FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2023-PIGBUTCHERING**" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

1. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. *See* U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).
3. Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).
4. While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). *See* Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.
5. *See* New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). *See also* DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world.[6] Multiple U.S. law enforcement sources estimate victims in the United States have lost billions of dollars to these scams and other virtual currency investment frauds.[7]

This alert explains the pig butchering scam methodology, provides red flag indicators to assist with identifying and reporting related suspicious activity, and reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA). Pig butchering scams are linked to fraud and certain types of cybercrime, which are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[8]

The information contained in this alert is derived from FinCEN's analysis of BSA data, open-source reporting, and information from law enforcement partners.

Methodology of a Pig Butchering Scam

Initial Contact with Victim

A scammer[9] typically makes initial contact with a potential victim through text messages, direct messages on social media, or other communication tools and platforms, usually under the guise of accidentally reaching a wrong number or trying to re-establish a connection with an old friend.[10] The scammer, who may claim to be an investor or money manager, may also create a social media

Scammers may communicate with victims using:

- Instant messaging services and text messages
- Professional networking sites
- Social media
- Dating sites

6. Michigan Department of Attorney General, Consumer Protection Division, "Cryptocurrency Scam – Pig Butchering" (Michigan AG Alert), and Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) Public Service Announcement (PSA), "The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds" (May 2023 FBI PSA) (May 22, 2023).
7. FBI PSA, "The FBI Warns of a Spike in Cryptocurrency Investment Schemes," (March 2023 FBI PSA) (Mar. 14, 2023). In 2022, investment fraud, as a general category, caused the highest losses of any scam reported by the public to the FBI IC3, totaling $3.31 billion. Fraud involving cryptocurrency, including pig butchering, represented the majority of these scams, and increased 183% from 2021 to a total of $2.57 billion in reported losses in 2022. FBI IC3, "2022 Internet Crime Report" (Mar. 9, 2023), at p. 12.
8. FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (Jun. 30, 2021). FinCEN periodically releases alerts and advisories on the use and abuse of virtual currencies. *See* FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019). *See also* FinCEN, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (Nov. 8, 2021); and FinCEN, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic" (Jul. 30, 2020); FinCEN, "Ransomware Trends in Bank Secrecy Act Data between January 2021 and June 2021" (Oct. 15, 2021); and FinCEN, "Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021" (Nov. 1, 2022).
9. According to media reports and law enforcement sources, a significant number of scammers who contact victims are likely victims themselves of human and labor trafficking rings operated by criminal organizations and are perpetrating such activity against their will. *See* May 2023 FBI PSA, *supra* note 6.
10. FBI PSA, "Cryptocurrency Investment Schemes" (October 2022 FBI PSA) (Oct. 3, 2022).

profile which showcases wealth and an enviable lifestyle.[11] Once the scammer elicits a response from a victim, the scammer will communicate with them over time to establish trust and build a relationship.[12]

The "Investment" Sales Pitch

Once trust or a relationship has been established, the scammer will introduce the victim to a supposedly lucrative investment opportunity in virtual currency and direct them to use virtual currency investment websites or applications designed to appear legitimate, but which are fraudulent and ultimately controlled or manipulated by the scammer.[13] This includes the use of legitimate applications with third-party plugins that allow the scammer to manipulate or falsify information presented to the victim. A scammer may also request remote access to the victim's devices to register accounts with virtual currency service providers (*i.e.*, virtual asset service providers, or VASPs) on the victim's behalf, or instruct their victims to take screenshots of their device so that the scammers can walk them through the process of purchasing virtual currency. According to the FBI, many victims also report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards to purchase virtual currency. The use of virtual currency and virtual currency kiosks is also an emerging method of payment.[14] Once a victim acquires virtual currency, the scammer directs them to "invest" the funds through the investment websites or applications, although the funds are funneled to virtual currency addresses and accounts controlled by scammers and their co-conspirators.

Occasionally, a scammer will leverage high-pressure sales tactics such as telling their victim that they will lose out on the opportunity if they do not invest by a certain deadline.[15] A scammer may also encourage the victim to bring their friends and family to invest into the scheme. In more recent iterations, the scammer will invite the victim to join online or mobile games, advertised as "play-to-earn" games offering financial incentives to players, but which in reality are fake gaming applications created by the scammer to steal virtual currency from players.[16]

The Promise of Greater Returns

Once the victim invests with the scammer, the scammer will show the victim extraordinary returns on the investment that have been fabricated.[17] The scammer may even allow the victim to withdraw a small amount of that investment to further build the victim's confidence before urging

11. *See* Michigan AG Alert, *supra* note 6.
12. USSS Alert, *supra* note 2, and October 2022 FBI PSA, *supra* note 10.
13. October 2022 FBI PSA, *supra* note 10, and March 2023 FBI PSA, *supra* note 7.
14. October 2022 FBI PSA, *supra* note 10.
15. FBI PSA, "Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams" (September 2021 FBI PSA) (Sept. 16, 2021).
16. FBI PSA, "Criminals Steal Cryptocurrency through Play-to-Earn Games" (Mar. 9, 2023).
17. October 2022 FBI PSA, *supra* note 10.

the victim to invest more.[18] Victims have been known to liquidate holdings in tax-advantaged accounts or take out home equity lines of credit (HELOC) and second mortgages on their homes in order to increase their investments.

The Point of No Return

When a victim's pace of investment slows or stops, the scammer will use even more aggressive tactics to extract any final payments. The scammer may present the victim with supposed losses on the investment and encourage them to make up the difference through additional deposits. If the victim attempts to withdraw their investment, the scammer may demand that the victim pay purported taxes or early withdrawal fees.[19] Once the victim is unable or unwilling to pay more into the scam, the scammer will abruptly cease communication with the victim, taking the victim's entire investment with them.

Case Study: Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency Pig Butchering Scheme

In November 2022, the U.S. Attorney's Office for the Eastern District of Virginia announced the seizure of seven domain names used in a pig butchering scam. According to court records, from at least May through August 2022, scammers induced five victims in the United States by using the seven seized domains, which were all spoofed domains of the Singapore International Monetary Exchange. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters or hackers seek to persuade individuals that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. The scammers convinced the victims that they were investing in a legitimate cryptocurrency opportunity. After the victims transferred investments into the deposit addresses that the scammers provided through the seven seized domain names, the victims' funds were immediately transferred through numerous private wallets and swapping services in an effort to conceal the source of the funds. In total, the victims lost over $10 million.[20]

18. September 2021 FBI PSA, *supra* note 15.
19. September 2021 FBI PSA, *supra* note 15.
20. DOJ, U.S. Attorney's Office, Eastern District of Virginia Press Release, "Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency 'Pig Butchering' Scheme" (Nov. 21, 2022).

Red Flag Indicators

FinCEN, in consultation with law enforcement, has identified the following indicators to help detect, prevent, and report potential suspicious activity related to pig butchering. As no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of pig butchering. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate.

Behavioral Red Flags

1. A customer with no history or background of using, exchanging, or otherwise interacting with virtual currency attempts to exchange a high amount of fiat currency from an existing or newly opened bank account for virtual currency or attempts to initiate high-value transfers to VASPs.

2. A customer mentions or expresses interest in an investment opportunity leveraging virtual currency with significant returns that they were told about from a new contact who reached out to them unsolicited online or through text message.[21]

3. A customer mentions that they were instructed by an individual who recently contacted them to exchange fiat currency for virtual currency at a virtual currency kiosk and deposit the virtual currency at an address supplied by the individual.[22]

4. A customer appears distressed or anxious to access funds to meet demands or the timeline of a virtual currency investment opportunity.

Financial Red Flags

5. A customer uncharacteristically liquidates savings accounts prior to maturation, such as a certificate of deposit, and then subsequently attempts to wire the liquidated fiat currency to a VASP or to exchange them for virtual currency.

6. A customer takes out a HELOC, home equity loan, or second mortgage and uses the proceeds to purchase virtual currency or wires the proceeds to a VASP for the purchase of virtual currency.

7. A customer receives what appears to be a deposit of virtual currency from a virtual currency address at or slightly above the amount that the customer previously transferred out of their virtual currency account. This deposit is then followed by outgoing transfers from the customer in substantially larger amounts.

21. October 2022 FBI PSA, *supra* note 10, and USSS Alert, *supra* note 2.

22. October 2022 FBI PSA, *supra* note 10.

8. Accounts with large balances that are inactive or have limited activity begin to show constant, uncharacteristic, sudden, abnormally frequent, or significant withdrawals of large amounts of money being transferred to a VASP or being exchanged for virtual currency.

9. A customer sends multiple electronic funds transfers (EFTs) or wire transfers to a VASP or sends part of their available balance from an account or wallet they maintain with a VASP and notes that the transaction is for "taxes," "fees," or "penalties."[23]

10. A customer with a short history of conducting several small-value EFTs to a VASP abruptly stops sending EFTs and begins sending multiple high-value wire transfers to accounts of holding companies, limited liability corporations, and individuals with which the customer has no prior transaction history. This is indicative of a victim sending trial transactions to a scammer before committing to and sending larger amounts.

Technical Red Flags

11. System monitoring and logs show that a customer's account is accessed repeatedly by unique IP addresses, device IDs, or geographies inconsistent with prior access patterns. Additionally, logins to a customer's online account at a VASP come from a variety of different device IDs and names inconsistent with the customer's typical logins.

12. A customer mentions that they are transacting to invest in virtual currency using a service that has a website or application with poor spelling or grammatical structure, dubious customer testimonials, or a generally amateurish site design.[24]

13. A customer mentions visiting a website or application that is purported to be associated with a legitimate VASP or business involved in investing in virtual currency. The website or application shows warning signs such as a web address or domain name that is misspelled in such a manner as to resemble that of another business, a recently registered web address or domain name, no physical street address, international contact information, or contact methods that include only chat or email.[25]

14. A customer mentions that they downloaded an application on their phone directly from a third-party website, rather than from a well-known third-party application store or an application store installed by the manufacturer of the device.

15. A customer receives a large amount of virtual currency such as ether at an exchange, subsequently converts the amount to a virtual currency with lower transaction fees such as TRX, and then abruptly sends it out of the exchange.

23. *See* NJ AG Press Release, *supra* note 5.

24. USSS Alert, *supra* note 2.

25. October 2022 FBI PSA, *supra* note 10. Another indicator is that the supposedly legitimate business is not registered with FinCEN as a money services business (MSB). MSB registrations may be searched online at: https://www.fincen.gov/msb-registrant-search.

Pig Butchering Fraud Reporting

In addition to filing a SAR, financial institutions are encouraged to refer their customers who may be victims of pig butchering to the FBI's IC3: https://www.ic3.gov/, and may also refer their customers to the Securities and Exchange Commission's tips, complaints, and referrals (TCR) system to report investment fraud: https://www.sec.gov/tcr.

In the case of elder victims of pig butchering, financial institutions may also refer their customers to DOJ's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions
Suspicious Activity Reporting
Other Relevant BSA Reporting
USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including pig butchering.[26] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[27]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[28] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[29] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A

26. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
27. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.
28. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
29. *Id.; see also* FinCEN, "Suspicious Activity Report Supporting Documentation" (Jun. 13, 2007).

financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

When filing a SAR in connection with this alert, FinCEN requests that financial institutions include the key term "**FIN-2023-PIGBUTCHERING**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial Institutions should also select "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[30]

Inclusion of Technical Cyber Indicators: When submitting a report pursuant to this alert, financial institutions should include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields on the SAR form or as part of the attachment field. Any data or information that helps identify the activity as suspicious can be included as an indicator. Examples include chat logs, phone numbers, and social media usernames used by the scammer; suspicious email addresses; type of virtual currency and digital assets involved; virtual currency and / or digital asset addresses and transaction hashes native to the blockchain(s) involved; apps used; and the URL, domain, and IP address of the service the victim was instructed to deposit into.

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this alert. These include obligations related to the Currency Transaction Report (CTR),[31] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[32] Report of Foreign Bank and

30. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).

31. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.

32. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 CFR § 1010.330; 31 CFR § 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.

Financial Accounts (FBAR),[33] Report of International Transportation of Currency or Monetary Instruments (CMIR),[34] Registration of Money Services Business (RMSB),[35] and Designation of Exempt Person (DOEP).[36] These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this alert, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**FIN-2023-PIGBUTCHERING**" in the "**Comments**" section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing pig butchering and related activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[37] FinCEN strongly encourages such voluntary information sharing.

For Further Information

Questions or comments regarding the contents of this alert should be sent to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

33. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 CFR § 1010.350; FinCEN Form 114.
34. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 CFR § 1010.340.
35. A form filed to register a MSB with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.
36. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.
37. *See* FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).