Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

April 14, 2022

Alert Number
I-041422-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Cybercriminals Trick Victims into Transferring Funds to "Reverse" Instant Payments

Cybercriminals are targeting victims by sending text messages with what appear to be bank fraud alerts asking if the customer initiated an instant money transfer using digital payment applications (apps). Once the victim responds to the alert, the cybercriminal then calls from a number which appears to match the financial institution's legitimate 1-800 support number. Under the pretext of reversing the fake money transfer, victims are swindled into sending payment to bank accounts under the control of the cyber actors.

THREAT

Cybercriminals are targeting victims with a sophisticated phishing and social engineering scam which results in victims unwittingly sending funds to the actors using digital payment apps. The actors take advantage of payment apps connected to bank accounts. These payment apps are meant for the quick transfer of funds between registered users, with only the recipient's email or mobile number needed to initiate an instant payment transaction. The scam starts when cyber actors send financial institution customers an automated text message similar to the following:

```
Free Msg- (Insert financial
institution name here) Bank
```

```
Fraud Alert- Did You Attempt an
Instant Payment in the amount of
$5,000.00? REPLY YES or NO or 1
To STOP ALERTS
```

The payment amount and financial institution name changes from victim to victim. If customers reply to the text with "No," a follow-up message is sent:

```
Our fraud specialist will be
contacting you shortly
```

The actors-who typically speak English without a discernable accent-then call the victim from a number which appears to match the financial institution's legitimate 1-800 support number, and claim to represent the institution's fraud department. Once the actor establishes credibility, they walk the victim through the various steps needed to "reverse" the fake instant payment transaction referenced in the text message.

In these schemes, background information on the victims appears to have been well researched. In addition to knowing the victim's financial institution, the actors often had further information such as the victim's past addresses, social security number, and the last four digits of their bank accounts. This information was used to convince customers that the steps being requested of them were the financial institution's legitimate process for retrieving stolen funds.

Using the bank's legitimate website or application, the actor instructs the victim to remove their email address from their digital payment app. The actor, after asking for the victim's email address, adds it to a bank account controlled by the actor. After the email address has been changed, the actor tells the victim to start another instant payment transaction to themselves that will cancel or reverse the original fraudulent payment attempt. Believing they are sending the transaction to themselves, the victims are in fact sending instant payment transactions from their bank account to the actor-controlled bank account. In many cases, the cyber actors engaged with victims for several days. Victims often only realized they had been scammed after they checked their financial account's balance.

RECOMMENDATIONS

The FBI recommends the following precautions:

- Be wary of unsolicited requests to verify account information. Cyber actors can use email addresses and phone numbers which may then appear to come from a legitimate financial institution. If a call or text is received regarding possible fraud or unauthorized transfers, do not respond directly.
- If an unsolicited request to verify account information is received, contact the financial institution's fraud department through verified telephone numbers and email addresses on official bank websites or documentation, not through those provided in texts or emails.
- Enable Multi Factor Authentication (MFA) for all financial accounts, and do not provide MFA codes or passwords to anyone over the phone.
- Understand financial institutions will not ask customers to transfer funds between accounts in order to help prevent fraud.
- Be skeptical of callers that provide personally identifiable information, such as social security numbers and past addresses, as proof of their legitimacy. The proliferation of large-scale data breaches over the last decade has supplied criminals with enormous amounts of personal data, which may be used repeatedly in a variety of scams and frauds.