller scam," "e-mail phishing," "text/SMS phishing," "fake calls phishing," "fraudster account hacking," "one-time-password/pin (OTP) scam," "fraudster identify theft," and other related schemes.

All CPs are also advised to be cautious as money launderers and perpetrators could be abusing the digitization, such as digital KYC/CDD, which many CPs adopted during the pandemic. As unemployment rises, the general public could be enticed by criminals to sell their profiles to create pass-through or money mule accounts and take advantage of CP's digital account applications and non-physical KYC process. Transaction behavior analysis and other innovative CDD methodologies (e.g., checking the geo-tag of the submitted KYC photo vis-à-vis the declared address; comparing addresses using open-source satellite maps of the address or declared income/business, etc.) will be crucial in the new economy as non-physical transactions become mainstream. Further, EMIs, MSBs, and other online fund transfer services are advised to be vigilant as the data comparing March-April 2020 vis-à-vis the same months in 2019 shows growth in suspicious transactions related to online activities.

Aside from AMLC-triggered information and requests, various local law enforcement agencies have issued several bulletins via their official websites. These include press releases relative to the names of suspects and arrests on drug-related cases and online sexual exploitation of children, as well as other unlawful activities, such as violations of Electronic Commerce Act of 2000, Price Act, Consumer Act, and Bayanihan to Heal as One Act, among others. This could be an additional reference for CPs when filing suspicious transactions. Official websites include those of the NCRPO and PNP Women and Children Protection Center.