FEDERAL BUREAU of INVESTIGATION

Cryptocurrency Fraud Report 2023

INTERNET CRIME COMPLAINT CENTER

2023 CRYPTOCURRENCY FRAUD REPORT

CONTENTS

INTRODUCTION 3
2023 CRYPTOCURRENCY-RELATED COMPLAINTS REPORTED TO IC3 4
2023 COMPLAINTS BY AGE GROUP 5
STATISTICS ON COMPLAINTS REPORTED TO IC3 OVER THE YEARS 5
2023 CRIME TYPES WITH CRYPTOCURRENCY NEXUS 6
2023 CRIME TYPES WITH CRYPTOCURRENCY NEXUS *CONTINUED* 7
2023 OVERALL STATE STATISTICS 8
2023 OVERALL STATE STATISTICS, *CONTINUED* 9
2023 COUNTRY STATISTICS 10
WHY DO CRIMINALS EXPLOIT CRYPTOCURRENCY? 11
GUIDANCE FOR CRYPTOCURRENCY SCAM VICTIMS 11
2023 CRYPTOCURRENCY TREND SPOTLIGHTS 12
INVESTMENT FRAUD 12
Confidence-Enabled Cryptocurrency Investment Fraud 13
Variations On Cryptocurrency Investment Fraud 14
CRYPTOCURRENCY KIOSKS 16
CRYPTOCURRENCY RECOVERY SCHEMES 16
TIPS TO PROTECT YOURSELF 17
THE FBI'S VIRTUAL ASSETS UNIT (VAU) 18
APPENDIX A: DEFINITIONS 19
APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA 22
APPENDIX C: PUBLIC SERVICE ANNOUCEMENTS PUBLISHED 23

INTRODUCTION

Dear Reader,

As the use of cryptocurrency in the global financial system continues to grow, so too does its use by criminal actors. In 2023, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received more than 69,000 complaints from the public regarding financial fraud involving the use of cryptocurrency, such as bitcoin, ether, or tether. Estimated losses with a nexus to cryptocurrency totaled more than $5.6 billion. While the number of cryptocurrency-related complaints represents only about 10 percent of the total number of financial fraud complaints, the losses associated with these complaints account for almost 50 percent of the total losses.

Complaints filed in 2023 show that criminal actors exploit cryptocurrencies in each scheme category tracked by IC3. The exploitation of cryptocurrency was most pervasive in investment scams, where losses accounted for almost 71 percent of all losses related to cryptocurrency. Call center frauds, including tech/customer support scams and government impersonation scams, accounted for about 10 percent of losses associated to cryptocurrency.

The decentralized nature of cryptocurrency, the speed of irreversible transactions, and the ability to transfer value around the world make cryptocurrency an attractive vehicle for criminals, while creating challenges to recover stolen funds. Once an individual sends a payment, the recipient owns the cryptocurrency and often quickly transfers it into an account overseas for cash out purposes. Rapid and accurate complaint reporting are key to assisting law enforcement in investigating fraud schemes that exploit cryptocurrencies.

The IC3 is the central intake point for individuals in the U.S. or abroad to report fraud. These complaints are analyzed and aggregated to identify trends and help develop strategies to combat these schemes and protect scam victims from loss. IC3 also shares the complaints it receives with FBI field offices, other law enforcement agencies, and regulatory entities for further investigation or action, as appropriate. Along with the Department of Justice, law enforcement, regulatory agencies, and financial institution partners, the FBI is continually dedicated to identifying the perpetrators of these schemes and bringing them to justice.

This cryptocurrency fraud report, which is supplemental to the 2023 IC3 Annual Report and the 2023 Elder Fraud Report filed earlier this year, is being released to bring attention to the proliferation of losses linked to cryptocurrency-related fraud, bolster awareness of the most prevalent schemes utilizing cryptocurrencies, and educate the public on the ways to protect themselves against these kinds of frauds.

Michael D. Nordwall
Assistant Director
Federal Bureau of Investigation
Criminal Investigative Division

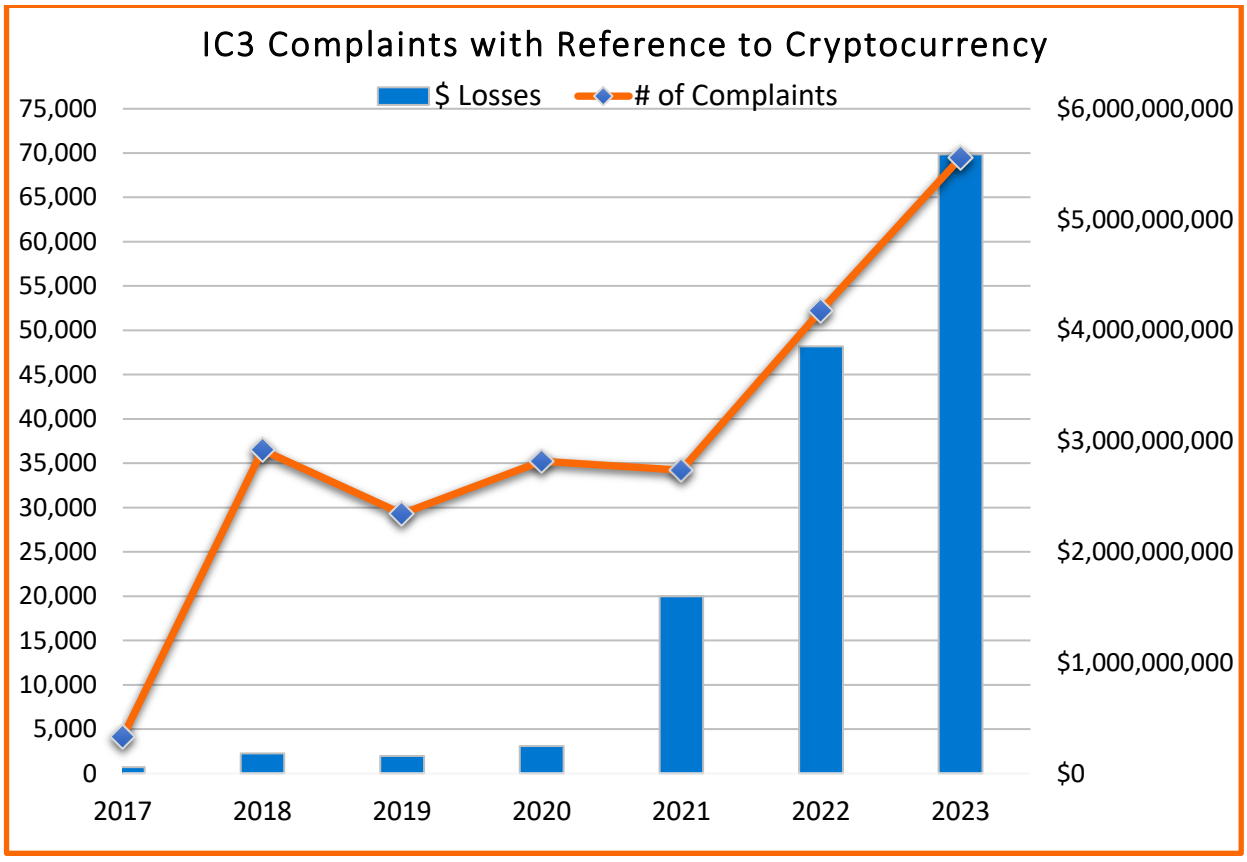
2023 CRYPTOCURRENCY-RELATED COMPLAINTS REPORTED TO IC3[a]

[a] Accessibility description: Image depicts key statistics regarding cryptocurrency complaints. The total number of complaints received in 2023 was 60,468. Total losses of $5.6 billion were reported, experiencing a 45 percent increase in losses from 2023. The most reported crime type related to cryptocurrency is Investment.

2023 COMPLAINTS BY AGE GROUP

COMPLAINTS REFERENCING CRYPTOCURRENCY		
Age Range[b]	Total Count	Total Loss
Under 20	858	$14,745,598
20 - 29	6,258	$168,585,320
30 - 39	10,849	$693,707,482
40 - 49	10,318	$843,877,119
50 - 59	8,918	$901,087,112
Over 60	16,806	$1,648,455,748

STATISTICS ON COMPLAINTS REPORTED TO IC3 OVER THE YEARS[c]



[b] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

[c] Charts depict the amount of Cryptocurrency complaints reported to the IC3 from 2017 – 2023.

2023 CRIME TYPES WITH CRYPTOCURRENCY NEXUS

COMPLAINTS			
Crime Type	**Complaints**	**Crime Type**	**Complaints**
Investment	32,094	**Lottery/Sweepstakes/Inheritance**	137
Tech Support	8,719	**Identity Theft**	133
Personal Data Breach	8,716	**Credit Card/Check Fraud**	119
Extortion	8,630	**Ransomware**	108
Confidence/Romance	3,749	**Overpayment**	90
Government Impersonation	2,266	**BEC**	70
Non-payment/Non-Delivery	810	**Real Estate**	60
Phishing/Spoofing	667	**Harassment/Stalking**	39
Advanced Fee	649	**Malware**	27
Data Breach	592	**Botnet**	13
Employment	581	**Crimes Against Children**	11
Other	369	**Threats of Violence**	6
SIM Swap	300	**IPR/Copyright and Counterfeit**	4

Descriptors		
Cryptocurrency	43,653	These descriptors relate to the currency used in the crime and the IC3 uses them for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Cryptocurrency Wallet	25,815	

2023 CRIME TYPES WITH CRYPTOCURRENCY NEXUS *Continued*

LOSSES

Crime Type	Loss	Crime Type	Loss
Investment	$3,961,033,779	**Phishing/Spoofing**	$9,630,206
Personal Data Breach	$494,493,759	**Extortion**	$9,281,906
Tech Support	$420,904,388	**BEC**	$4,768,674
Confidence/Romance	$215,821,314	**Lottery/Sweepstakes/Inheritance**	$4,462,513
Data Breach	$150,154,167	**Credit Card/Check Fraud**	$3,317,381
Government Impersonation	$112,878,842	**Identity Theft**	$2,732,795
Advanced Fee	$39,375,337	**Harassment/Stalking**	$1,854,329
SIM Swap	$30,263,667	**Overpayment**	$1,582,857
Ransomware*	$27,355,793	**Real Estate**	$887,285
Other	$26,258,782	**Malware**	$341,178
Non-payment/Non-Delivery	$19,656,091	**Crimes Against Children**	$185,921
Botnet	$17,002,000	**IPR/Copyright and Counterfeit**	$51,952
Employment	$10,104,795	**Threats of Violence**	$27,500

Descriptors	
Cryptocurrency	$3,809,090,856
Cryptocurrency Wallet	$1,778,399,729

These descriptors relate to the currency used in the crime and the IC3 uses them for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

* Regarding Ransomware adjusted losses: this number does not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victims directly reporting to FBI field offices/agents.

2023 OVERALL STATE STATISTICS

COMPLAINTS BY STATE*

	State	Complaints		State	Complaints
1	**California**	9,522	30	**Kentucky**	427
2	**Florida**	5,076	31	**Louisiana**	420
3	**Texas**	4,770	32	**New Mexico**	374
4	**New York**	3,202	33	**Arkansas**	348
5	**Washington**	2,049	34	**Kansas**	340
6	**Illinois**	1,928	35	**Iowa**	304
7	**Arizona**	1,920	36	**Idaho**	297
8	**Pennsylvania**	1,773	37	**Hawaii**	276
9	**Virginia**	1,734	38	**Nebraska**	239
10	**New Jersey**	1,732	39	**Mississippi**	230
11	**Georgia**	1,590	40	**Montana**	220
12	**North Carolina**	1,466	41	**New Hampshire**	217
13	**Maryland**	1,385	42	**West Virginia**	213
14	**Ohio**	1,348	43	**Maine**	210
15	**Colorado**	1,319	44	**Puerto Rico**	188
16	**Michigan**	1,319	45	**Alaska**	172
17	**Massachusetts**	1,216	46	**District of Columbia**	162
18	**Minnesota**	976	47	**Rhode Island**	158
19	**Tennessee**	942	48	**Delaware**	157
20	**Nevada**	938	49	**South Dakota**	117
21	**Oregon**	872	50	**North Dakota**	103
22	**Missouri**	838	51	**Wyoming**	96
23	**South Carolina**	755	52	**Vermont**	69
24	**Indiana**	749	53	**United States Minor Outlying**	19
25	**Wisconsin**	707	54	**Virgin Islands, U.S.**	13
26	**Utah**	637	55	**Guam**	8
27	**Connecticut**	564	56	**Northern Mariana Islands**	2
28	**Alabama**	511	57	**American Samoa**	1
29	**Oklahoma**	488			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

2023 OVERALL STATE STATISTICS, *Continued*

LOSSES BY STATE*

	State	Loss		State	Loss
1	**California**	$1,155,315,595	30	**Louisiana**	$32,184,662
2	**Texas**	$411,914,142	31	**Hawaii**	$31,800,598
3	**Florida**	$390,222,375	32	**New Mexico**	$26,752,361
4	**New York**	$317,311,547	33	**Oklahoma**	$25,031,191
5	**New Jersey**	$179,431,143	34	**South Dakota**	$22,983,646
6	**Illinois**	$160,315,355	35	**Iowa**	$21,961,344
7	**Washington**	$141,756,936	36	**Arkansas**	$20,100,771
8	**Arizona**	$127,358,454	37	**Kansas**	$20,087,852
9	**Pennsylvania**	$123,530,269	38	**Idaho**	$19,941,423
10	**Virginia**	$122,004,080	39	**Kentucky**	$16,501,731
11	**Georgia**	$118,750,468	40	**Puerto Rico**	$15,285,209
12	**Nevada**	$115,553,999	41	**Nebraska**	$14,552,697
13	**Maryland**	$93,903,097	42	**Delaware**	$13,708,256
14	**Massachusetts**	$91,595,803	43	**Mississippi**	$12,711,955
15	**North Carolina**	$89,727,708	44	**Rhode Island**	$10,357,335
16	**Colorado**	$81,620,212	45	**New Hampshire**	$10,169,760
17	**Michigan**	$79,894,360	46	**Alaska**	$9,291,972
18	**Ohio**	$75,372,665	47	**West Virginia**	$8,942,357
19	**Minnesota**	$75,351,238	48	**District of Columbia**	$8,339,883
20	**Tennessee**	$68,133,794	49	**Wyoming**	$7,353,803
21	**Oregon**	$65,933,876	50	**North Dakota**	$6,564,076
22	**Indiana**	$60,606,356	51	**Maine**	$5,946,252
23	**Missouri**	$55,022,745	52	**Vermont**	$4,805,229
24	**Connecticut**	$52,373,549	53	**United States Minor**	$661,840
25	**South Carolina**	$47,139,835	54	**Virgin Islands, U.S.**	$326,678
26	**Alabama**	$37,646,792	55	**Guam**	$55,440
27	**Utah**	$36,098,268	56	**American Samoa**	$26,660
28	**Wisconsin**	$35,428,790	57	**Northern Mariana Islands**	$8,309
29	**Montana**	$33,067,773			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

2023 COUNTRY STATISTICS

In 2023, the IC3 received complaints with a cryptocurrency nexus from victims in over 200 countries.

TOP 20 COUNTRIES BY COMPLAINT COUNT*			TOP 20 COUNTRIES BY COMPLAINT LOSSES*		
	Country	Complaints		Country	Losses
1	**United States of America**	57,762	1	**United States of America**	$4,809,737,956
2	**Canada**	1,236	2	**Cayman Islands**	$195,663,025
3	**United Kingdom**	962	3	**Mexico**	$126,994,051
4	**Nigeria**	841	4	**Canada**	$72,080,498
5	**India**	840	5	**United Kingdom**	$59,367,008
6	**Australia**	537	6	**India**	$44,054,244
7	**Germany**	444	7	**Australia**	$24,747,551
8	**France**	374	8	**Israel**	$19,606,997
9	**South Africa**	349	9	**Germany**	$16,763,084
10	**Pakistan**	326	10	**Nigeria**	$15,608,489
11	**Brazil**	323	11	**Estonia**	$12,766,310
12	**Turkey**	303	12	**South Africa**	$12,709,141
13	**Japan**	280	13	**Singapore**	$10,644,446
14	**Philippines**	277	14	**China**	$10,322,825
15	**Mexico**	257	15	**Korea (Republic of)**	$10,208,414
16	**Netherlands**	238	16	**Philippines**	$9,462,902
17	**Spain**	225	17	**United Arab Emirates**	$9,372,704
18	**Italy**	222	18	**Taiwan**	$8,769,391
19	**United Arab Emirates**	216	19	**Hong Kong**	$8,730,474
20	**Iran (Islamic Republic of)**	213	20	**Japan**	$8,528,868

*Note: This information is based on the total number of complaints from each country. Please see Appendix B for more information regarding IC3 data.

WHY DO CRIMINALS EXPLOIT CRYPTOCURRENCY?

Decentralized Nature: Cryptocurrency is decentralized and distributed, which can offer a secure method to transfer value. Today's market includes thousands of cryptocurrencies users can transfer around the globe in exchange for goods, services, and other cryptocurrencies. Since cryptocurrencies eliminate the need for financial intermediaries to validate and facilitate transactions, criminals can exploit these characteristics to support illicit activity such as thefts, fraud, and money laundering.[d]

Irrevocable Transactions that Move Quickly: A cryptocurrency transfer can occur anywhere. The only requirements for transmitting funds from a particular address is the associated private key (which functions like a password or a PIN) and an Internet connection. Third parties do not sit between, or authorize, transactions and transactions are irrevocable – meaning they cannot be reversed. Criminal actors connected to the Internet from anywhere in the world can also exploit these characteristics to facilitate large-scale, nearly instantaneous cross-border transactions without traditional financial intermediaries that employ anti-money laundering programs.[e]

Challenges to Following Funds: Cryptocurrency transactions are permanently recorded on publicly available distributed ledgers called blockchains. As a result, law enforcement can trace cryptocurrency transactions to follow money in ways not possible with other financial systems. Nevertheless, since cryptocurrency also allows transfers of funds to exchanges overseas, US law enforcement may encounter significant challenges when following cryptocurrency that enters other jurisdictions, especially those with lax anti-money laundering laws or regulations.[f]

GUIDANCE FOR CRYPTOCURRENCY SCAM VICTIMS

What to do if you were the target of a cryptocurrency scam

The FBI encourages the public to submit a complaint through IC3.gov, even if a financial loss did not occur. Some of the most important information you can provide are details related to transactions. For cryptocurrency transactions, these details include cryptocurrency addresses; the amounts and types of cryptocurrencies; transaction hashes; and the dates and times of the transactions. If possible, please provide any other information you may have about the scam. These details may include how you met the scammer, what platforms you used to communicate, any web domain involved in the scheme, and any phone numbers or other identifiers. Be wary of cryptocurrency recovery services, especially those charging an up-front fee.[g]

- For more information on what to report, please reference PSA I-082423-PSA: FBI Guidance for Cryptocurrency Scam Victims (ic3.gov)
- File a complaint with IC3. www.ic3.gov
- Individuals aged 60 or older can contact the National Elder Fraud Hotline (833-372-8311) to assist with filing an IC3 complaint.

---

[d] See October 2020 DOJ Report "Cryptocurrency Enforcement Framework" for more information.
[e] See June 2022 DOJ Report "How to Strengthen International Law Enforcement Cooperation for Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets" for more information.
[f] See June 2022 DOJ Report "How to Strengthen International Law Enforcement Cooperation for Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets" for more information.
[g] See "Spotlight: Cryptocurrency Recovery Schemes" on page 16 of this report for more information.

2023 CRYPTOCURRENCY TREND SPOTLIGHTS

Investment Fraud

Investment fraud generally involves a deceptive practice to induce investment based on false information. These schemes offer individuals large returns with the promise of minimal risk. Over the years, cryptocurrency's widespread promotion as an investment vehicle, combined with a mindset associated with the "fear of missing out," has led to opportunities for criminals to target consumers and retail investors—particularly those who seek to profit from investing but are unfamiliar with the technology and the attendant risks.[h]

Losses from cryptocurrency-related investment fraud schemes reported to the IC3 rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. Many individuals have accumulated massive debt to cover losses from these fraudulent investments. While individuals in the age ranges of 30 - 39 and 40 - 49 filed the most cryptocurrency-investment fraud complaints (approximately 5,200 reports in each age group), complainants over the age of 60 reported the highest losses (over $1.24 billion).

[h] See June 2022 DOJ Report "How to Strengthen International Law Enforcement Cooperation for Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets" for more information.

Confidence-Enabled Cryptocurrency Investment Fraud

The Scheme

Although there are many variations of cryptocurrency-related investment fraud, in 2023, the most prominent was a unique kind of confidence-enabled cryptocurrency investment fraud. The schemes are socially engineered and trust-enabled, whereby criminals use dating applications (apps), social media platforms, professional networking sites, or encrypted messaging apps to establish relationships with their targets. Once trust is established, criminals introduce the topic of cryptocurrency investment. Criminals claim to have some expertise or know an expert who can help potential investors achieve financial success. Criminals then convince their targets to use fraudulent websites or apps, controlled by the criminals, to invest in cryptocurrency. Criminals coach their targets through the investment process, show them fake profits, and encourage them to invest more. Criminals may allow victims to withdraw small amounts early in the scam to engender more trust in the fraudulent platforms. Nevertheless, when the targets attempt to fully withdraw their investment and any purported earnings, they are told they need to pay a fee or taxes. The criminals never release the bulk of funds, even if their targets pay the imposed fees or taxes.

Individuals who report losing money to these schemes are sometimes also targeted by fraudulent businesses that claim to help recover lost cryptocurrency funds.[i]

Have You Been Taking Investment Advice from an Online Friend?

Scammers will build trust for weeks and months before trying to convince you to invest in cryptocurrency. They will use text messages, video chats, phone calls, and emails to lure you in.

But there is one thing these scammers typically will not do – **they will *not* meet with you in real life.** If an investment opportunity comes from someone who you have never met in person – you have never met them for coffee, never walked together in the park, never gone together to see a movie – be **extremely cautious** of the advice.

You should still carefully evaluate all investment advice but be especially cautious of advice coming from a long-distance "friend" you have never met in person.

Labor Trafficking Nexus

US citizens and individuals who travel or live abroad should be aware of the risk of false job advertisements linked to labor trafficking at scam compounds overseas.[j] These compounds hold workers against their will and use intimidation to force the workers to participate in scam operations. Criminal actors post false job advertisements on social media and online employment sites to target people, primarily in Asia. The schemes cover a wide range of opportunities, to include tech support, call center customer service, and beauty salon technicians. Job seekers are offered competitive salaries, lucrative benefits, paid travel expenses as well as room and board. Often throughout the process, the position location is shifted from the advertised location. Once the job seeker arrives in the

[i] See "Spotlight: Cryptocurrency Recovery Schemes" on page 16 of this report for more information.

[j] A scam compound is a property housing fraud operations conducted using a variety of schemes, sometimes also housing trafficked victims who are forced to commit the frauds.

foreign country, criminal actors may confiscate the job seeker's passport and travel documents and threaten or use violence to coerce the job seeker into cooperating.

Workers are often told they must pay for travel and other expenses, meaning the worker starts off in debt. They must then work off the debt while also trying to pay off their room and board. The criminal actors use the worker's mounting debt and fear of local law enforcement as additional means to control them. Trafficked workers are sometimes sold and transferred between compounds, further adding to their debt.

Tips to protect yourself related to potential labor trafficking.

- Research the advertised company before accepting a job offer. Beware of vague language about the company or limited employment details.
- Beware of job advertisements with unusually high salaries and many perks.
- If you plan on relocating to a different country for a new job, inform family and friends of employment details, to include contact information from the job advertisement.
- Prior to relocating, schedule regular check-ins with family and friends to confirm safety and well-being.
- Enroll in the Smart Traveler Enrollment Program (STEP) at step.state.gov to receive safety, security, and travel advisories for your destination country. By registering for STEP, local US Embassy or US Consulates can contact you during an emergency.
- If you are the potential victim of labor trafficking, contact the nearest US Embassy.

Variations On Cryptocurrency Investment Fraud

Liquidity Mining Schemes[k]

Liquidity Mining is an investment strategy used to earn passive income with cryptocurrency. In legitimate liquidity mining operations, investors stake[l] their cryptocurrency in a liquidity pool to provide traders with the liquidity necessary to conduct transactions. In return, investors receive a portion of the trading fees.

In this variation of cryptocurrency investment fraud, scammers exploit owners of cryptocurrency, typically Tether (USDT) and/or Ethereum (ETH). The scammer builds a professional or personal relationship with their target over a few days to weeks, gives instructions for purchasing if they do not already own cryptocurrency, and entices them to participate in liquidity mining by guaranteeing a return on investment of one to three percent daily. Scammers convince targets to link their cryptocurrency wallet[m] to a fraudulent liquidity mining application. Scammers then wipe out the funds without notification or permission from the owner.[n]

---

[k] Scammers may refer to the investment opportunity as a liquidity pool, liquidity mining, or mining pool; for purposes of this report, the term liquidity mining will be used to describe all iterations of the scheme.
[l] Term used to describe investing cryptocurrency and receiving rewards for holding it for a period.
[m] A "cryptocurrency wallet" is software for storing cryptocurrency and other virtual assets.
[n] This linkage is achieved using dApps aka decentralized applications. Although similar to normal apps, dApps run on peer-to-peer networks or on the blockchain and are not controlled by a single entity; once published, the dApps become public and open-source.

Tips to protect yourself from Liquidity Mining Schemes.

- Be cognizant that investors in legitimate liquidity mining operations deposit funds into the platform and later withdraw the original funds along with any returns generated. Reconsider joining pools that deviate from this procedure. In a legitimate liquidity mining process, returns are usually tied to cryptocurrency market fluctuations in the specific cryptocurrency or cryptocurrency pair being used.
- Be vigilant when learning of investment opportunities via online research. Scam websites or applications are not usually advertised online, nor are they allowed to be indexed by webcrawlers from search engines like Google and others. Verify the spelling of web addresses, websites, and email addresses that look trustworthy, but may be imitations of legitimate websites.
- If you are concerned about the legitimacy of the domain, do not connect your cryptocurrency wallet.
- Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.
- Authenticate all links sent from known and unknown contacts before clicking.
- Periodically use a third-party token allowance checker to determine whether you have inadvertently permitted any sites or applications access to your wallet.

Fraudulent Play-to-Earn Gaming Applications

Criminals create fake gaming apps to steal cryptocurrency, which they advertise as play-to-earn games offering financial incentives to players.

Criminals contact potential targets online and build a relationship with them over time. Criminals then introduce targets to an online or mobile game, in which players purportedly earn cryptocurrency rewards in exchange for some activity, such as growing “crops” on an animated farm.

To participate in the game, criminals direct targets to create a cryptocurrency wallet, purchase cryptocurrency, and join a specific game app. The more money they store in their wallet, the more rewards they will purportedly earn in the game. Targets play the game and see fake rewards accumulating in the app. When targets stop depositing funds into the wallet, criminals drain them using a malicious program that was activated upon joining the game. Although criminals tell targets they may reclaim funds by paying additional taxes or fees, they are unable to get their money back, even if they pay the extra fees.

Tips to protect yourself from Fraudulent Pay-to-Earn Gaming Applications

- If you wish to participate in cryptocurrency-related gaming, create a unique wallet to use. This isolates your primary cryptocurrency holdings should you unknowingly grant illicit actors access to your gaming wallet.
- Use a third-party blockchain explorer to independently check the balances of the addresses in your gaming wallet.
- Periodically use a third-party token allowance checker to help you see which sites or apps you have inadvertently permitted to access funds in your wallet and revoke those permissions.

Cryptocurrency Kiosks

Cryptocurrency kiosks are ATM-like devices or electronic terminals that allow users to exchange cash and cryptocurrency. Criminals are known to direct individuals to use a cryptocurrency kiosk to send funds, which enables a more anonymous transaction than depositing the cash at a financial institution.

According to IC3 data, the use of cryptocurrency kiosks to perpetrate fraudulent activity against the US population is increasing. In 2023, the IC3 received more than 5,500 complaints reporting the use of cryptocurrency kiosks, with losses over $189 million.

Typically, criminals give detailed instructions to individuals, to include how to withdraw cash from their bank, how to locate a kiosk, and how to deposit and send funds using the kiosk. In most instances, the cryptocurrency kiosk transactions are facilitated using QR codes, square barcodes with information that can be scanned and read with a smartphone or kiosk camera. An individual can scan the QR code of an intended recipient at a cryptocurrency kiosk, making it easier to send cryptocurrency to the correct destination.

IC3 data includes complaints in which a cryptocurrency kiosk was used in the scam. The complaint may also include other types of transactions.

USE OF CRYPTOCURRENCY KIOSKS REPORTED IN IC3 COMPLAINTS – 2023

Age Range	Complaints	Losses
Under 20	65	$252,198
20 - 29	416	$3,529,680
30 - 39	451	$8,651,706
40 - 49	391	$9,634,346
50 - 59	476	$11,409,372
Over 60	2,676	$124,332,127

TOP FIVE CRIME TYPES INVOLVING CRYPTOCURRENCY KIOSKS IN IC3 COMPLAINTS -- 2023

Crime Type	Percent of Total Complaints
Tech Support	46%
Extortion	17%
Government Impersonation	10%
Investment	8%
Confidence/Romance	6%

Cryptocurrency Recovery Schemes

Individuals who report losing money to various schemes, particularly cryptocurrency investment fraud, are sometimes also targeted by fraudulent businesses that claim to help recover lost cryptocurrency funds. In some situations, this is the next iteration of the ongoing fraud scheme. Representatives from these fraudulent businesses claim to provide cryptocurrency tracing and promise an ability to recover lost funds. They contact individuals who have lost money via social media or messaging platforms or

advertise their fraudulent cryptocurrency recovery services in the comment sections of online news articles and videos about cryptocurrency; among online search results for cryptocurrency; or on social media.

Fraudulent businesses claiming to recover stolen funds charge an up-front fee and either cease communication after receiving an initial deposit or produce an incomplete or inaccurate tracing report and request additional fees to recover funds. These fraudulent companies may claim affiliation with law enforcement or legal services to appear legitimate.

Please note that private sector recovery companies cannot issue legal orders to recover or seize stolen cryptocurrency. Cryptocurrency exchanges freeze accounts only based on internal processes or in response to legal documents issued by a court. Individuals who have lost money to scams may choose to pursue civil litigation to seek recovery of their funds.

Additional information on cryptocurrency recovery schemes is available in **PSA I-081123-PSA**: Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams (ic3.gov).

TIPS TO PROTECT YOURSELF

- Criminals will seek to instill a sense of urgency and isolation.
- When receiving an unsolicited call by an unknown caller claiming to work for a well-known company or government agency, hang up and independently research the company or agency's publicly published phone number and call it to confirm authenticity of the original call.
- No legitimate law enforcement or government official will call to demand payment via a cryptocurrency kiosk.
- Never give personally identifying information to anyone without verifying the person is who they say they are.
- Verify the validity of any investment opportunity strangers or long-lost contacts offer on social media websites. If you have never met an individual in real life, even if you have spoken on the phone or video chatted, be very cautious of accepting investment advice or opportunities.
- Be on the lookout for domain or website names that impersonate legitimate financial institutions, especially cryptocurrency exchanges.
- Fraudulent businesses often use website addresses that mimic real financial institutions, but are often slightly different, to convince people the fraudulent website is legitimate.
- 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.
- Investment involves risk. Individuals should invest based on their financial objectives and financial resources and, if in any doubt, should seek advice from a licensed financial adviser.

THE FBI'S VIRTUAL ASSETS UNIT (VAU)

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. With its cyber and investigative expertise, the FBI has been at the center of efforts to detect, investigate, and prosecute criminal activity related to virtual assets worldwide, including through its 63 Legal Attaché (Legat) offices and 30 sub-offices in key cities around the globe, providing coverage for more than 180 countries, territories, and islands. To further those efforts, in February 2022, the FBI formed the Virtual Assets Unit (VAU), a specialized team dedicated to investigating cryptocurrency-related crimes. The VAU centralizes the FBI's cryptocurrency expertise into one nerve center, providing technological equipment, blockchain analysis, and virtual asset seizure training, and other sophisticated training for FBI personnel.

APPENDIX A: DEFINITIONS

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise (BEC): BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by criminals by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Botnet: A botnet is a group of two or more computers controlled and updated remotely for an illegal purchase such as a Distributed Denial of Service or Telephony Denial of Service attack or other nefarious activity.

Confidence/Romance: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent's Scheme and any scheme in which the perpetrator preys on the targeted individual's "heartstrings."

Credit Card Fraud/Check Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH, EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Data Breach: A data breach in the cyber context is the use of a computer intrusion to acquire confidential or secured information. This does not include computer intrusions targeting personally owned computers, systems, devices, or personal accounts such as social media or financial accounts.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Government Impersonation: A government official is impersonated to collect money.

Harassment/Stalking: Repeated words, conduct, or action that serve no legitimate purpose and are directed at a specific person to annoy, alarm, or distress that person. Engaging in a course of conduct directed at a specific person that would cause a reasonable person to fear for his/her safety or the safety of others or suffer substantial emotional distress.

Identity Theft: Someone wrongfully obtains and uses personally identifiable information in some way that involves fraud or deception, typically for economic gain.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer those targeted large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

IPR/Copyright and Counterfeit: The illegal theft and use of others' ideas, inventions, and creative expressions – what's called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

Lottery/Sweepstakes/Inheritance: An individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

Malware: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Phishing/Spoofing: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Real Estate: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

SIM Swap: The use of unsophisticated social engineering techniques against mobile service providers to transfer a victim's phone service to a mobile device in the criminal's possession.

Tech Support: Subject posing as technical or customer support/service.

Threats of Violence: An expression of an intention to inflict pain, injury, self-harm, or death not in the context of extortion.

APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- As appropriate, complaints are reviewed by IC3 analysts, who apply a crime type and adjust the total loss.
- Crime types and losses can be variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which can change.
- Complainant is identified as the individual filing a complaint.
- Some complainants may have filed more than once, creating a possible duplicate complaint.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.

APPENDIX C: PUBLIC SERVICE ANNOUCEMENTS PUBLISHED

TITLE	DATE
Criminals Steal Cryptocurrency through Play-to-Earn Games	3/9/2023
The FBI Warns of a Spike in Cryptocurrency Investment Schemes	3/14/2023
The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds	5/22/2023
Business Email Compromise: The $50 Billion Scam	6/9/2023
Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition	8/4/2023
Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams	8/11/2023
FBI Guidance for Cryptocurrency Scam Victims	8/24/2023
"Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings	9/29/2023
Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers	10/18/2023
Scammers Solicit Fake Humanitarian Donations	10/24/2023
2023 Holiday Shopping Scams	11/15/2023