Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 215

ACG-CSB 081821215

Reference Number ACG-CSB 081821215

HOW TO AVOID DIGITAL WALLET FRAUD

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as **"Restricted"** pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

More and more, digital currency and mobile payment apps are becoming the preferred option for consumers across all demographics to pay for the goods and services they need. Of course, with this rise in popularity comes an increased risk of being targeted by fraudsters and scam artists that utilize these apps for their schemes. As is the case with most fraud, your first and best line of defense is awareness. That's why today, we'll tell you how you can spot mobile payment scams and avoid digital wallet fraud.

A mobile payment or digital wallet app simply refers to a program you use on your smartphone that allows you to quickly and easily send funds to someone else. While these can often be used as an alternative to credit cards, they are frequently used to send money to a friend or family member as a form of repayment. For example, if you need to pay your friend for your portion of the restaurant bill, or if you have to pay your roommate for your half of the utilities, these apps can make that process simple.

There are many different mobile payment apps available today. These are some of the most popular apps that people are using to pay for goods and services like **Apple Pay, Google Pay, Cash App** and etc. The features of each mobile payment app vary, but most of them can be used to send electronic payments, to accept credit card payments, and to manage an account with money.

In this scam, scammers will pose as users on the most popular mobile payment apps. While most authentic users will link their personal credit card or business credit card to their account, these scammers use stolen credit cards to make fraudulent payments across a variety of platforms. Often times, they convince the sellers to send an item prior to making the payment. They make the payment with a stolen card after the item has been shipped, leaving the seller completely empty-handed.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of **DIGITAL WALLET FRAUD:**

- **Use money transfer with friends:** Protect yourself from scams by only using money transfer apps for their intended purpose -- sending money to people you personally know.
- **If someone sends you money by mistake, ask them to cancel the transaction:** The sender can request that the vendor cancel the transaction. If the person refuses, it's probably a scam.
- **Enable additional security settings**: Check your account settings to see if you can turn on additional security measures, such as multi-factor authentication, requiring a PIN, or using fingerprint recognition.
- **Link your money transfer app to a credit card.** As with many other purchases, using a credit card will help protect you if you don't get the goods or services you paid for. Linking to a debit card or directly to your bank account does not give you that added protection.

For additional information, please refer to the following websites:

- https://germaniainsurance.com/blogs/post/germania-insurance-blog/2020/11/02/mobile-payment-scams-how-to-avoid-digital-wallet-fraud
- https://www.wafb.com/2020/05/12/bbb-beware-digital-wallet-scams/

POINT OF CONTACT

Please contact **PMAJ ROVELITA ROBIÑOS AGLIPAY** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723 0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.