



Financial Trend Analysis

Digital Asset Investment Scams: 2023-2025 Threat Pattern & Trend Information

September 2026



Digital Asset Investment Scams: 2023-2025 Threat Pattern & Trend Information

This Financial Trend Analysis (FTA) focuses on patterns and trends identified in Bank Secrecy Act (BSA) data linked to digital asset investment scams. This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020, which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish threat pattern and trend information.¹ On September 8, 2023, FinCEN issued an “Alert on Prevalent Virtual Currency Investment Scam Commonly Known as ‘Pig Butchering,’” which provided behavioral, financial, and technical red flags to help financial institutions identify and report suspicious activity involving digital asset investment scams. This Financial Trend Analysis shares patterns and observations from BSA reporting involving digital asset investment scams since the Alert was published, up to the end of 2025.

Executive Summary: FinCEN analyzed 33,904 BSA reports involving suspected digital asset investment scam-related activity filed between 8 September 2023 and 31 December 2025 (the “review period”). These reports identified approximately \$12.7 billion in financial activity tied to suspected digital asset investment scams. Based on these reports, FinCEN observed a rising rate of suspected scam activity. Illicit actors engaging in these scams used complex typologies to defraud victims while using various types of financial institutions to launder illicit proceeds.

- *MSB’s and Depository Institutions’ Reporting Volume and Financial Activity Growing at an Accelerating Rate:* Money Services Businesses (MSBs), predominantly those related to the digital asset sector, and depository institutions reported 96 percent of all suspected digital asset investment scam-related BSA reports analyzed by FinCEN during the review period. On average, each month FinCEN received 10.9 percent more suspected digital asset investment scam-related reports than the prior month, and 18 percent more reported total funds involved in suspected digital asset investment scam-related financial activity during the review period.
- *New Methodologies Combined with Common Tactics:* Analysis of BSA reporting indicated the use of a variety of well-known fraud tactics. Illicit actors often used assumed names or identities to pose as potential romantic partners, new friends, or new business partners to target scam victims. Scammers often created websites and mobile applications that imitated legitimate investment services to carry out their criminal activity. Because scammers rely on multiple institutions to receive or transfer scam proceeds, most filing institutions reported only a snapshot of different phases in a scam’s lifecycle.

1. The Anti-Money Laundering Act of 2020 was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).

- *Digital Asset Investment Scams Target Americans Throughout the United States:* Individuals of all ages across all 50 states and several U.S. territories were the target of suspected digital asset investment scams, according to BSA reports. According to the 2020 U.S. census, older adults make up approximately 24.4 percent of the population, and approximately 25 percent of BSA reports involved both digital asset investment scams and elder financial exploitation, suggesting older Americans are not at a higher risk of victimization than other age demographics.

Scope and Methodology:

FinCEN examined BSA reports referencing the key term highlighted in FinCEN’s 2023 Prevalent Virtual Currency Investment Scam Alert (FIN-2023-PIGBUTCHERING).² Between 8 September 2023 and 31 December 2025 (the “review period”), financial institutions submitted 33,904 BSA reports referencing the key term mentioned in the Alert, involving \$12.7 billion in reported suspected digital asset investment scam-related financial activity.³ FinCEN conducted both manual and automated review of these reports to determine prominent trends and patterns. FinCEN identified these BSA reports using the filing date, rather than the date of the underlying activity. Accordingly, these reports may refer to incidents that occurred prior to the review period.

A Note About Suspicious Activity Reporting

Suspicious activity reporting reflects only suspicious activity that has been identified and reported and therefore should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. These suspicious activity amounts may also include transfers between accounts, typos, and errors as submitted by filers. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, and transfers between accounts. The reported suspicious activity in any individual BSA filing may include both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity and therefore may reflect cumulative transactions from a single filer involving the same subject.

2. See “FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as ‘Pig Butchering’” FinCEN Alert #FIN-2023-Alert005, 8 September 2023, https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.
3. Amounts associated with these BSA reports may include attempted transactions and payments that were unpaid. This figure also includes BSA reports that describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity. These suspicious activity amounts may also include duplicates, counting both inbound and outbound transactions, transfers between accounts, typos, and errors as submitted by filers. FinCEN’s analysis excluded a small number of reports involving outlier dollar values.

What are Digital Asset Investment Scams?

Digital asset investment scams are a type of confidence scheme using complex fake personas and social engineering techniques to manipulate individuals into investing in digital assets with promises of large returns. The intent of these schemes is to defraud victims of money they “invest” in digital assets. These scams are also known by other names, such as “pig butchering,” “romance baiting,” “cryptocurrency confidence scheme,” or “virtual asset investment fraud.”⁴

The scams typically begin with unsolicited or “wrong number” messages via text message, social media, dating sites, or messaging platforms. If potential victims respond to the message, the scammers will use fake personas to develop a seemingly deep personal connection with the victims over time.⁵ Once a trusted relationship has been established, the scammer will introduce the victim to a supposedly lucrative digital asset investment opportunity. The scammer will direct the victim to send funds, either fiat or digital asset, to an account or address affiliated with the scammer while the victim believes the funds are being used to invest in digital assets. Using a combination of inducement payments (when the scammer sends the victim small amounts of money to indicate returns on the investments) or false information, the victim will be led to believe their investments are rapidly growing. The scammer will entice the victim to invest more using the allure of seemingly large investment gains and emotionally manipulative tactics informed by their deep personal connection. In some instances, victims are directed to liquidate investment accounts or personal savings accounts, take out home equity lines of credit and second mortgages, or solicit funds from friends and family. Victims attempting to withdraw their supposed gains are led to believe they must pay taxes or fees before being granted access to their funds. When a victim is no longer willing or able to provide more funds, the scammer will cease communications with the victim.

4. See “INTERPOL urges end to ‘Pig Butchering’ term, cites harm to online victims,” International Criminal Police Organization, <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-urges-end-to-Pig-Butchering-term-cites-harm-to-online-victims>.
5. See “FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as ‘Pig Butchering’” FinCEN Alert #FIN-2023-Alert005, 8 September 2023; see also Operation Shamrock, “The Pig Butchering Lifecycle,” <https://www.operationshamrock.org/education/pig-butchering-lifecycle>.

Money Services Businesses Report Most Frequently; Depository Institutions Report Largest Dollar Amounts

Approximately 1,300 different financial institutions filed 33,904 BSA reports involving suspected digital asset investment scams with FinCEN during the review period. These financial institutions reported approximately \$12.7 billion in suspected digital asset investment scam-related financial activity. FinCEN received reports from Money Services Businesses (MSBs), depository institutions, securities and futures firms, and financial institutions categorized as “Other.”⁶

MSBs – predominantly those engaged in the digital asset sector – filed 18,568 BSA reports, or 55 percent of all suspected digital asset investment scam reports during the review period. MSBs identified over \$5.5 billion of all suspected scam-related financial transactions reported to FinCEN during the review period. These MSBs frequently reported victims sending digital assets to scammer-affiliated addresses. Some of these reports aided law enforcement by linking networks of scammers and victims to common digital asset addresses. MSB filings overall provided further insight into the laundering process for scam proceeds, identifying intermediary points that scammers appear to be using to transfer funds.

Depository institutions filed 13,810 BSA reports, or approximately 41 percent, of all suspected digital asset investment scam reports during the review period. Depository institutions reported approximately \$6.4 billion of all suspected digital asset investment scam-related financial activity. Depository institutions often detected schemes when a victim sent funds to an MSB in the digital asset sector to purchase digital assets, or when a customer sent a wire transfer to a scam-affiliated beneficiary, frequently referencing digital asset investments. Depository institutions also reported large transfers between victim accounts, including applications for loans, second mortgages, or other types of financing; and suspicious interactions with customers they believe were involved in digital asset investment scams such as the victim implying they have a trusted investment advisor but refusing to discuss anything about the advisor or certainty in the outcome of their investment.

Financial institutions categorized in FinCEN reporting as “Securities and Futures Firms” filed 1,504 BSA reports involving suspected digital asset investment scam activity during the review period. Securities and futures firms reported over \$784.5 million in suspected digital asset investment scam-related financial activity. Securities and futures firms most frequently reported when victims liquidated their investment accounts to fund digital asset purchases, attempted wire transfers to scammer-affiliated accounts, or made large transfers out of investment accounts.

6. “Other” is selected by the filer when the filer believes no other type of financial institutions apply to their type of business. For the purposes of this analysis, FinCEN categorized financial institutions that file as “Other” into the primary financial institution category associated with the underlying products and services offered. The remaining “Other” financial institution types include real estate holding companies or precious metals dealers. There were 22 suspected digital asset investment scam-related reports that were filed by institutions categorized as “Other” during the review period. These filings reported over \$8.4 million in financial activity reportedly related to investment scams. For more information, see “SAR Filing by Industry,” Financial Crimes Enforcement Network, <https://www.fincen.gov/reports/sar-stats/sar-filings-industry>.

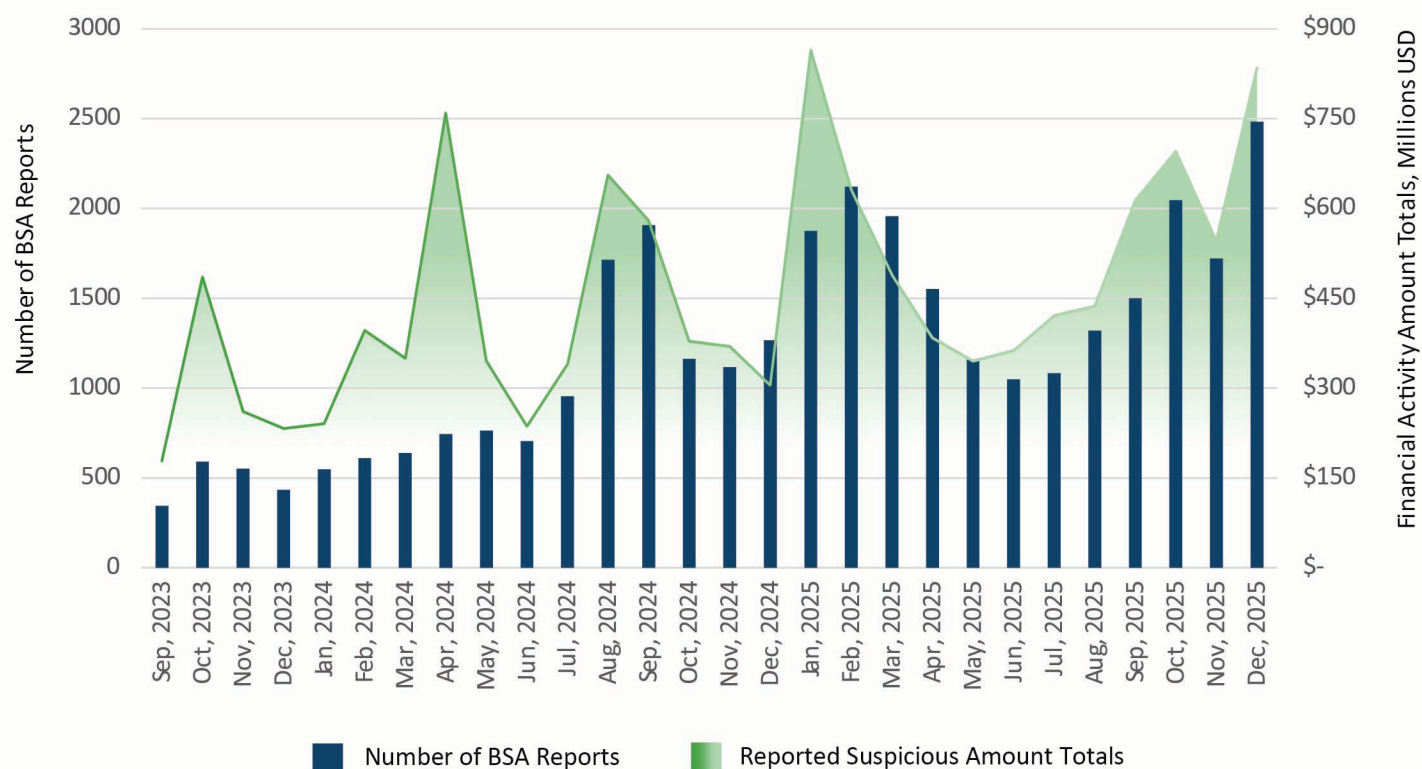
Figure 1: BSA Reports by Filer Type

Filing Institution Type	Reports Filed	Percent of All Filings	Activity Amounts
Money Services Businesses (MSBs)	18,568	54.8%	\$5.5 billion
Depository Institutions	13,810	40.7%	\$6.4 billion
Securities or Futures Firms	1,504	4.4%	\$784.5 million
Other	22	0.1%	\$8.4 million
Total	33,904	100%	\$12.7 billion

Volume and Value of Digital Asset Investment Scams Increasing Month Over Month

On average, the number of monthly reports and the total amount of financial activity grew significantly between September 2023 and December 2025, though not at a consistent rate. The number of BSA reports filed with FinCEN increased by an average of 10.9 percent month-over-month, and the total dollar value of reported suspected digital asset investment scam-related financial activity grew, on average, by 18 percent month-over-month during the review period. In October 2023—the first full month of reporting after the Alert was issued—FinCEN received 590 BSA reports, involving financial activity worth over \$485.7 million in suspected digital asset investment scam-related financial transactions. In December 2025, the last full month of the review period, FinCEN received 2,482 BSA reports, involving financial activity worth over \$833.5 million in suspected digital asset investment scam-related financial transactions.⁷ Despite the general increase in average reporting, there were significant fluctuations in the number of reports and financial amount totals. For example, August 2024 saw an 80 percent increase in digital asset investment scam reports from the prior month, whereas September 2024 only saw an 11 percent increase and October 2024 reported a 19 percent decrease.

7. This may indicate an increased adoption of the Alert's key term and does not necessarily indicate there is an accelerating rate of investment scams.

Figure 2: BSA Reports and Financial Activity Amount Totals, by Filing Month

Digital Asset Investment Scam Methodologies

Victims Finance Investments Using Variety of Sources

Analysis of BSA reporting indicates a wide range in amounts lost per victim, with some losing their life savings to suspected digital asset investment schemes. Scammers use the emotional connection they formed with the victim, knowledge of the victim's finances, and the promise of easy returns to manipulate the victim into continuing to invest increasingly larger amounts. In extreme cases, this forces victims to resort to financial options with significant negative repercussions, such as taking out loans or incurring penalties by withdrawing from their retirement accounts.

- An MSB involved in the digital assets sector reported an older adult victim transferred nearly \$640,000 from her retirement fund to send to a suspected scammer in connection with an apparent digital asset investment scheme. The victim stated she met an individual over social media who instructed her to invest in an apparently fictitious digital asset-related company.
- A depository institution reported a customer withdrew nearly \$150,000 from his retirement account, initiated a home equity line of credit, took out a personal loan, and refinanced his mortgage to obtain funds to transfer to suspected scammers in another alleged digital asset

investment scam. The depository institution also noted the victim was denied for personal loans twice during the apparent scam. The victim claimed to be following his purported romantic partner's investment advice by sending her the newly purchased digital assets.

- A depository institution reported a victim lost more than \$1 million to a digital asset investment scam over the course of a six-month period. The depository institution noted the victim used proceeds from the sale of a deceased family member's home and took out a second mortgage on her own home, as well as withdrawing from her retirement savings and from a business account to finance some of her so-called "investments."
- In another case, a depository institution reported a victim persuaded a friend to join him in a digital asset investment opportunity, which ultimately resulted in both individuals losing several million dollars. The victim took his own life shortly after learning their funds were lost to an apparent investment scam.

Digital Asset Investment Scams and Self-Harm

Scam victims can be extremely distressed upon learning they were scammed. Some reporting suggests that digital asset investment scam victims are potentially at risk of engaging in self-harm. Law enforcement partners, open-source reporting, and BSA reports identified instances of scam victims taking or attempting to take their own lives. Victims and those around them are encouraged to seek mental health services and support. Resources such as the 988 Suicide and Crisis Lifeline are available to anyone considering self-harm.⁸

Two Distinct Tactics, Techniques, and Procedures Identified

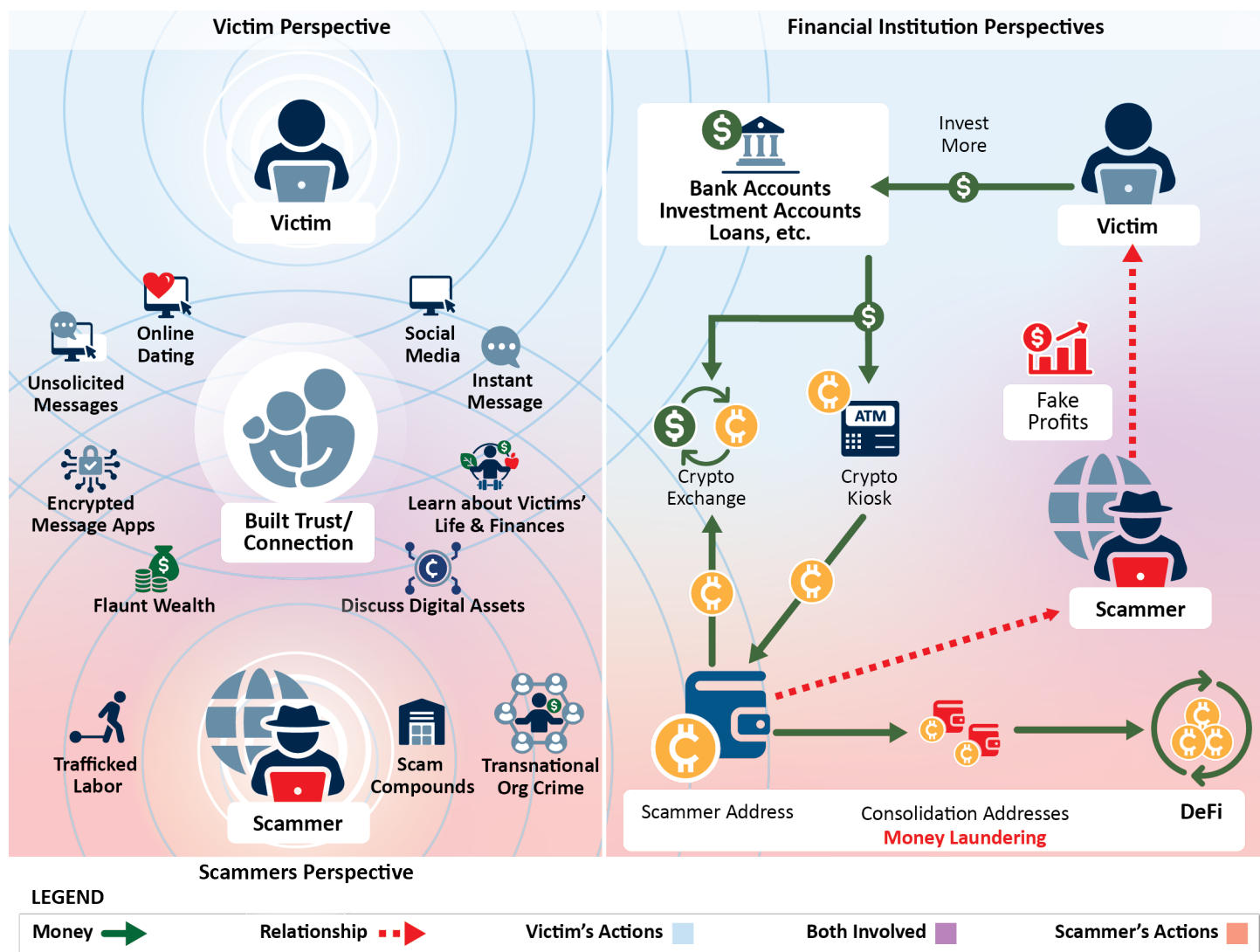
FinCEN analysis of BSA reporting identified two distinct tactics, techniques, and procedures (TTPs) digital asset investment scammers rely on to receive funds from their victims. Based on FinCEN's analysis of BSA reporting, scammers often instruct their victims to open accounts with MSBs offering digital asset services to purchase specific digital assets. Then, the victim is told to send these funds to a digital asset address controlled by the scammers. Scammers often use these addresses to accumulate funds from several victims before laundering the funds through multiple digital asset transactions. Financial institutions have reported difficulty in detecting this TTP, because the victim technically maintains control of funds in the accounts at the MSB before any scam proceeds are transferred to scammer-controlled addresses.

In other, less-frequently reported digital asset investment scheme TTPs, victims were directed to send fiat-denominated funds through a wire transfer or Automated Clearing House transaction to another, fiat-denominated financial account affiliated with the scammers. Scammers often leveraged realistic-looking mobile apps, websites, or social media posts to convince victims these fund transfers were digital asset purchases; however, the victims never actually took custody of any digital assets. Scammers often used these fiat-denominated funds to purchase digital assets.

8. 988 Lifeline, <https://988lifeline.org/>.

Scammers next laundered these digital asset-denominated funds through multiple transactions using several digital asset addresses. In this TTP, the victims do not purchase and at no point have control of digital assets.

Figure 3: Example Flow of Digital Asset Investment Funds



Centralized Exchanges Most Frequent Onboarding Method for Digital Assets; Kiosks Also Used

According to BSA reporting, suspected digital asset investment scammers frequently relied on MSBs, namely centralized digital asset exchanges, to facilitate a victim's purchase of digital assets. The scammers typically instruct their victims to purchase digital assets from reputable centralized exchanges and to then send these funds directly to unattributed addresses off platform. In some

instances, scammers instruct their victims to use digital asset kiosks to purchase digital assets with cash in order to send these funds directly to scammer-controlled unattributed addresses.⁹

Similarities Across Scam TTPs Include Information Manipulation, Digital Assets, and Reliance on Unattributed Addresses

Digital asset investment scammers rely on misleading their victim into believing their so-called “investments” grow in value over time. This stage of manipulation takes various forms based on BSA information.

- In some instances, scammers send inducement payments that indicate relatively large returns on small early “investments” in order to incentivize victims to make increasingly larger “investments.” BSA reporting indicates the total dollar amounts involved in these inducement payments vary greatly but are typically sent as digital assets and occur in the early phases of the scam.
- In other instances, scammers will send information to victims through encrypted messaging platforms, custom-built mobile applications, or websites to show the victims that their “investments” have grown.
- BSA reporting also showed that some scammers used legitimate third-party mobile applications or platforms to create the illusion of investment gains. Scammers opened brokerage accounts with the third-party investment platforms and controlled funds on behalf of the victim.
- Some reports show scammers communicated with their targets entirely using messaging apps, forgoing the use of investment platforms, mobile applications, or scam websites.

Financial institutions reported suspected digital asset investment scammers used at least 22 different digital assets to receive or transfer scam proceeds. Most BSA filings noted the use of popular or well-known digital assets. Ethereum, Tether (USDT), and USD Coin (USDC) were the most frequently used by both victim and scammer, though many BSA reports filed by depository institutions did not specify the type of digital assets involved in the scam. Fake or nonexistent digital assets were rarely reported. FinCEN analysis of BSA reports using commercial blockchain analytics tools indicated that regardless of the asset used in the original investment, scammers nearly always exchanged scam proceeds for stablecoins, almost exclusively USDT.

9. Kiosks—often called convertible virtual currency kiosks or Bitcoin automated teller machines (ATMs)—are ATM-like electronic terminals that allow users to exchange cash and virtual currency. See “FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity,” FinCEN Advisory #FIN-2025-NTC1, 4 August 2025, <https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf>.

Common Addresses Reused to Collect Scam Proceeds From Multiple Victims

BSA reporting indicates that scammers often use the same digital asset addresses to collect scam proceeds from multiple victims at the same time. Some MSBs reported they identified suspected digital asset investment scam-related activity by observing multiple apparent victims sending funds to the same suspicious addresses. Scammers controlling these common sets of suspicious addresses then sent scam proceeds to decentralized finance protocols or foreign-based digital asset exchanges, according to FinCEN's analysis of BSA reports and commercial blockchain analytics tools.¹⁰

Scammers Adopt Techniques Common to Other Fraud Schemes

Digital asset investment schemes incorporate TTPs commonly observed in other fraud schemes, like advance fee schemes, fraud recovery scams, bank impersonation scams, government impersonation scams, and romance scams, according to analysis of BSA reports. As a result, digital asset investment scams are often difficult for financial institutions to distinguish from other fraud schemes.

- According to BSA reporting, suspected scammers will insist that a victim cannot withdraw their investments without paying “fees” or “taxes” on their supposed gains. Requiring victims to pay an advance fee is a common TTP in fiat investment schemes and lottery scams. BSA reporting indicates that an advance fee request often marks the final stages of the scam. Some victims reported to financial institutions they realized they were victimized by an apparent digital asset investment scam after the scammer demanded payment to release funds.
- BSA reporting identified a small number of instances where scammers may have attempted to further defraud scam victims by posing as an “asset recovery service.” After a victim realizes they were scammed, the perpetrators of the investment scam, or other unrelated scammers posing as recovery specialists, revictimized victims by offering to recover stolen funds for an additional fee. FinCEN notes this TTP is often seen in timeshare fraud scams.
- Scammers used numerous methods to initially contact and further communicate with victims. These communication methods often included unsolicited messages through social media apps, encrypted messaging services, dating websites, SMS text messages, job-searching websites, telephone calls, and emails. According to FinCEN analysis of BSA reports, scammers frequently used one method to make initial contact with the victim, and then shifted to another method of communication, typically an encrypted messaging service.
- Scammers often attempted to establish trust with their victims by manipulating them into believing they were in a close personal relationship. Financial institutions frequently noted that scam victims often justified changes to their normal financial activity based on guidance from a romantic partner, close friend, investment guide, mentor, or business partner they met online.

10. Decentralized finance or “DeFi” broadly refers to a variety of financial products, services, activities, and arrangements supported by smart contract-enabled distributed ledger technology.

FinCEN Analysis Provides Additional Insights into Victims, Money Laundering Methods, and Top Financial Intermediaries

Digital Asset Investment Scams Target Americans of All Ages Throughout the United States

BSA reports indicated older adults, typically defined as those aged 60 or above, did not represent a disproportionate amount of digital assets investment scam victims or losses. Financial institutions indicated involvement of elder financial exploitation in 10,082, or nearly 25 percent, of the digital asset investment scam-related BSA reports filed during the review period. Older adults make up approximately 24.4 percent of the national population based on the 2020 Census.¹¹ FinCEN identified digital asset investment activity involving victims located in all 50 U.S. states, the District of Columbia, Guam, the Northern Mariana Islands, and Puerto Rico.

Victims Finance Investments Using a Variety of Financial Services including Retirement Accounts

Victims often withdrew funds from numerous sources to finance their “investments.” Analysis of BSA reporting indicates victims typically started investing with readily available funds in personal checking or savings accounts, and then turned to other sources of funds, including withdrawals from retirement or investment accounts, the sale of securities or other investment assets, or taking on debt through home equity lines of credit, credit card advances, and personal loans. A smaller portion of scam victims used funds they solicited from others to obtain more funds to send when the victim began to deplete their funds or other assets. These were received as incoming wire transfers, peer-to-peer transfers, and cash deposits before purchasing digital assets and transferring them to scammers, according to BSA reports.

Scams Often Detected After Victims Lost Funds

Financial institutions often reported to FinCEN that they became aware of suspected digital asset investment-related financial activity after the scam had concluded, or when a victim lost a significant amount of money but were still manipulated to send more funds to scammers. When financial institutions detected the scam early, they often attempted to stop the victim—typically a client—from sending funds to the scammers. Financial institutions often reported that victims would insist on completing the financial transaction, despite the risk. In a small number of BSA reports, financial institutions reported either successfully dissuading victims from sending funds, or a victim changing their mind and funds being successfully recalled after being sent to cooperative third-party financial institutions before scammers were able to further transmit these funds elsewhere.

11. U.S. Census Bureau, “The Older Population: 2020” May 2023, <https://www2.census.gov/library/publications/decennial/2020/census-briefs/c2020br-07.pdf>.

FinCEN's Rapid Response Program

FinCEN's Rapid Response Program (RRP) is a partnership between FinCEN, U.S. law enforcement, and foreign partners working together to help victims and their financial institutions recover stolen funds sent abroad as the result of cyber-enabled fraud. As the financial intelligence unit (FIU) of the United States, FinCEN uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to stop and repatriate the fraudulent transactions using authorities under their respective legal and regulatory frameworks. Since its inception in 2015, RRP has facilitated the interdiction of \$1.8 billion and the recovery of over \$1 billion in stolen proceeds on behalf of 5,790 U.S. victims.¹²

Cyber Scam Compounds

Open-source publications, law enforcement partners, and international organizations indicate that many scammers are likely human trafficking victims coerced into conducting these scams by transnational criminal organizations (TCOs).¹³ TCOs have reportedly converted hotels and casinos into prison-like compounds to house tens of thousands of trafficked individuals who are forced to conduct scam activity for extended periods of time each day, based on media reporting.¹⁴ Frequently, TCOs use fake employment opportunities listing lucrative salaries for English speakers in Southeast Asia, the Middle East, Latin America, or Eastern Europe to lure unsuspecting individuals to travel to the area near the compound. These job opportunities tend to have elaborate procedures that included interviews, assessments, and individuals posing as marketers and human resource specialists, among other roles.¹⁵

Once these job seekers arrive at these compounds, TCOs confiscate their passports and mobile phones and move them into secured sections of these compounds to start scamming. Trafficked victims are subject to harsh treatment in the compounds, including forced labor, beatings, electrocution, withholding of food, water, and medical treatment, and a host of other human rights violations.¹⁶ These compounds are primarily located in remote areas or Special Economic Zones in Cambodia, Laos, and Burma. The United Nations estimates that hundreds of thousands of trafficked victims are held at compounds in Southeast Asia, primarily Cambodia

12. FinCEN Rapid Response Program Fact Sheet, <https://www.fincen.gov/system/files/2026-04/RRPFactSheet.pdf>.

13. See "Inflection Point: Global Implications of Scam Centres, Underground Banking, and Illicit Online Marketplaces in Southeast Asia," April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

14. See "They Were Forced To Scam Others Worldwide. Now Thousands Are Detained on the Myanmar Border," 10 March 2025, <https://www.pbs.org/wgbh/frontline/article/scam-centers-trafficking-myanmar/>.

15. See "Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response," 2023, https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf.

16. See "Revealed: Leaked Chats Expose the Daily Life of a Scam Compound's Enslaved Work Force," 27 January 2026, <https://www.wired.com/story/the-red-bull-leaks/>.

and Burma.¹⁷ Some open-source research suggests TCOs have spread the scam compound methodology to countries outside Southeast Asia, including Latin America, the Middle East, and Africa. Open-source reporting also indicates scammers are adopting artificial intelligence technology, such as deepfakes and large language models, to enhance their criminal operations.

The information in this report is based on suspected digital asset investment scam-related information obtained from analysis of BSA data, and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to FinCEN at www.fincen.gov/contact/.

17. See Inflection Point, *supra* note 13.