

Cryptocurrency Crimes: Common Schemes and Documentation Guidance for Victims

Critical Intelligence for Decision Makers

Executive Summary

Financially motivated threat actors conduct cryptocurrency scams, often targeting specific populations such as the elderly, to generate revenue and fuel criminal enterprises. Cryptocurrency facilitates decentralized, fast, and irreversible global transactions, serving as an ideal exploitation vector for financial fraud. In 2024, the Federal Bureau of Investigation (FBI) received 149,686 complaints regarding cryptocurrency fraud, with reported losses totaling \$9.3 billion.¹ Cryptocurrency investment fraud accounted for roughly 62 percent of cryptocurrency losses in 2024, with other common schemes including cryptocurrency job scams, blackmail and extortion scams, market manipulation scams, and cryptocurrency recovery scams.^{2, 3, 4, 5} Individuals should be familiar with red flag indicators of common cryptocurrency crimes, and if identified, be prepared to quickly document and report key transaction information to U.S. law enforcement. According to the FBI, “rapid and accurate” reporting is essential for enabling U.S. law enforcement to investigate and mitigate cryptocurrency fraud.⁶

In the event of a cryptocurrency crime, victims should take the following steps:

1. Immediately cease all contact with the suspected threat actor(s) and stop sending funds.
2. Capture key transaction information, including cryptocurrency types and amounts, cryptocurrency addresses, transaction hashes, and transaction dates and times. This information enables U.S. law enforcement to trace cryptocurrency transactions, send requests to cooperative virtual asset service providers (VASPs),¹ and attempt recovery of financial losses.
3. Document key transaction information in the Center for Internet Security’s (CIS’s) Cryptocurrency Crime Documentation Form, which is provided on page five, and use the completed form to file a complaint with the FBI’s [Internet Crime Complaint Center \(IC3\)](#).

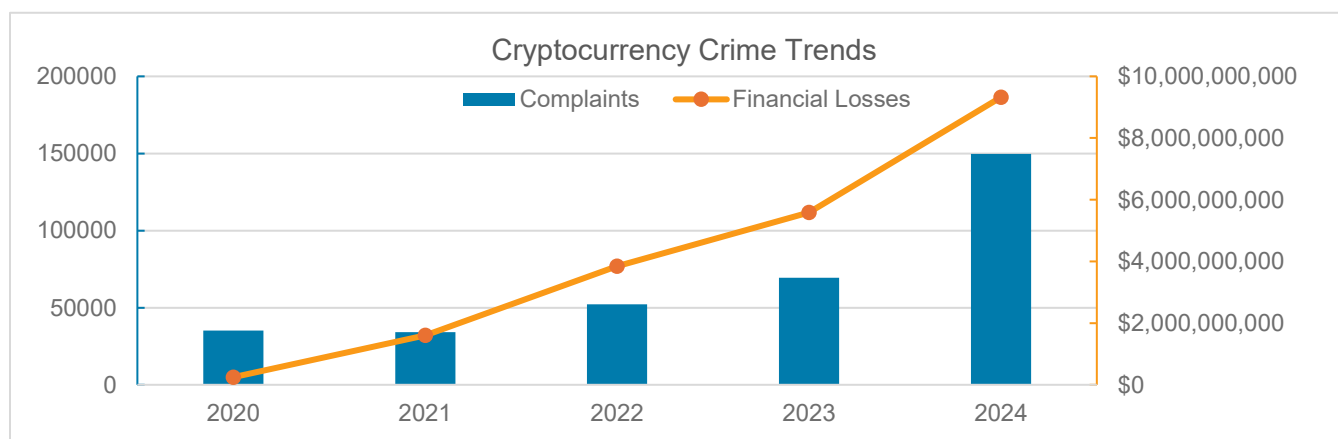


Figure 1: Cryptocurrency crime complaints and financial losses from 2020 to 2024. These figures likely underrepresent the totality of financial losses, given these statistics only account for crimes reported to the FBI.^{7, 8, 9, 10, 11}

¹ Virtual asset service providers (VASPs) are organizations that facilitate the use of cryptocurrency, including cryptocurrency exchanges and cryptocurrency wallet providers.

Common Cryptocurrency Crimes

Cryptocurrency Investment Fraud

During a cryptocurrency investment fraud scam, also known as a pig butchering scam, threat actors contact victims via social media, text messages, or dating sites; work to build trust and rapport; and then encourage victims to invest in cryptocurrency using fraudulent applications or websites.¹² Initially, these investments appear extremely profitable and victims may be able to withdraw their earnings, enticing victims to continue investing.^{13, 14} However, once victims invest a significant amount, their accounts suddenly become frozen and require taxes or fees to regain access. According to the FBI, at this point in the scam “there is usually nothing the victim can do: the scammers will never unlock the funds and it’s likely they have already withdrawn those funds into criminally controlled cryptocurrency wallets inaccessible to the victim.”¹⁵ These scams are primarily conducted by Southeast Asian criminal organizations, who force labor trafficking victims to contact potential targets.¹⁶ In 2024, the FBI received 41,557 cryptocurrency investment fraud complaints, resulting in approximately \$5.8 billion in financial losses.¹⁷

Individuals should be aware of the following red flag indicators of cryptocurrency investment fraud:

-  An online contact, who has never been met in-person, provides cryptocurrency investment advice and opportunities via encrypted messaging applications like WhatsApp or Telegram.
-  Cryptocurrency investments on unfamiliar websites or applications show rapid growth and exceptional returns.
-  Taxes and fees are suddenly required to regain access to cryptocurrency investments or to withdraw earnings.

Cryptocurrency Job Scams

In a cryptocurrency job scam, threat actors pose as employees at legitimate organizations to recruit victims for remote, online jobs.¹⁸ If a victim expresses interest in the position, threat actors will conduct online training before assigning the victim specific tasks to earn a salary or commission. According to the FBI, “these tasks vary from scheme to scheme – but they all require the victim to deposit their own money, via cryptocurrency or money transfers, into a platform for the job to be completed.”¹⁹ Initially, victims appear to make a profit and can withdraw their earnings. However, over the course of the scam, victims are required to deposit larger sums, until the deposit requirement becomes unfeasible. Once victims can no longer meet the deposit requirement, their accounts are frozen, and threat actors steal the entirety of their account balance.²⁰ According to the Federal Trade Commission (FTC), there have been “skyrocketing” cryptocurrency losses to job scams, with roughly \$41 million lost in the first half of 2024, compared to only \$21 million lost in all of 2023.²¹

Individuals should be aware of the following red flag indicators of cryptocurrency job scams:

-  An online contact, who has never been met in-person, reaches out via social media or encrypted messaging applications offering a remote, online job opportunity.
-  A remote, online job opportunity requires employees to deposit their own money, including cryptocurrency or money transfers, to perform job-related tasks.
-  A job opportunity instructs employees not to tell financial institutions, including banks and VASPs, about the employment tasks.

Blackmail and Extortion Scams

During a blackmail scam, threat actors send emails or physical mail to victims threatening to publish “embarrassing or compromising photos, videos, or personal information” unless they receive a cryptocurrency payment.²² Oftentimes, threat actors do not actually possess this information.²³ One of the most prolific cryptocurrency

blackmail scams is sextortion, where threat actors claim to have installed malware on victims' devices and recorded the victim watching pornographic material.²⁴ Threat actors demand a cryptocurrency payment to avoid sending the recording to the victims' friends and family. According to the FBI, extortion was the most reported cryptocurrency crime in 2024, with approximately \$33.5 million in financial losses.²⁵

Individuals should be aware of the following red flag indicators of blackmail and extortion scams:

-  Emails or physical mail use pressure tactics, intimidation, fear, or coercion to encourage recipients to send cryptocurrency payments.
-  Emails demanding cryptocurrency payments include information indicating the device has been infected with malware.
-  Emails or physical mail requesting cryptocurrency payments reference adult content, pornographic materials, or purported extramarital affairs.

Market Manipulation Scams

Market manipulation scams seek to impact the price of a cryptocurrency or token,² with one common tactic including pump-and-dump schemes.²⁶ According to the blockchain³ intelligence firm Chainalysis, "pump-and-dump schemes lure unsuspecting investors by driving up the price of an asset, often through coordinated hype, only for insiders to sell off their holdings at a peak, leaving unwitting holders of the asset with significant losses."²⁷ Chainalysis analyzed 40,521 tokens launched in 2022 and found roughly 24 percent had a price drop within the first week, indicating possible pump-and-dump activity.²⁸

Individuals should be aware of the following red flag indicators of market manipulation scams:

-  A newly launched cryptocurrency token shows a rapid price increase and an unexpected surge in trading volume.
-  A newly launched cryptocurrency token is advertised via online forums or social media and uses fraudulent news stories or manufactured celebrity endorsements.
-  A newly launched cryptocurrency token has limited information available online outside of social media.

Cryptocurrency Recovery Scams

Victims of cryptocurrency crimes, especially cryptocurrency investment fraud, are also vulnerable to cryptocurrency recovery scams.²⁹ Threat actors will contact cryptocurrency crime victims via social media, encrypted messaging applications, or online advertisements posing as businesses that can help victims recover stolen funds. These fraudulent businesses may impersonate or claim affiliation with U.S. law enforcement or law firms.^{30, 31} According to the FBI, "fraudulent businesses claiming to recover stolen funds charge an up-front fee and either cease communications after receiving an initial deposit or produce an incomplete or inaccurate tracing report and request additional fees to recover funds."³² This scam targets vulnerable populations, especially the elderly.³³

Individuals should be aware of the following red flag indicators of cryptocurrency recovery scams:

-  Purported cryptocurrency recovery businesses, law firms, or law enforcement organizations require payment via cryptocurrency or gift cards to recover stolen funds.
-  Purported cryptocurrency recovery businesses, law firms, or law enforcement organizations reference fake government or regulatory agencies to feign legitimacy.

² Tokens are assets built on top of existing blockchains that can be used for investments, transactions, or trading.

³ Blockchains are digital, public ledgers that record all cryptocurrency transactions.



Purported cryptocurrency recovery businesses, law firms, or law enforcement organizations advertise their asset recovery services on social media.

Cryptocurrency ATMs and Mounting Fraud

Cryptocurrency ATMs, also known as cryptocurrency kiosks, are electronic terminals that enable users to buy and sell cryptocurrency. According to the [FBI's 2023 Cryptocurrency Fraud Report](#), "the use of cryptocurrency kiosks to perpetrate fraudulent activity against the US population is increasing."

The [FBI's 2024 Internet Crime Report](#) details 10,956 complaints involving cryptocurrency ATMs, with estimated losses totaling \$246.7 million. Compared to 2023 figures, the FBI recorded a 99% increase in complaints (up from 5,500) and a 31% increase in financial losses (up from \$189 million).

Legitimate government and law enforcement agencies will never request payment via cryptocurrency ATMs, and individuals should be suspicious of any requests to withdraw large amounts of cash for conversion to cryptocurrency.

Key Documentation Information for Cryptocurrency Crimes

In the event of a cryptocurrency crime, victims should be prepared to capture key transaction information, including cryptocurrency types and amounts, cryptocurrency addresses, transaction hashes, and transaction dates and times. This information enables U.S. law enforcement to trace cryptocurrency transactions, send requests to cooperative VASPs, and attempt recovery of financial losses.



Cryptocurrency type: Note the type of cryptocurrency involved in the specified transactions. There are thousands of unique cryptocurrencies, but common cryptocurrencies include Bitcoin (BTC), Ethereum (ETH), and Tether (USDT).



Cryptocurrency amount: Document the amount of cryptocurrency involved in the relevant transactions (i.e. 0.75 BTC, 2 ETH). Also note the approximate value of the cryptocurrency in U.S. dollars, which can be calculated via a [cryptocurrency converter tool](#).



Cryptocurrency addresses: Capture the cryptocurrency addresses that sent and received funds, including the victim address(es) and the threat actor address(es). Cryptocurrency addresses are a string of numbers and letters with varying lengths depending on the type of cryptocurrency. Common address types include:

- **Bitcoin addresses:** Bitcoin addresses start with "1," "3," or "bc1" and consist of 26 to 63 alphanumeric characters.³⁴
- **Ethereum addresses:** Ethereum addresses start with "0x" and consist of 42 hexadecimal characters (numbers 0-9 and letters A-F).³⁵



Transaction hash: Document the transaction hash of any relevant transactions. A transaction hash, also known as a transaction ID, is a unique identifier of a transaction, typically comprised of 64 hexadecimal characters.³⁶



Transaction date and time: Capture the date, time, and time zone of any relevant transactions. Keep in mind the date and time of cryptocurrency transactions is often denoted in Coordinated Universal Time (UTC).

This information can be documented in CIS's Cryptocurrency Crime Documentation Form, which is provided on the next page, and should also be provided to the FBI's [Internet Crime Complaint Center \(IC3\)](#).

Cryptocurrency Crime Documentation Form

Provided by the Center for Internet Security (CIS). For further guidance, contact CIS [here](#).

Contact Information:

Name: Telephone Number:

Cryptocurrency Type(s):

Cryptocurrency Amount:
Approximate USD Value:

Cryptocurrency Addresses:

Victim Address(es):	Threat Actor Address(es):
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Transaction Hash(es):

1.	<input type="text"/>
2.	<input type="text"/>
3.	<input type="text"/>
4.	<input type="text"/>
5.	<input type="text"/>

Transaction Date(s) and Time(s):

	Date	Time	Time Zone
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>

Notes:

References

- ¹ https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- ² https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- ³ https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf
- ⁴ <https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams>
- ⁵ <https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022#Fraud-and-Scams>
- ⁶ https://www.ic3.gov/annualreport/reports/2023_ic3cryptocurrencyreport.pdf
- ⁷ https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf
- ⁸ https://www.ic3.gov/AnnualReport/Reports/2021_ic3report.pdf
- ⁹ https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf
- ¹⁰ https://www.ic3.gov/annualreport/reports/2023_ic3cryptocurrencyreport.pdf
- ¹¹ https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- ¹² https://www.ic3.gov/Outreach/Brochures/2024_aba_cryptocurrency_infographic.pdf
- ¹³ <https://www.secretservice.gov/investigations/investmentfraud-pigbutchering>
- ¹⁴ <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud>
- ¹⁵ <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud>
- ¹⁶ https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf
- ¹⁷ https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- ¹⁸ <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-job-scams>
- ¹⁹ <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-job-scams>
- ²⁰ <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-job-scams>
- ²¹ <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/12/paying-get-paid-gamified-job-scams-drive-record-losses>
- ²² <https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams>
- ²³ <https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022#Fraud-and-Scams>
- ²⁴ <https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022#Fraud-and-Scams>
- ²⁵ https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- ²⁶ <https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022#Fraud-and-Scams>
- ²⁷ <https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/>
- ²⁸ <https://www.chainalysis.com/blog/2022-crypto-pump-and-dump-schemes/>
- ²⁹ https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf
- ³⁰ <https://www.ic3.gov/PSA/2023/PSA230811>
- ³¹ <https://www.ic3.gov/PSA/2025/PSA250813>
- ³² https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf
- ³³ <https://www.ic3.gov/PSA/2025/PSA250813>
- ³⁴ <https://www.ic3.gov/CrimeInfo/Cryptocurrency>
- ³⁵ <https://info.etherscan.com/what-is-an-ethereum-address/>
- ³⁶ <https://www.ic3.gov/CrimeInfo/Cryptocurrency>