Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 3, 2022

Alert Number
I-100322-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

Cryptocurrency Investment Schemes

The FBI Miami Field Office, in coordination with the Internet Crime Complaint Center (IC3), warns of investment schemes involving cryptocurrency, called Pig Butchering. In this scheme, fraudsters, posing as highly successful traders in cryptocurrency, entice victims to make purported investments in cryptocurrency providing fictitious returns to encourage additional investments.

The fraudsters make contact with their victims on various social media or dating applications (either spoofing long lost contacts known to the victim or posing as a potential friend or romantic partner) and often spend time gaining the victim's confidence and trust. The victims are then coached through the investment process and encouraged to make continuous deposits by the fraudsters. The fake websites/apps allow the victims to track their investments and give the impression they are growing exponentially. When the victims attempt to cash out their investments, they are told they need to pay income taxes or additional fees, causing them to lose additional funds. The victims are unable to retrieve their purported investments and often lose contact with the fraudsters, either due to the closing of the fraudulent website or the fraudster ceases contact with the victim.

Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards. The use of cryptocurrency and cryptocurrency ATMs is also an emerging method of payment. Individual losses related to these schemes ranged from tens of thousands to millions of dollars.

The FBI has identified potential ways individuals can recognize and deter this activity:

- Verify the validity of any investment opportunity from strangers or long-lost contacts on social media websites.
- Be on the lookout for domain names that impersonate legitimate financial institutions, especially cryptocurrency exchanges.
- Misspelled URLs, often with a slight deviation from the actual financial institutions' website, may be fake.
- Do not download or use suspicious looking apps as a tool for investing unless you can verify the legitimacy of the app.
- If an investment opportunity sounds too good to be true, it likely is. Be cautious of get rich quick schemes.

If you believe you have been a victim of a Pig Butchering scheme or other fraudulent scheme, please file a report with the FBI's Internet Crime Complaint Center at www.ic3.gov. If possible, include the following:

- Information regarding how the individual initially contacted you and how they identified themselves. Include identifying information such as name, phone number, address, and email address, and username.
- Financial transaction information such as the date, type of payment, amount, account numbers involved (to include cryptocurrency wallet), the name and address of the receiving financial institution, and receiving cryptocurrency addresses.