國泰世華銀行
Cathay United Bank

SCAM ALERT

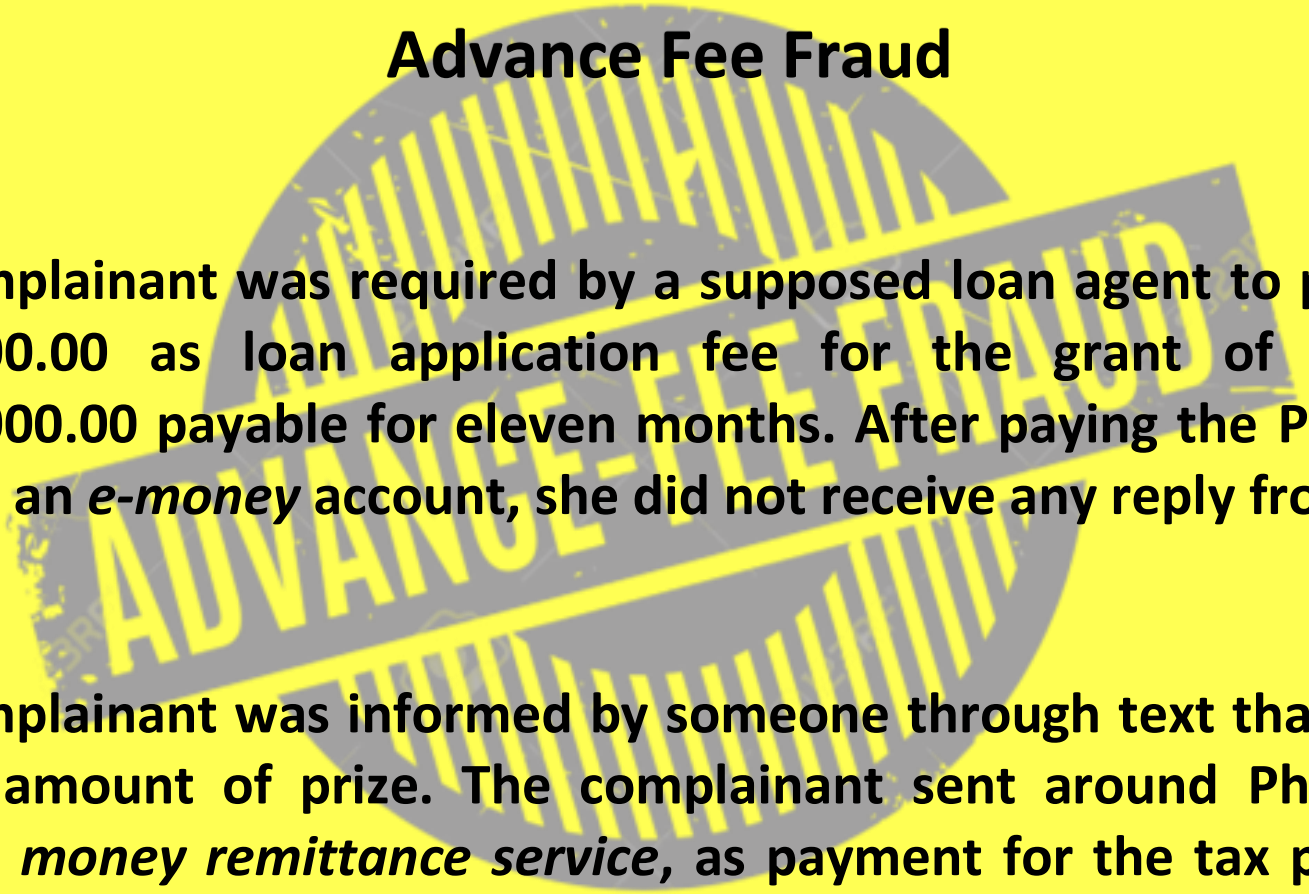
- **Emails, calls, texts or website ads from fake companies or people pretending as personnel of banks, financial institutions, or government agencies, asking for personal information, such as account number, PIN, password, or login credentials.**

PROTECT YOURSELF FROM CYBER THREATS:

- **Scrutinize emails, texts and websites**
- **Perform a background check**
- **Use strong passwords**
- **Use multi-factor authentication**
- **Keep personal and account information private**
- **Report suspicious communications, personnel or transactions to regulatory authorities**

Sample Typologies of Scams / Frauds

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 Php21,000.00 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.**

Sample Typologies of Scams / Frauds

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 Php375,000.00. 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 Php20,000.00 in the deposit account of another person, a Filipino, purportedly for import administrative charges and another Php43,000.00 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 Php1,800,000.00 to the bank accounts of three different individuals of Filipino names. After making the deposits, complainant can no longer contact the supposed foreigner**

Sample Typologies of Scams / Frauds

Bogus Online Seller/Agent

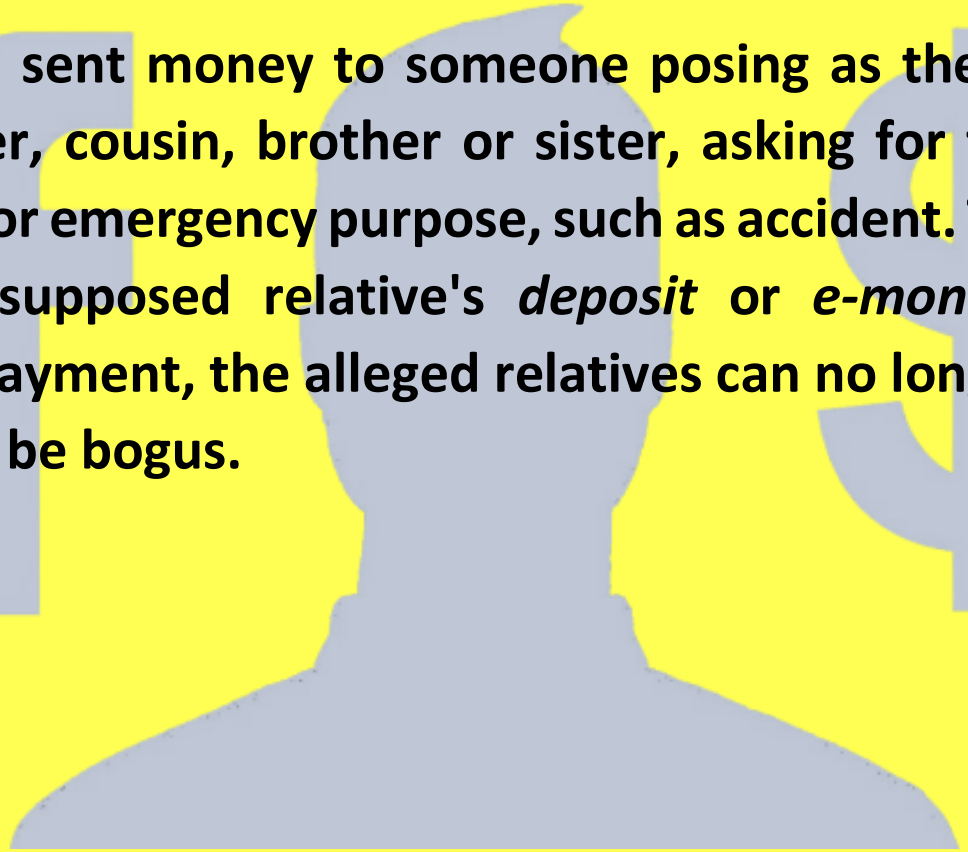
- **Complainants bought items sold online, such as airline ticket, cell phones, dining set, and unlimited internet connection. The payments were sent to the supposed seller's bank *deposit accounts* or *e-money accounts*. After sending payments, the sellers can no longer be contacted.**

- **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). After which, the complainant received an e-mail notification from her bank informing her that a transaction worth around Php50,000.00 has been posted. The alleged local bank representative cannot be contacted by the complainant after her account was debited.**

Sample Typologies of Scams / Frauds

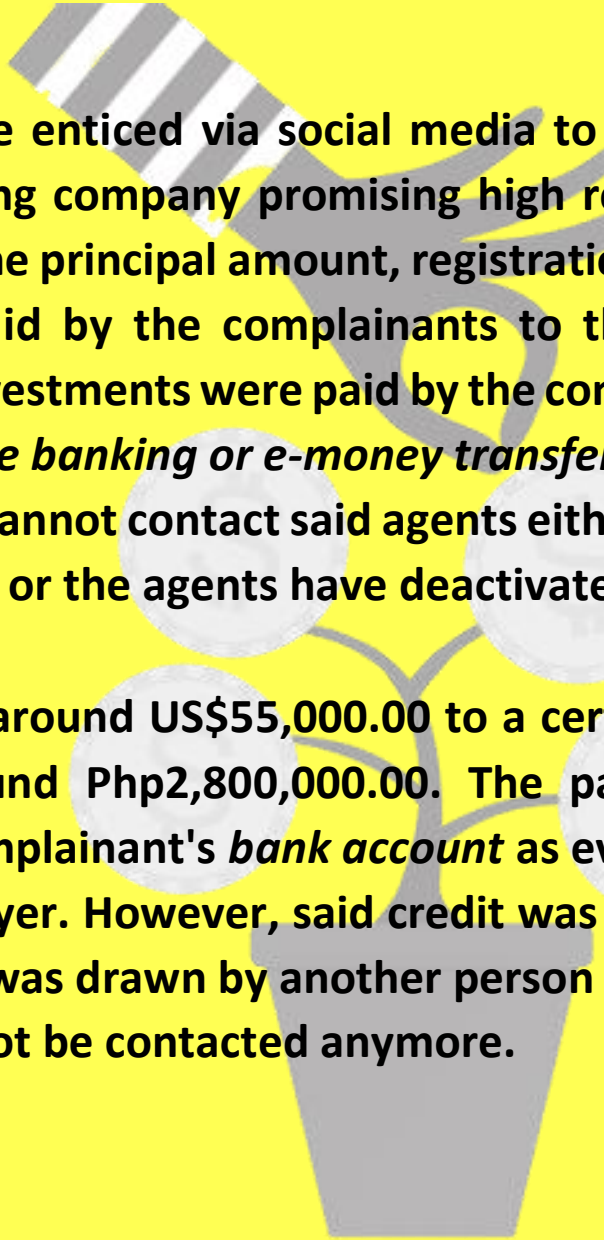
Facebook/Text Scam by a Bogus Relative

- **Complainants sent money to someone posing as their relative, such as granddaughter, 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.**



Sample Typologies of Scams / Frauds

Investment/FX dealing Scam

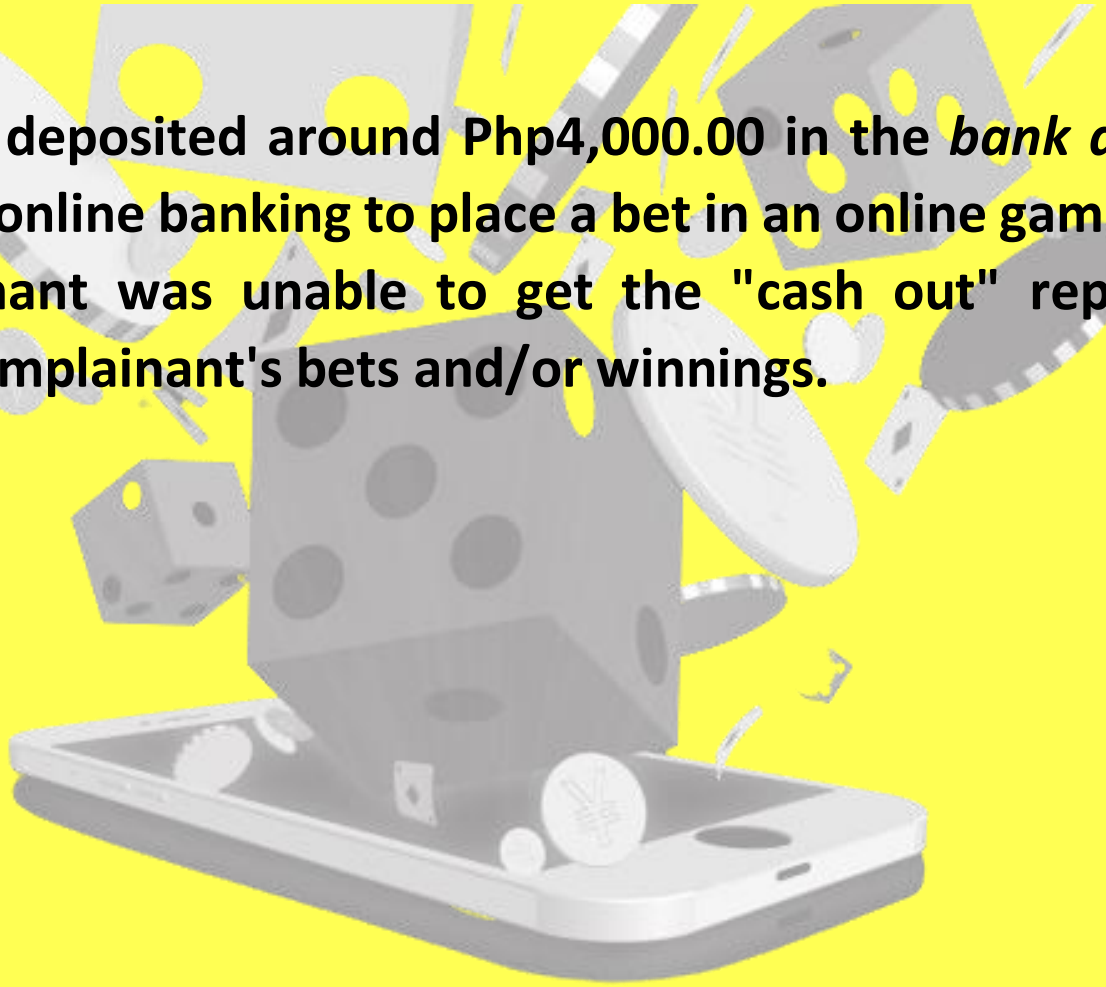


- **Complainants were enticed via social media to place money in an investment, forex trading, or financing company promising high returns/profits within short periods of time. Aside from the principal amount, registration fees, upgrade fees and costs of fund transfers, were paid by the complainants 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 agent's 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$55,000.00 to a certain buyer purportedly from a trading company for around Php2,800,000.00. 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.**

Sample Typologies of Scams / Frauds

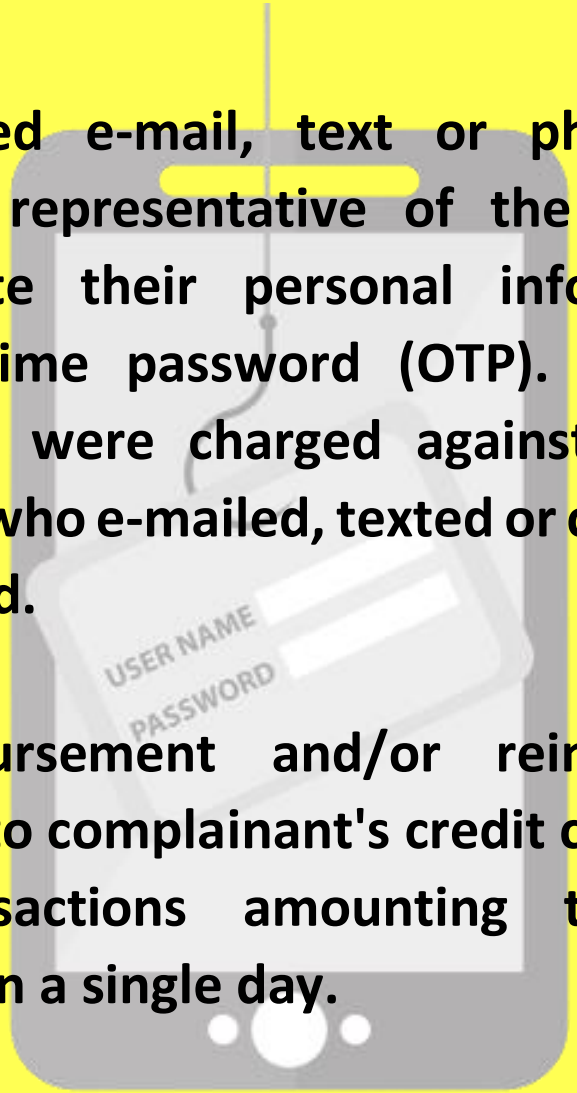
Online Gaming Scam



- **Complainant deposited around Php4,000.00 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.**

Sample Typologies of Scams / Frauds

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



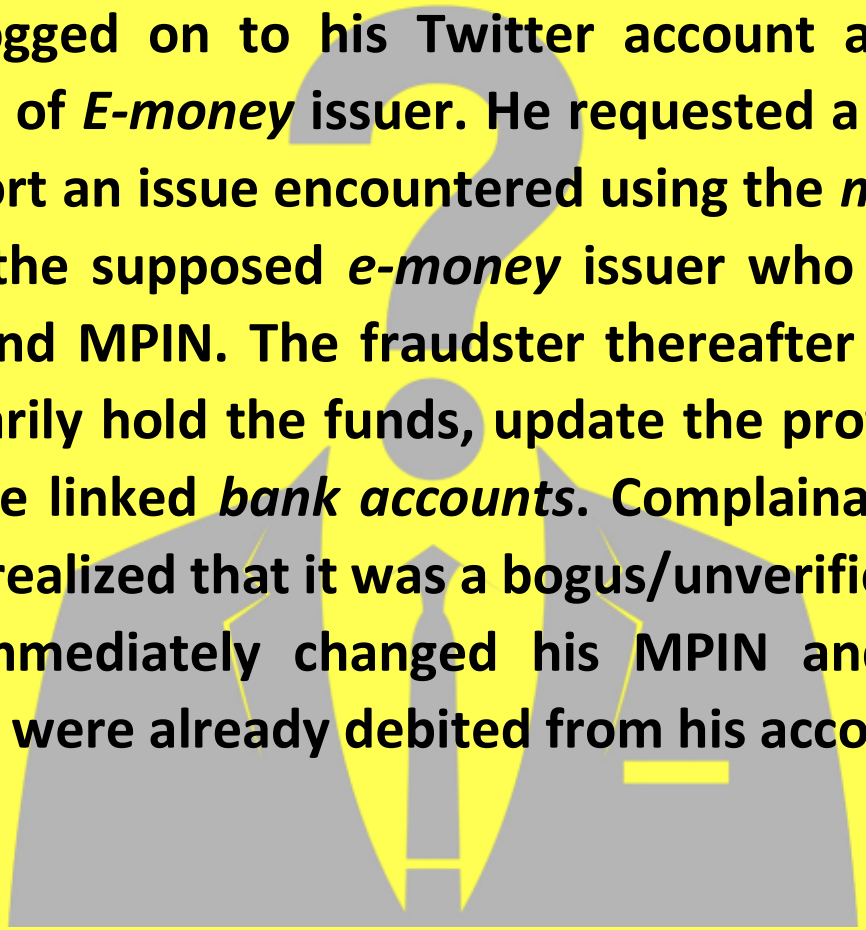
- **Complainants received e-mail, text or phone call from someone purporting to be a representative of the financial institution and requesting to update their personal information, including their username and one-time password (OTP). Afterwhich, unauthorized debits/fund transfers were charged against the complainant's *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 Php80,000.00 simultaneously done in a single day.**

Sample Typologies of Scams / Frauds

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.**



Sample Typologies of Scams / Frauds

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 Php100,000.00 in the bank account of someone purporting to recruit complainant for employment abroad. The money deposited was allegedly part of the requirements for her to work abroad.**