FEDERAL BUREAU of INVESTIGATION

Elder Fraud Report

2023

INTERNET CRIME COMPLAINT CENTER

2023 ELDER FRAUD REPORT

TABLE OF CONTENTS

INTRODUCTION

Dear Reader,

Every day, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) receives thousands of complaints reporting a wide array of scams, many of them targeting the elderly. In 2023, total losses reported to the IC3 by those over the age of 60 topped $3.4 billion, an almost 11% increase in reported losses from 2022. There was also a 14% increase in complaints filed with IC3 by elderly victims. However, these numbers do not fully capture the frauds and scams targeting this vulnerable cross-section of our population, as only about half of the more than 880,000 complaints received by IC3 in 2023 included age data. The FBI is publishing the 2023 IC3 Elder Fraud Annual Report in hopes of shining a spotlight on the frauds and scams impacting those over 60 and preventing not only future victimization but also revictimization.

Combatting the financial exploitation of those over 60 years of age continues to be a priority of the FBI. Along with our partners, we continually work to aid victims and to identify and investigate the individuals and criminal organizations that perpetrate these schemes and target the elderly. The IC3 serves as the FBI's central intake point for reports of frauds and scams. Compilation of statistics based on these reports helps law enforcement develop strategies to combat these schemes and protect victims from loss. This year, as in 2022, tech support fraud was the number one crime type impacting complainants over 60, while investment scams continued to be the costliest to the elderly in terms of financial losses suffered.

Frauds and scams will continue to evolve, but many characteristics of these schemes remain the same even as new trends develop. I encourage the public to review previous IC3 Annual Reports and Public Service Announcements (PSAs) to further educate and protect yourself, as well as your family, friends, and community.

I also want to thank all those who have reported these schemes and encourage the public to report any kind of fraud or scam, even attempted fraud, to the IC3 as soon as possible. Reporting fraud helps the FBI identify trends and typologies, open new investigations, enhance ongoing investigations, and produce public awareness messaging. Do not be afraid or embarrassed to report. The FBI stands ready to assist and is here to help combat these threats.

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

THE IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world. To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes. As of December 31, 2023, the IC3 has received over eight million complaints. The IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber-enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate. That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds. Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends. The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.

BY THE NUMBERS

IC3 Over 60 Complaints by the Numbers

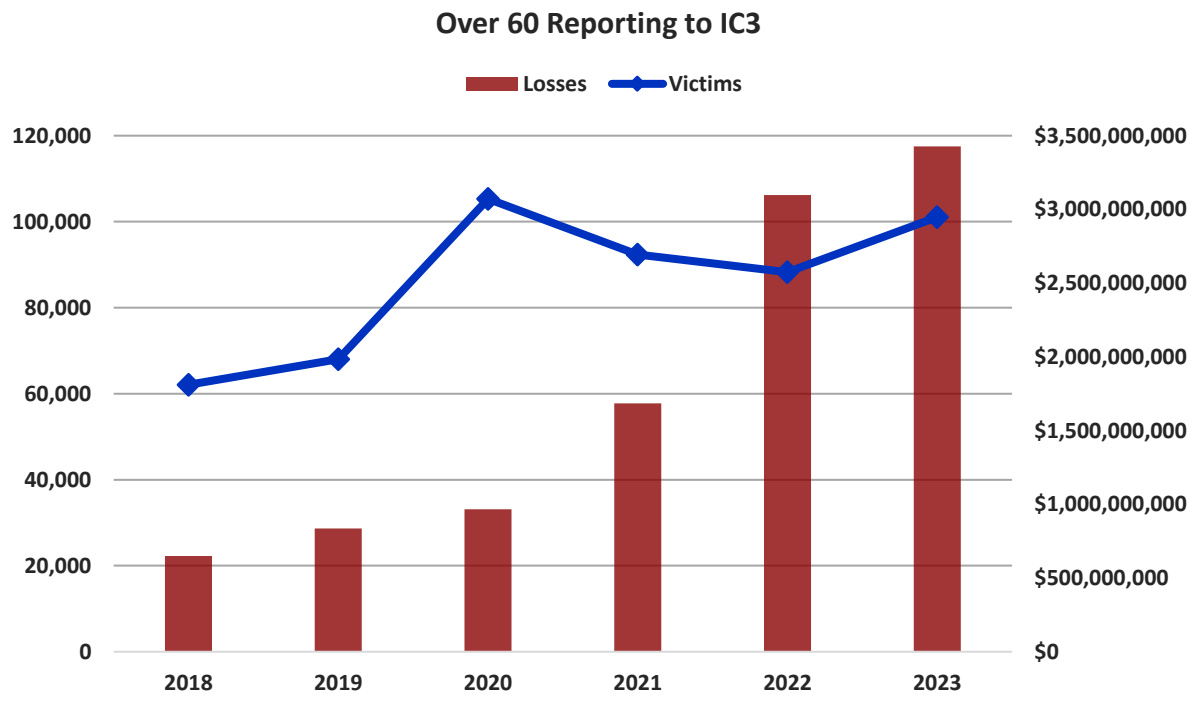
2023

[1] Accessibility description: Image depicts key statistics regarding Over 60 complaints. The total number of complaints received in 2023 was 101,068. Total losses of $3.4 billion were reported. Over 60 complainants experienced 11 percent increase in losses from 2022. 5,920 individuals lost more than $100,000. The average loss per complaint was $33,915.

2023 COMPLAINTS BY AGE GROUP

COMPLAINTS		
Age Range[2]	Total Count	Total Loss
Under 20	18,174	$40,703,428
20 - 29	62,410	$360,743,568
30 - 39	88,138	$1,167,165,071
40 - 49	84,052	$1,501,216,581
50 - 59	65,924	$1,681,873,944
Over 60	101,068	$3,427,717,654

COMPLAINTS FILED BY INDIVIDUALS OVER 60 TRENDS[3]



[2] 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.

[3] Charts describe Count and Loss Trends for those Over 60 from 2018 – 2023.

2023 CRIME TYPES

COMPLAINANTS OVER 60			
Crime Type	**Count**	**Crime Type**	**Count**
Tech Support	17,696	**Other**	1,447
Personal Data Breach	7,333	**Spoofing**	1,171
Confidence/Romance	6,740	**Employment**	1,079
Non-payment/Non-Delivery	6,693	**Overpayment**	698
Investment	6,443	**Harassment/Stalking**	568
Extortion	5,396	**Data Breach**	336
Government Impersonation	3,517	**Ransomware**	175
Credit Card/Check Fraud	3,182	**SIM Swap**	174
BEC	3,080	**IPR/Copyright and Counterfeit**	152
Identity Theft	3,010	**Threats of Violence**	115
Advanced Fee	1,951	**Malware**	67
Lottery/Sweepstakes/Inheritance	1,771	**Crimes Against Children**	26
Real Estate	1,498	**Botnet**	17

Descriptors*	
Cryptocurrency	12,284
Cryptocurrency Wallet	4,684

These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 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 BEC counts: A whole number is given to depict the overall complaint count and includes when a Complainant Over 60 may be reporting on behalf of a business or personally.

2023 CRIME TYPES *Continued*

COMPLAINANTS OVER 60 LOSS			
Crime Type	**Loss**	**Crime Type**	**Loss**
Investment	$1,243,010,600	**Data Breach**	$23,913,130
Tech Support	$589,759,770	**Extortion**	$23,093,451
BEC	$382,372,731	**SIM Swap**	$15,148,072
Confidence/Romance	$356,888,968	**Overpayment**	$7,496,049
Government Impersonation	$179,646,103	**Employment**	$6,835,684
Personal Data Breach	$109,724,027	**Threats of Violence**	$5,128,768
Other	$72,707,042	**Spoofing**	$2,623,837
Advanced Fee	$67,923,263	**Harassment/Stalking**	$1,930,347
Lottery/Sweepstakes/Inheritance	$67,396,206	**Crimes Against Children**	$1,159,939
Real Estate	$65,634,851	**Ransomware**	$635,548
Non-payment/Non-Delivery	$59,018,965	**Malware**	$261,144
Credit Card/Check Fraud	$37,862,023	**IPR/Copyright and Counterfeit**	$183,169
Identity Theft	$34,551,900	**Botnet**	$23,142

Descriptors*	
Cryptocurrency	$1,336,565,297
Cryptocurrency Wallet	$316,919,147

These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 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 BEC counts: A whole number is given to depict the overall complaint count and includes when a Complainant Over 60 may be reporting on behalf of a business or personally.

** 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 complainant. In some cases, complainants do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what complainants report to the FBI via the IC3 and does not account for complainants directly reporting to FBI field offices/agents.

LAST 3 YEARS COMPARISON

OVER 60 COMPLAINT COUNT			
Crime Type	**2023**	**2022**	**2021**
Advanced Fee	1,951	3,153	3,029
BEC	3,080	3,938	3,755
Botnet	17	33	--
Civil Matter	--	--	184
Computer Intrusion	--	--	176
Confidence Fraud/Romance	6,740	7,166	7,658
Credit Card/Check Fraud	3,182	4,956	3,164
Crimes Against Children	26	84	42
Data Breach	336	333	158
Denial of Service/TDos	--	--	61
Employment	1,079	1,286	1,408
Extortion	5,396	4,285	5,987
Gambling	--	--	19
Government Impersonation	3,517	3,425	3,319
Harassment/Stalking	568	754	--
Health Care Related	--	--	74
IPR/Copyright and Counterfeit	152	235	686
Identity Theft	3,010	4,825	8,902
Investment	6,443	4,661	2,104
Lottery/Sweepstakes/Inheritance	1,771	2,388	2,607
Malware	67	125	134
Non-payment/Non-Delivery	6,693	7,985	13,220
Other	1,447	2,016	2,933
Overpayment	698	1,183	1,448
Personal Data Breach	7,333	7,849	6,189
Phishing/Spoofing	2,856	8,369	9,767
Ransomware	175	215	365
Real Estate	1,498	1,862	1,764
SIM Swap	174	301	--
Tech Support	17,696	17,810	13,900
Threats of Violence	115	166	719
Cryptocurrency/Cryptocurrency Wallet	16,968	9,991	5,109

LAST 3 YEARS COMPARISON, *CONTINUED*

OVER 60 COMPLAINT LOSSES			
Crime Type	**2023**	**2022**	**2021**
Advanced Fee	$67,923,263	$49,322,099	$36,464,491
BEC	$382,372,731	$477,342,728	$355,805,098
Botnet	$23,142	$120,621	--
Civil Matter	--	--	$6,530,661
Computer Intrusion	--	--	$4,575,956
Confidence Fraud/Romance	$356,888,968	$419,768,142	$432,081,901
Credit Card/Check Fraud	$37,862,023	$61,649,198	$39,019,072
Crimes Against Children	$1,159,939	$48,373	$550
Data Breach	$23,913,130	$17,681,749	$7,095,746
Employment	$6,835,684	$6,403,021	$9,610,615
Extortion	$23,093,451	$15,555,047	$19,533,187
Gambling	--	--	$20,116
Government Impersonation	$179,646,103	$136,500,338	$69,186,858
Harassment/Stalking	$1,930,347	$254,659	--
Health Care Related	--	--	$1,233,632
IPR/Copyright and Counterfeit	$183,169	$203,140	$4,954,221
Identity Theft	$34,551,900	$42,653,578	$59,022,153
Investment	$1,243,010,600	$990,235,119	$239,474,635
Lottery/Sweepstakes/Inheritance	$67,396,206	$69,845,106	$53,557,330
Malware	$261,144	$1,851,421	$1,177,864
Non-payment/Non-Delivery	$59,018,965	$51,531,615	$52,023,580
Other	$72,707,042	$31,410,237	$22,196,542
Overpayment	$7,496,049	$10,977,231	$9,214,129
Personal Data Breach	$109,724,027	$127,736,607	$103,688,489
Phishing/Spoofing	$3,355,436	$36,715,205	$28,639,277
Ransomware	$635,548	$210,052	$424,852
Re-shipping	--	--	$360,455
Real Estate	$65,634,851	$135,239,020	$102,071,631
SIM Swap	$15,148,072	$19,515,629	--
Tech Support	$589,759,770	$587,831,698	$237,931,278
Threats of Violence	$5,128,768	$376,458	$361,549
Cryptocurrency/Cryptocurrency Wallet	$1,653,484,444	$1,088,330,051	$241,143,166

2023 OVERALL STATE STATISTICS

COMPLAINTS FILED BY INDIVIDUALS OVER 60 BY STATE*

Rank	State	Count	Rank	State	Count
1	California	11,622	30	Kentucky	908
2	Florida	8,138	31	New Mexico	759
3	Texas	7,035	32	Louisiana	736
4	Arizona	5,003	33	Iowa	674
5	New York	4,328	34	Arkansas	665
6	Ohio	3,299	35	Kansas	579
7	Pennsylvania	3,020	36	Idaho	514
8	Colorado	2,905	37	Hawaii	453
9	Illinois	2,887	38	Mississippi	434
10	Washington	2,873	39	New Hampshire	408
11	Virginia	2,475	40	Maine	397
12	North Carolina	2,423	41	West Virginia	386
13	Georgia	2,114	42	Nebraska	381
14	Michigan	2,109	43	South Dakota	369
15	New Jersey	2,049	44	Montana	359
16	Maryland	1,985	45	Delaware	314
17	Nevada	1,824	46	Alaska	297
18	Massachusetts	1,611	47	Rhode Island	274
19	Oregon	1,606	48	Puerto Rico	215
20	Tennessee	1,577	49	Wyoming	190
21	Missouri	1,502	50	District of Columbia	185
22	South Carolina	1,485	51	Vermont	163
23	Indiana	1,255	52	North Dakota	127
24	Minnesota	1,230	53	Virgin Islands, U.S.	21
25	Wisconsin	1,119	54	United States Minor Outlying	17
26	Alabama	976	55	Guam	15
27	Oklahoma	955	56	American Samoa	3
28	Connecticut	949	57	Northern Mariana Islands	2
29	Utah	945			

*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*

COMPLAINTS FILED BY INDIVIDUALS OVER 60 LOSSES BY STATE*

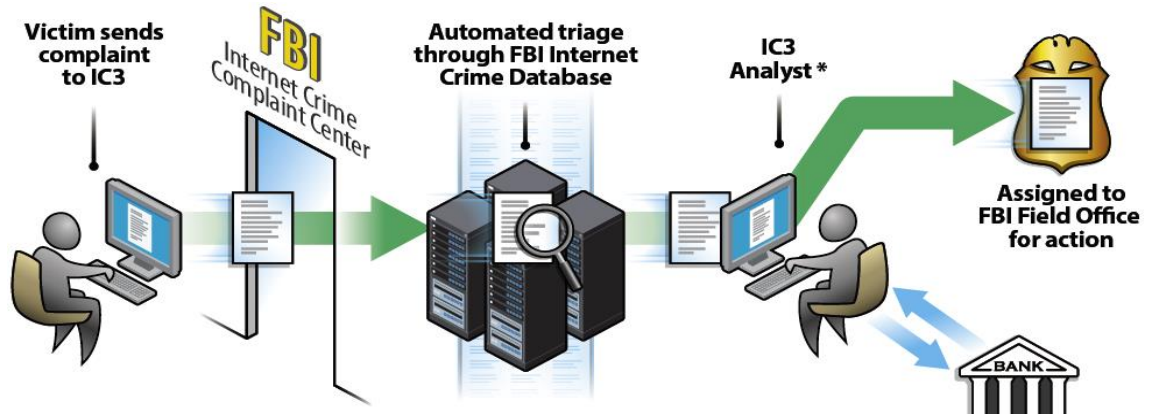
Rank	State	Loss	Rank	State	Loss
1	**California**	$643,230,534	30	**Wisconsin**	$26,069,500
2	**Florida**	$293,817,911	31	**Oklahoma**	$22,430,973
3	**Texas**	$278,320,107	32	**Idaho**	$20,844,974
4	**New York**	$203,437,635	33	**New Mexico**	$17,784,632
5	**Illinois**	$137,940,620	34	**Iowa**	$16,434,421
6	**Arizona**	$127,977,700	35	**Delaware**	$15,363,401
7	**Pennsylvania**	$117,427,238	36	**Arkansas**	$14,696,548
8	**New Jersey**	$104,087,085	37	**Kansas**	$13,900,498
9	**Virginia**	$94,037,054	38	**Kentucky**	$12,769,949
10	**Georgia**	$92,422,609	39	**West Virginia**	$11,829,064
11	**Washington**	$88,958,679	40	**New Hampshire**	$11,339,097
12	**North Carolina**	$77,364,165	41	**District of Columbia**	$10,645,609
13	**Maryland**	$72,384,277	42	**Nebraska**	$9,642,093
14	**Ohio**	$64,434,384	43	**Mississippi**	$9,328,015
15	**Massachusetts**	$63,771,718	44	**Alaska**	$8,732,051
16	**Michigan**	$58,552,106	45	**Montana**	$7,917,918
17	**Minnesota**	$54,886,221	46	**Rhode Island**	$7,377,668
18	**Colorado**	$54,454,519	47	**Maine**	$7,162,225
19	**Missouri**	$52,775,722	48	**Wyoming**	$5,689,358
20	**Nevada**	$45,239,607	49	**Vermont**	$4,880,944
21	**Oregon**	$44,271,609	50	**North Dakota**	$4,405,702
22	**South Carolina**	$43,758,611	51	**South Dakota**	$3,804,551
23	**Tennessee**	$43,753,076	52	**Puerto Rico**	$2,845,110
24	**Connecticut**	$38,693,615	53	**Guam**	$597,922
25	**Indiana**	$37,812,966	54	**United States Minor Outlying**	$335,268
26	**Alabama**	$33,942,649	55	**American Samoa**	$297,660
27	**Louisiana**	$31,037,438	56	**Virgin Islands, U.S.**	$88,477
28	**Hawaii**	$27,965,497	57	**Northern Mariana Islands**	$9,489
29	**Utah**	$26,101,164			

*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.

THE IC3 RECOVERY ASSET TEAM (RAT)

The FBI IC3 Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for individuals who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[4]



* If criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

In 2023, the IC3 RAT initiated the Financial Fraud Kill Chain (FFKC) for 626 incidents involving complaints filed by individuals over 60, with a combined total reported loss of $58,176,605. The RAT was able to freeze $32,079,603 of the funds with the support of domestic banking partners. The top reported crime types for these specific FFKC incidents were Tech Support scams, BEC scams and BEC scams with a Real Estate nexus, and Investments scams.

Guidance for Individuals who send Wire Transfers

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device.

[4] Accessibility description: Image shows the different stages of a complaint in the RAT process.

COMMON FRAUDS COMMONLY AFFECTING OVER 60 INDIVIDUALS

Call Center Fraud: Tech and Customer Support / Government Impersonation

Illegal call centers defraud thousands of people each year. Two categories of fraud reported to IC3, Tech/Customer Support and Government Impersonation, are responsible for over $1.3 billion in losses among all complaints reported to IC3.

Call centers overwhelmingly target older adults, to devastating effect. Almost half the complainants reported to be over 60 (40%), and experienced 58% of the losses (almost $770 million). Complainants over the age of 60 lost more to these scams than all other age groups combined, and reportedly remortgaged/foreclosed homes, emptied retirement accounts, and borrowed from family and friends to cover losses in these scams. Some incidents have resulted in suicide because of shame or loss of sustainable income.

	Complaints	Losses	Trend
Government Impersonation	3,517	$179,646,103	▲ 32%
Tech and Customer Support	17,696	$589,759,770	▲ 3%
TOTAL	**21,213**	**$769,405,872**	

In 2023, newer trends identified include the “Phantom Hacker” scam and the use of couriers to retrieve cash and precious metals from individuals in call center-related scams. Additional information regarding “Phantom Hacker” is available in the published I-091223-PSA .

The use of cash, gold, and other precious metals by criminals are increasing. Criminals instruct individuals, many of whom are senior citizens, to protect their funds by liquidating their assets into cash and/or buy gold, silver, or other precious metals. Criminals then arrange for couriers to meet in-person to pick up the cash or precious metals. From May to December 2023, the IC3 saw an uptick in this activity with aggregated losses over $55 million.

IC3 2023 PSAs Related to Tech/Customer Support and Government Impersonation

- "Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings
- Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies
- Criminals Pose as Chinese Authorities to Target US-based Chinese Community (简体中文版) (繁體中文版)

Investment

Investment fraud involves complex financial crimes often characterized as low-risk investments with guaranteed returns. They comprise of advanced fee frauds, Ponzi schemes, pyramid schemes, market manipulation fraud, real estate investing, and trust-based investing such as cryptocurrency investment scams. More than 6,400 complaints from individuals over the age of 60 reported losses over $1.2 billion to these schemes.

Most cryptocurrency investment scams are socially engineered and trust-enabled, usually initiating through a romance or confidence scam, and evolving into cryptocurrency investment scam. Criminals often target individuals using dating applications, social media platforms, professional networking sites, or encrypted messaging applications. Criminals use fictitious identities to develop relationships and establish rapport with targeted individuals.

IC3 publications in 2023 Related to Investment Fraud

- The FBI Warns of a Spike in Cryptocurrency Investment Schemes
- FBI Guidance for Cryptocurrency Scam Victims
- Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams
- Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition (ic3.gov)

Confidence/Romance Scams

Confidence/Romance scams encompass those designed to pull on an individual's "heartstrings". In 2023, the IC3 received reports from 6,740 individuals over the age of 60 who experienced almost $357 million in losses to Confidence/Romance scams.

Romance scams occur when a criminal adopts a fake online identity to gain an individual's affection or confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from an individual. The criminals will seem genuine, caring, and believable, with the intent to quickly establish a relationship and endear themselves to someone. They gain trust and eventually will ask for money. Scam artists often claim to be serving in the military or employed in a trade-based industry engaged in projects outside the U.S. This makes it easier to avoid meeting in person, and more plausible when they request money be sent overseas for a medical emergency or unexpected legal fee.

Also contained within this category are Grandparent Scams, which occur when a criminal impersonates a panicked loved one, usually a grandchild, nephew, or niece of an older person, and claims to be in trouble and needs money immediately. In 2023, the IC3 received over 200 complaints from people over the age of 60 reporting Grandparent Scams, with approximate losses of $2.3 million.

Sometimes, confidence/romance scams can evolve into sextortion if the individual has provided illicit pictures to the scammer. In 2023, complainants over the age of 60 reported 3,318 sextortion complaints with reported losses over $6 million.

IC3 2023 PSA Related to Confidence/Romance Fraud

- FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers

Cryptocurrency

In 2023, the IC3 received over 15,000 complaints from individuals over the age of 60 involving the use of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. Losses to these complaints totaled over $1.1 billion.

The largest losses among complainants over the age of 60 are from cryptocurrency investment scams, which account for approximately 64% of all losses related to cryptocurrency for this age group. Call center fraud, such as Tech and Customer Support scams and Government Impersonation, are second with approximately 16% of losses associated with cryptocurrency.

The use of cryptocurrency ATMs and kiosks has continued to increase as a payment mechanism, especially among Tech and Customer Support, Government Impersonation, and Confidence/Romance scams. Scammers convince targeted individuals to withdraw large sums of cash and deposit into cryptocurrency ATMs or kiosks at locations provided by the scammers. Once cash is deposited and converted into cryptocurrency, the scammer transfers it to other cryptocurrency accounts. Over 2,000 complaints were filed by individuals over the age of 60 regarding the use of cryptocurrency ATMs and kiosks.

COMPLAINTS FILE BY INDIVIDUALS OVER 60 WITH A CRYPTOCURRENCY NEXUS			
Crime Type	**Count**	**Crime Type**	**Count**
Investment	3,292	**Lottery/Sweepstakes/Inheritance**	57
Tech Support	2,076	**Employment**	50
Extortion	1,963	**Ransomware**	36
Confidence/Romance	810	**Overpayment**	30
Personal Data Breach	792	**BEC**	16
Government Impersonation	223	**Real Estate**	15
Spoofing	178	**Data Breach**	9
Advanced Fee	175	**Malware**	9
Credit Card/Check Fraud	144	**Harassment/Stalking**	6
Phishing	140	**IPR/Copyright and Counterfeit**	5
Non-payment/Non-Delivery	134	**Threats of Violence**	3
SIM Swap	98	**Botnet**	2
Identity Theft	97	**Crimes Against Children**	1
Other	71		

COMPLAINTS FILED BY INDIVIDUALS OVER 60 LOSSES WITH A CRYPTOCURRENCY NEXUS			
Crime Type	**Loss**	**Crime Type**	**Loss**
Investment	$716,466,087	**Lottery/Sweepstakes/Inheritance**	$3,517,513
Tech Support	$166,138,710	**Other**	$3,479,107
Confidence/Romance	$93,483,020	**Extortion**	$3,461,352
Personal Data Breach	$58,734,792	**Employment**	$956,324
Government Impersonation	$19,955,542	**Overpayment**	$499,037
SIM Swap	$11,211,168	**BEC**	$465,534
Phishing	$5,603,806	**Malware**	$69,963
Spoofing	$5,315,101	**Harassment/Stalking**	$51,240
Advanced Fee	$4,902,036	**Ransomware**	$37,500
Real Estate	$4,590,165	**Threats of Violence**	$21,769
Credit Card/Check Fraud	$4,560,408	**IPR/Copyright and Counterfeit**	$3,135
Non-payment/Non-Delivery	$4,526,507	**Crimes Against Children**	$1,300
Identity Theft	$3,816,394	**Botnet**	0
Data Breach	$3,622,102		

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 fraudsters 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 complainant'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 in an attempt 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 steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (account takeover) a fraudster obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer 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 person'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 descriptive data, such as crime type and adjusted loss.
- Descriptive data for complaints, such as crime type or loss, is variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which may change.
- Each complaint will only have one crime type.
- 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 ANNOUNCEMENTS PUBLISHED IN 2023

TITLE	PUBLISHED
Scammers Targeting Owners of Timeshares in Mexico	3/3/2023
Criminals Steal Cryptocurrency through Play-to-Earn Games	3/9/2023
The FBI Warns of a Spike in Cryptocurrency Investment Schemes	3/14/2023
Business Email Compromise Tactics Used to Facilitate the Acquisition of Commodities and Defrauding Vendors	3/24/2023
For-Profit Companies Charging Sextortion Victims for Assistance and Using Deceptive Tactics to Elicit Payments	4/7/2023
Criminals Pose as Chinese Authorities to Target US-based Chinese Community	4/10/2023
Multinational Non-Governmental Organizations Potentially Exploited in Aftermath of Earthquakes Affecting Turkey and Syria	4/28/2023
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
Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes (ic3.gov)	7/5/2023
Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies	7/18/2023
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
Cyber Criminals Targeting Victims through Mobile Beta-Testing Applications (ic3.gov)	8/14/2023
FBI Guidance for Cryptocurrency Scam Victims	8/24/2023
Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material	9/12/2023
"Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings	9/29/2023
Situation in Israel	10/10/2023
Cybercriminals are Targeting Plastic Surgery Offices and Patients	10/17/2023
Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers	10/18/2023
Scammers Solicit Fake Humanitarian Donations	10/24/2023
Threats Associated with the Israel-HAMAS Conflict	10/26/2023
2023 Holiday Shopping Scams	11/15/2023
FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers	11/17/2023
Threat of Violence Likely Heightened Throughout Winter	12/12/2023