BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2020-053
Series of 2020

To : **All BSP-Supervised Financial Institutions (BSFIs)**

Subject: **Reminder on Sound Risk Management Practices to Mitigate Risks from Scams or Frauds using BSFI's Products and Services**

The BSP has been receiving complaints from the public who were reportedly defrauded by scammers or fraudsters using financial products and services, such as deposit or electronic money accounts, credit cards and remittance services as modes to fraudulently funnel out funds. In this regard, it is important that BSFIs remain vigilant and steadfast to mitigate and prevent risks arising from these illegal activities and preserve the public's confidence in using financial services. In line with this, BSFIs are reminded to maintain the soundness and propriety of their risk management policies and practices, consistent with the BSP's regulations on Anti-Money Laundering/Countering the Financing of Terrorism and Consumer Protection, among others. Specifically, BSFIs are reminded to:

1. Identify, assess, understand and measure the risks associated with these scams/frauds. This will enable identification of the products and services that are being used by scammers/fraudsters or vulnerable to be used for illegal activities.

2. Adopt and/or enhance policies, procedures and controls commensurate with the identified risks to prevent the use of their financial products or services as delivery channels for the proceeds of unlawful activities or as a conduit, knowingly or unknowingly. Such policies and procedures should include the following, among others:

   a. Conducting risk-based due diligence on customers with occasional but relevant business transactions with the BSFI;

   b. Proactive monitoring of accounts using relevant parameters or alert scenarios that capture the customer's financial profile, transactional capabilities and behavioral account activities. This may include, among other things, matching transactions vis-à-vis the BSFI's understanding of the account holder's financial profile, source of wealth and expected transactions;

   c. Using customer complaints as input to accounts review or trigger to conduct transactional enhanced due diligence or further investigation, and file suspicious transaction report (STR), as warranted;

   d. Updating the risk profile of customers, considering historical transactions and activities, including whether the customer was suspected of involvement in scams/frauds, and reviewing the relationship based on updated information;

e. Adopting policies and guidelines with defined criteria or grounds for the review, escalation, and/or handling of customer complaints and business relationships, including basis for decision to retain, restrict or terminate the account, when warranted, of customers subject to reported cases or incidents;

f. Using customer complaints as part of the triggers for transaction cancellation, reversal or refund;

g. Developing a robust due diligence process for the recruitment of cash agents to minimize onboarding of agents with poor reputation or those likely to commit fraud; and

h. Using the results of investigation in screening existing and prospective customers and cash agents, where applicable.

3. Adopt and implement an effective financial consumer protection framework pursuant to the financial consumer protection regulations in the Manual of Regulations (MOR) for Banks and MOR for Non-Bank Financial Institutions which should include, among others, the following:

   a. Proactively promoting digital literacy and cybersecurity awareness of consumers to reduce the vulnerability of financial consumers to usage errors, scams and frauds, to prevent losses, protect consumer welfare and ensure positive customer experiences and outcomes as they use digital financial services; and

   b. Providing responsive complaint and redress mechanism through widely accessible channels such as, social media platforms, website, e-mail, live-chat and text to entrench consumer trust in the use of BSFIs' products and services.

4. Adopt appropriate security policies and measures to strengthen cybersecurity and ensure that these are tested, monitored and updated on a regular basis.

5. Continue programs to enhance awareness and capability of personnel and cash agents, where applicable, to proactively identify irregularities in customer's activities or transactions.

Annex A contains sample typologies of scams/frauds gathered from the complaints received by the BSP.

For information, guidance and implementation.

CHUCHI G. FONACIER
Deputy Governor

Att: a/s

19 June 2020

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
06/23/2020
RYA ROSE D. NUNEZ
Manager, RMD
Administrative Services Department

Annex A

Sample Typologies of Scams/Frauds Gathered from the Complaints Data

1. *Advance Fee Fraud.*

   - The complainant was required by a supposed loan agent to pay around Php1,000.00 as loan application fee for the grant of a loan of Php11,000.00 payable for eleven months. After paying the Php1,000.00 through an *e-money account*, she did not receive any reply from the loan agent.
   - The complainant was informed by someone through text that he won a certain amount of prize. The complainant sent around Php21,000 through *money remittance service*, as payment for the tax prior to the release of the prize. After sending the money, the complainant no longer received any response from the scammer.

2. *Romance scam/ Impostor scam*

   - Complainant has been chatting online with a guy who is allegedly from Houston, Texas. She fell in love and gave all her savings plus borrowed money estimated at Php375 thousand. The funds were deposited to the *deposit and e-money accounts* of Filipino nationals. After sending money to these individuals, she did not receive any reply from the supposed "foreigner".
   - Complainant met an alleged seaman via online chat and accepted his proposal to be in a relationship. The "seaman" told complainant that he sent a package to the Philippines containing gifts, such as gadgets. However, to claim the said package, complainant has to deposit around Php20,000 in the *deposit account* of another person, a Filipino, purportedly for import administrative charges and another Php43,000 for penalty charges. The package was not delivered after payment.
   - Complainant met someone posing as a foreigner via online mode. The foreigner represented that he will go to the Philippines to work as consultant engineer and that he will meet her. When the foreigner purportedly arrived in the Philippines, he asked money from the complainant and promised to return double the amount sent. Complainant reportedly deposited around Php1.8 million to the *bank accounts* of three different individuals of Filipino names. After making the deposits, complainant can no longer contact the supposed foreigner.

3. *Bogus Online Seller/Agent.*

   - Complainants bought items sold online, such as airline ticket, cell phones, dining set, and unlimited internet connection. The payments were sent to the supposed seller's *bank deposit accounts or e-money accounts*. After sending payments, the sellers can no longer be contacted.
   - Complainant joined a supposed online promotional game of an alleged local bank representative using a social media account. The game asked the complainant to provide her username, accounts' last four (4) digits, and One-Time-Password (OTP). Afterwhich, the complainant received an e-mail notification from her bank informing her that a transaction

worth around Php50,000 has been posted. The alleged local bank representative cannot be contacted by the complainant after her *account* was debited.

4. *Facebook/Text Scam by a Bogus Relative.*

   - Complainants *sent money* to someone posing as their relative, such as grand daughter, cousin, brother or sister, asking for financial assistance purportedly for emergency purpose, such as accident. The payments were sent to the supposed relative's *deposit or e-money accounts*. After sending the payment, the alleged relatives can no longer be contacted or turned out to be bogus.

5. *Investment/FX dealing Scam.*

   - Complainants were enticed via social media to place money in an investment, forex trading, or financing company promising high returns/profits within short periods of time. Aside from the principal amount, registration fees, upgrade fees and costs of fund transfers, were paid by the complainants to the supposed agents of the aforesaid companies. The investments were paid by the complainants through *cash deposits, fund transfers via mobile banking or e-money transfers* to the agents' accounts. Afterwhich, the complainants cannot contact said agents either because their social media accounts have been blocked or the agents have deactivated their own social media accounts.

   - Complainant sold around US$55,000 to a certain buyer purportedly from a trading company for around Php2.8 million. The payment of the peso equivalent was credited to the complainant's *bank account* as evidenced by a cash deposit transaction slip sent by the buyer. However, said credit was subsequently reversed by the bank as the check deposit was drawn by another person (accomplice) against a closed account. The FX buyer cannot be contacted anymore.

6. *Online Gaming Scam.*

   - Complainant deposited around Php4,000 in the *bank account* of the scammer via online banking to place a bet in an online game. Afterwards, the complainant was unable to get the "cash out" representing the balance of complainant's bets and/or winnings.

7. *Phishing through e-mail, text (smshing) or phone call (vishing).*

   - Complainants received e-mail, text or phone call from someone purporting to be a representative of the financial institution and requesting to update their personal information, including their username and one-time password (OTP). Afterwhich, unauthorized debits/fund transfers were charged against the complainants' *bank accounts*. The person who e-mailed, texted or called the complainants can no longer be contacted.
   - Request for reimbursement and/or reinvestigation of disputed transactions charged to complainant's credit card consisting of several *e-money* online transactions amounting to around Php80,000 simultaneously done in a single day.

8. *Fake social media site/account*

- Complainant logged on to his Twitter account and searched for the Official account of E-money issuer. He requested a Direct Message (DM) in order to report an issue encountered using the *mobile app*. A DM was received from the supposed e-money issuer who asked for his mobile number, OTP and MPIN. The fraudster thereafter mentioned that they had to temporarily hold the funds, update the profile and transfer back the funds to the linked *bank accounts*. Complainant found the process suspicious and realized that it was a bogus/unverified account. While the complainant immediately changed his MPIN and unlinked his bank accounts, funds were already debited from his account.

9. *Bogus Employment Abroad.*

- Complainant paid via *money transfer agent* to someone allegedly from a manning agency offering the complainant through social media to attend a seminar for employment abroad.
- Complainant made an over-the-counter cash deposit amounting to around Php100,000 in the *bank account* of someone purporting to recuit complainant for employment abroad. The money deposited was allegedly part of the requirements for her to work abroad.