SCAM ALERT: "PIG BUTCHERING"

BEWARE: THIS SCAM CAN CAUSE SERIOUS HARM TO YOUR BANK AND YOUR CUSTOMERS!

This scam is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.

How the Scam Works:

- **Perpetrators contact victims at random** via text messages, dating apps, social media platforms, and later switch to VOIP chat applications.
- **Perpetrators develop meaningful relationships with victims**, gain their trust, and offer them high-yield investment opportunities in virtual assets, such as cryptocurrency.
- **Perpetrators tell victims to open accounts on online investment websites** and instruct them to deposit money via wire transfer to shell companies, or direct transfers on legitimate virtual asset service providers (VASPs) or cryptocurrency exchanges.
- **Perpetrators pressure victims** to investment more money, or the relationship will end.
- **Victims are duped and the fraud ends:** When a victim attempts to withdraw money, websites may demand that victims pay additional fees to do so; other victims are locked out of the account and never hear back from the perpetrator. **Perpetrators disappear with all of the victim's funds**.

What to Watch For: "Red Flags"

- A customer with no prior interactions with virtual exchanges suddenly exchanges large sums of fiat currency from their bank account for virtual currency or transfers money to VASPs.
- A customer's account shows frequent and large withdrawals of money or multiple wire transfers to a VASP-when in the past, there was limited or no activity in the account.
- A customer appears distressed or anxious to access funds immediately to meet the timeline of a virtual currency investment opportunity or a bank receives calls from a victim requesting the cancellation of a transfer.

What to Do: Mitigate Your Risk!

- **Focus on "Know Your Customer" (KYC) requirements:** Do the businesses and individuals have websites? Are they registered with the appropriate state and federal compliance office?
- **Immediately freeze accounts and conduct compliance checks:** Follow up with account owners who you suspect to be victims. Justify the origin of the money. Request supporting documentation, such as invoices for services provided.
- **Contact recipients of outbound transactions:** Ensure transfers are for legitimate purposes.

OIG
Office of Inspector General

REPORT: File a Suspicious Activity Report (SAR) and 314(b) filings. Financial institutions are encouraged to refer their customers who may be victims of Pig Butchering Scams to their local police department to file a police report and to file a complaint on the FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov.

Scan to learn more