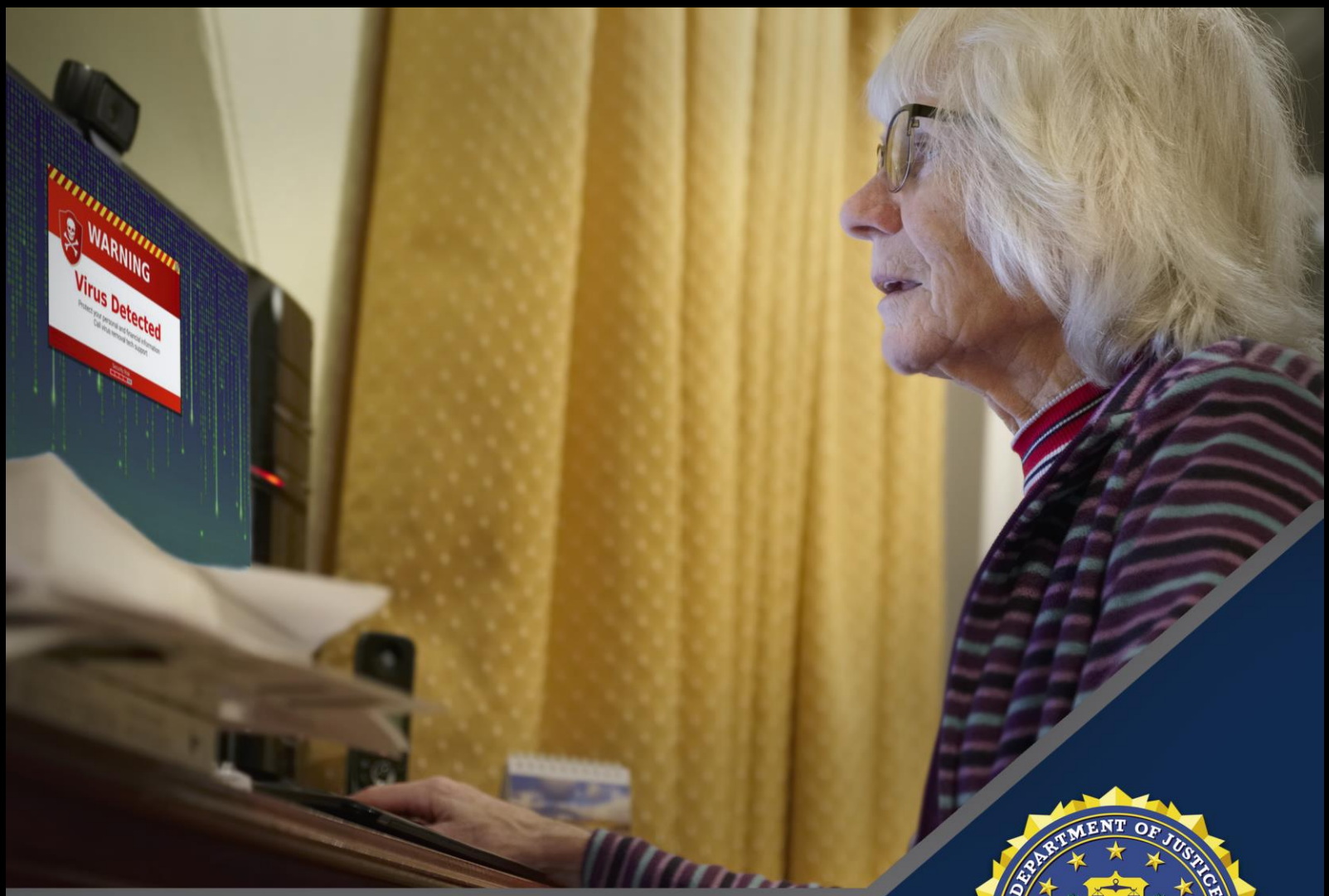


FEDERAL BUREAU of INVESTIGATION

Elder Fraud Report

2022

INTERNET CRIME COMPLAINT CENTER

2022 ELDER FRAUD REPORT

TABLE OF CONTENTS

Introduction 3
By the Numbers 4
2022 Victims by Age Group 5
VICTIMS OVER 60 Reporting for past five years 5
2022 Crime Types 6
LAST THREE YEARS COMPARISON 8
LAST THREE YEARS COMPARISON, *Continued* 9
2022 OVERALL STATE STATISTICS 10
2022 OVERALL STATE STATISTICS, *Continued* 11
COMMON FRAUDS AFFECTING Victims OVER 60 12
Call Center Fraud: Tech and Customer Support / Government Impersonation 12
Investment 13
Lottery/Sweepstakes/Inheritance 13
Confidence/Romance Scams 14
Extortion 14
Non-Payment/Non-Delivery 15
Cryptocurrency 15
Appendix A: Definitions 17
Appendix B: Additional Information about IC3 Data 20
Appendix C: Tips for Protection 21
Appendix D: referenced publications 22

INTRODUCTION

Dear Reader,

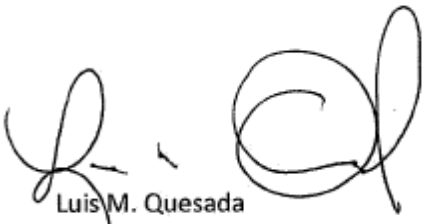
The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is a central intake point for victims to report fraud. IC3 shares the complaints it receives with FBI field offices and other law enforcement and regulatory agencies for further investigation or action, as appropriate. Along with the Department of Justice's Elder Fraud Initiative and other partners, the FBI is continually dedicated to identifying the perpetrators of these schemes and bringing them to justice.

Every day, the IC3 receives thousands of complaints reporting a wide variety of schemes, many of them targeting seniors. These complaints are analyzed and aggregated to identify trends and help develop strategies to combat these schemes and protect potential victims from loss.

In 2022, total losses reported to the IC3 by elderly victims increased 84% from 2021. Tech and Customer Support schemes continued to be the most common type of fraud reported, with 17,800 complaints filed by victims over 60. Monetary losses due to Investment Fraud reported by victims over 60 increased over 300%, more than any other kind of fraud, largely due to the rising trend of crypto-investment scams. In almost every crime type tracked by the IC3, losses involving cryptocurrency increased. Overall, cryptocurrency-related losses reported by the elderly increased by 350%.

As in previous years, the FBI is publishing the 2022 IC3 Elder Fraud Annual Report in hopes of bringing awareness to this problem and preventing future victimization. I encourage you to share the information from this report with your friends and families and take the opportunity to talk about these scams.

We also encourage the public to report any internet-related fraud, even attempted fraud, to the IC3 as soon as possible. Providing detailed information, including complete summaries and financial transactions, assists the FBI with investigating and disrupting the frauds that are devastating our citizens.



Luis M. Quesada
Assistant Director
Federal Bureau of Investigation
Criminal Investigative Division

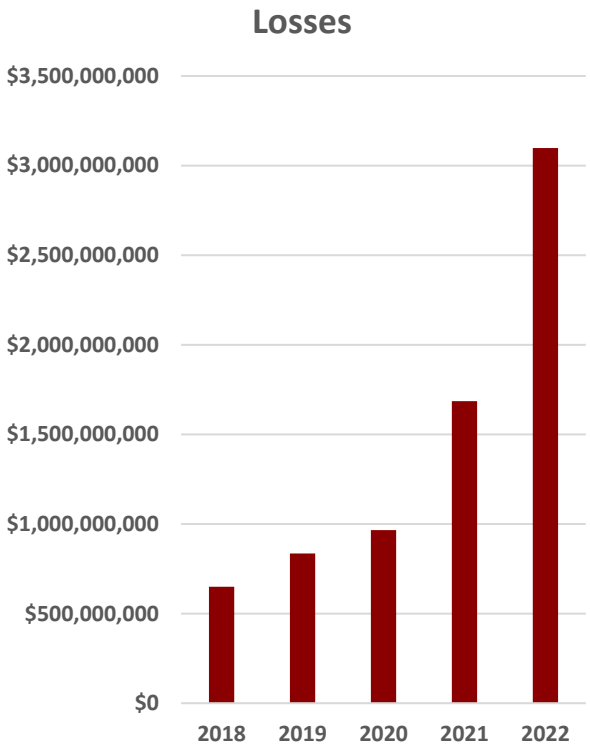
BY THE NUMBERS

[1] Accessibility description: Image depicts key statistics regarding victims over 60 complaints. The total number of complaints received in 2022 was 88,262. Total losses of $3.1 billion were reported. Victims over 60 experienced 84 percent increase in losses from 2021. The average loss per victim was $35,101. 5,456 victims lost more than $100,000.

2022 VICTIMS BY AGE GROUP

VICTIMS		
Age Range[2]	Total Count	Total Loss
Under 20	15,782	$210,482,785
20 - 29	57,978	$383,137,848
30 - 39	94,506	$1,277,981,506
40 - 49	87,526	$1,551,296,778
50 - 59	64,551	$1,830,440,552
Over 60	88,262	$3,098,100,121

VICTIMS OVER 60 REPORTING FOR PAST FIVE YEARS[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 Counts and Losses for Victims over 60 from 2018 – 2022.

2022 CRIME TYPES

VICTIMS OVER 60 COUNTS			
Crime Type	**Victims**	**Crime Type**	**Victims**
Tech Support	17,810	**Lottery/Sweepstakes/Inheritance**	2,388
Non-payment/Non-Delivery	7,985	**Other**	2,016
Personal Data Breach	7,849	**Real Estate**	1,862
Confidence/Romance	7,166	**Employment**	1,286
Credit Card/Check Fraud	4,956	**Overpayment**	1,183
Identity Theft	4,825	**Harassment/Stalking**	754
Investment	4,661	**Data Breach**	333
Extortion	4,285	**SIM Swap**	301
Spoofing	4,201	**IPR/Copyright and Counterfeit**	235
Phishing	4,168	**Ransomware**	215
BEC*	3,938	**Threats of Violence**	166
(Reporting a potential business victimization)	*2,552*	**Malware**	125
(Reporting a personal victimization)	*1,386*	**Crimes Against Children**	84
Government Impersonation	3,425	**Botnet**	33
Advanced Fee	3,153		

Descriptors*	
Cryptocurrency	6,854
Cryptocurrency Wallet	3,137

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 victim counts: A whole number is given to depict the overall victim count and is then broken out into separate counts to identify when a Victim over 60 may be reporting victimization on behalf of a business or personally.

2022 CRIME TYPES, *Continued*

VICTIM OVER 60 LOSSES			
Crime Type	**Loss**	**Crime Type**	**Loss**
Investment	$990,235,119	**Spoofing**	$22,261,276
Tech Support	$587,831,698	**SIM Swap**	$19,515,629
BEC*	$477,342,728	**Data Breach**	$17,681,749
(Reporting a potential business loss)	*$369,773,371*	**Extortion**	$15,555,047
(Reporting a personal loss)	*$107,569,357*	**Phishing**	$14,453,929
Confidence/Romance	$419,768,142	**Overpayment**	$10,977,231
Government Impersonation	$136,500,338	**Employment**	$6,403,021
Real Estate	$135,239,020	**Malware**	$1,851,421
Personal Data Breach	$127,736,607	**Threats of Violence**	$376,458
Lottery/Sweepstakes/Inheritance	$69,845,106	**Harassment/Stalking**	$254,659
Credit Card/Check Fraud	$61,649,198	**Ransomware****	$210,052
Non-payment/Non-Delivery	$51,531,615	**IPR/Copyright and Counterfeit**	$203,140
Advanced Fee	$49,322,099	**Botnet**	$120,621
Identity Theft	$42,653,578	**Crimes Against Children**	$48,373
Other	$31,410,237		

Descriptors*	
Cryptocurrency	$827,633,473
Cryptocurrency Wallet	$260,696,578

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 victim losses: A whole number is given to depict the overall victim loss and is then broken out into separate counts to identify when a victim over 60 may be reporting victimization 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 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.

LAST THREE YEARS COMPARISON

OVER 60 VICTIM COUNT			
Crime Type	**2022**	**2021**	**2020**
Advanced Fee	3,153	3,029	3,008
BEC	3,938	3,755	3,530
(Reporting a potential business loss)	*2,552*	*2,143*	--
(Reporting a personal loss)	*1,386*	*1,612*	--
Botnet *	33	--	--
Confidence/Romance	7,166	7,658	6,817
Credit Card/Check Fraud	4,956	3,164	3,195
Crimes Against Children	84	42	58
Data Breach	333	158	285
Employment	1,286	1,408	1,867
Extortion	4,285	5,987	23,100
Government Impersonation	3,425	3,319	4,159
Harassment/Stalking *	754	--	--
IPR/Copyright and Counterfeit	235	686	552
Identity Theft	4,825	8,902	7,581
Investment	4,661	2,104	1,062
Lottery/Sweepstakes/Inheritance	2,388	2,607	3,774
Malware	125	134	287
Non-payment/Non-Delivery	7,985	13,220	14,534
Other	2,016	2,933	3,259
Overpayment	1,183	1,448	2,196
Personal Data Breach	7,849	6,189	6,121
Phishing	4,168	5,831	7,353
Ransomware	215	365	365
Real Estate	1,862	1,764	1,882
SIM Swap *	301	--	--
Spoofing	4,201	3,936	7,279
Tech Support	17,810	13,900	9,429
Threats of Violence *	166	719	1,699
Cryptocurrency/Cryptocurrency Wallet	9,991	5,109	9,447

*New Crime Type added in 2022.

LAST THREE YEARS COMPARISON, *Continued*

OVER 60 VICTIM LOSS			
Crime Type	**2022**	**2021**	**2020**
Advanced Fee	$49,322,099	$36,464,491	$33,184,114
BEC	$477,342,728	$355,805,098	$168,793,903
(Reporting a potential business loss)	$369,773,371	$277,547,598	--*
(Reporting a personal loss)	$107,569,357	$78,257,500	--
Botnet *	$120,621	--	--
Confidence/Romance	$419,768,142	$432,081,901	$281,134,006
Credit Card/Check Fraud	$61,649,198	$39,019,072	$20,780,800
Crimes Against Children	$48,373	$550	$411,349
Data Breach	$17,681,749	$7,095,746	$10,148,817
Employment	$6,403,021	$9,610,615	$16,092,611
Extortion	$15,555,047	$19,533,187	$18,503,168
Government Impersonation	$136,500,338	$69,186,858	$45,909,970
Harassment/Stalking *	$254,659	--	--
IPR/Copyright and Counterfeit	$203,140	$4,954,221	$479,375
Identity Theft	$42,653,578	$59,022,153	$39,006,465
Investment	$990,235,119	$239,474,635	$98,040,940
Lottery/Sweepstakes/Inheritance	$69,845,106	$53,557,330	$38,804,343
Malware	$1,851,421	$1,177,864	$671,667
Non-payment/Non-Delivery	$51,531,615	$52,023,580	$40,377,167
Other	$31,410,237	$22,196,542	$49,689,594
Overpayment	$10,977,231	$9,214,129	$11,212,323
Personal Data Breach	$127,736,607	$103,688,489	$24,641,539
Phishing	$14,453,929	$9,166,217	$18,829,999
Ransomware	$210,052	$424,852	$5,332,312
Real Estate	$135,239,020	$102,071,631	$50,098,565
SIM Swap *	$19,515,629	--	--
Spoofing	$22,261,276	$19,473,060	$40,886,040
Tech Support	$587,831,698	$237,931,278	$116,415,126
Threats of Violence *	$376,458	$361,549	$1,112,825
Cryptocurrency/Cryptocurrency Wallet	$1,088,330,051	$241,143,166	$55,056,901

*New Crime Type added in 2022.

2022 OVERALL STATE STATISTICS

VICTIMS OVER 60 BY STATE*

Rank	State	Victims	Rank	State	Victims
1	California	11,517	30	Utah	741
2	Florida	8,480	31	New Mexico	728
3	Texas	5,674	32	Louisiana	721
4	New York	4,239	33	Arkansas	649
5	Arizona	3,543	34	Iowa	557
6	Ohio	3,099	35	Kansas	472
7	Colorado	2,925	36	Idaho	466
8	Pennsylvania	2,901	37	Maine	459
9	Illinois	2,495	38	Hawaii	399
10	Virginia	2,447	39	New Hampshire	372
11	New Jersey	2,368	40	Mississippi	356
12	Washington	2,335	41	West Virginia	340
13	Michigan	2,243	42	Nebraska	335
14	Georgia	2,005	43	South Dakota	331
15	North Carolina	1,959	44	Alaska	316
16	Nevada	1,914	45	Delaware	305
17	Maryland	1,724	46	Montana	295
18	Massachusetts	1,653	47	Rhode Island	219
19	Missouri	1,503	48	Wyoming	209
20	Tennessee	1,462	49	District of Columbia	195
21	Oregon	1,314	50	Puerto Rico	190
22	South Carolina	1,312	51	Vermont	188
23	Minnesota	1,185	52	North Dakota	109
24	Indiana	1,172	53	United States Minor Outlying Islands	21
25	Wisconsin	1,029	54	Virgin Islands, U.S.	19
26	Kentucky	937	55	Guam	15
27	Alabama	916	56	American Samoa	8
28	Connecticut	908	57	Northern Mariana Islands	2
29	Oklahoma	790			

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

2022 OVERALL STATE STATISTICS, *Continued*

VICTIMS OVER 60 LOSSES BY STATE*

Rank	State	Loss	Rank	State	Loss
1	California	$624,509,520	30	Arkansas	$24,314,902
2	Florida	$328,114,489	31	Kentucky	$22,494,352
3	Texas	$243,067,545	32	Oklahoma	$19,455,718
4	New York	$212,045,216	33	Idaho	$18,984,217
5	Washington	$96,213,728	34	Louisiana	$18,374,982
6	New Jersey	$92,712,866	35	Hawaii	$16,334,492
7	Arizona	$82,255,007	36	Nebraska	$16,117,012
8	Pennsylvania	$80,250,904	37	New Hampshire	$14,665,788
9	Georgia	$78,736,227	38	Delaware	$14,023,134
10	Illinois	$75,905,639	39	New Mexico	$13,382,175
11	Massachusetts	$70,100,868	40	Maine	$12,741,072
12	Colorado	$66,826,911	41	Iowa	$12,082,177
13	Maryland	$63,662,134	42	Alaska	$7,646,998
14	North Carolina	$63,464,255	43	Rhode Island	$7,314,666
15	Virginia	$60,641,280	44	Montana	$6,968,157
16	Michigan	$52,520,999	45	Vermont	$5,663,838
17	Ohio	$51,041,223	46	South Dakota	$5,634,355
18	Oregon	$46,324,137	47	Mississippi	$5,459,509
19	Minnesota	$39,211,355	48	Wyoming	$5,265,283
20	Nevada	$38,563,008	49	West Virginia	$4,460,124
21	Tennessee	$36,568,079	50	District of Columbia	$4,399,340
22	South Carolina	$35,610,994	51	North Dakota	$3,054,570
23	Missouri	$34,961,102	52	Puerto Rico	$2,363,832
24	Connecticut	$33,660,316	53	United States Minor Outlying Islands	$564,494
25	Wisconsin	$31,024,115	54	Guam	$163,555
26	Utah	$27,657,757	55	Virgin Islands, U.S.	$142,162
27	Alabama	$26,756,713	56	Northern Mariana Islands	$15,500
28	Indiana	$26,497,603	57	American Samoa	$14,136
29	Kansas	$24,435,433			

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

COMMON FRAUDS AFFECTING VICTIMS OVER 60

Call Center Fraud: Tech and Customer Support / Government Impersonation

Illegal call centers defraud thousands of victims each year. Two categories of fraud reported to the IC3, Tech/Customer Support and Government Impersonation, are responsible for over $1 billion in losses to victims.

Call centers overwhelmingly target the elderly, with devastating effects. Almost half the victims report to be over 60 (46%), and experience 69% of the losses (over $724 million). Victims over 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. Almost 100 elderly victims reportedly lost over $1 million to these scams, while the majority lost between $1,000 - $10,000.

	Victims	***Losses***	***Trend***
Government Impersonation	*3,425*	*$136,500,338*	▲ *97%*
Tech and Customer Support	*17,810*	*$587,831,698*	▲ *147%*
TOTAL	***21,235***	***$724,332,036***	

While the number of victims and losses from Government Impersonation scams are significantly lower, the fraud tends to occur over a longer period as it takes the victim longer to realize they are caught in a scam. Tech and Customer Support scammers take advantage of victims' unfamiliarity with technology, online banking, and newer payment methods, like cryptocurrency, to quickly take as much money as possible. It is not uncommon for the scammers to execute a combination of the two scams or re-victimize a previous victim with the other form of scam.

The scams primarily emanate from call centers in South Asia, mainly India. In response to the increasing victimization, the Department of Justice (DOJ) and the FBI are collaborating with law enforcement in India, such as the Central Bureau of Investigation in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud. This cooperation has secured the testimony of U.S. victims of call center fraud for use in enforcement proceedings against the alleged perpetrators.

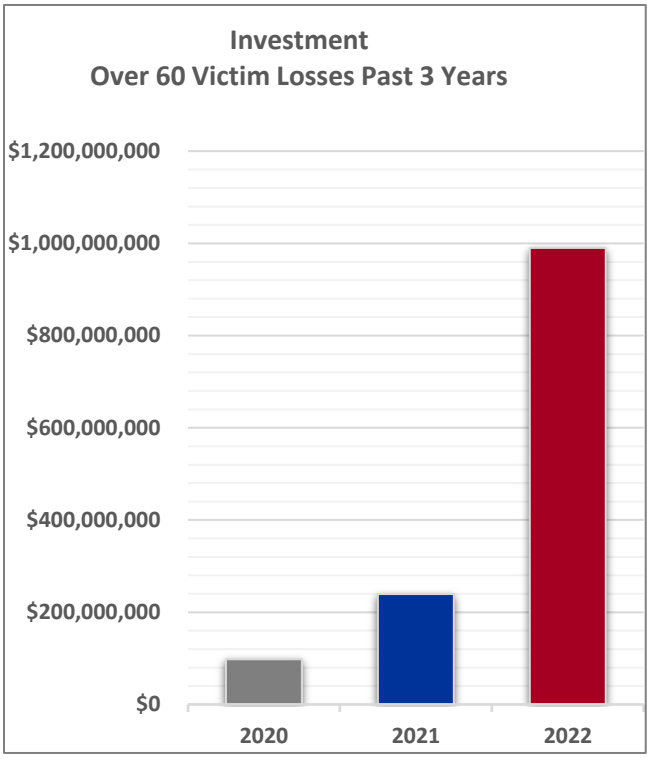
In 2022, with the assistance of U.S. law enforcement, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these cyber-enabled financial crimes and global telemarketing frauds.

To learn more about these types of scams, please see these 2022-published Public Service Announcements on the IC3 website and recently published podcast on FBI.gov[4]

[4] See Appendix D: Referenced Publications

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 pig butchering.



Trust-based Investment scams represent the biggest portion of losses for investment in 2022. These scams often target individuals online and most commonly involve a form of cryptocurrency. The scammers aim to gain the victim's trust and offer an opportunity to invest in a low-risk, and unusually high-yield type of scam. Victims over 60 are pressured into accessing their retirement accounts, the equity of their home, or even convinced to go into debt to invest as much money as possible into the fraudulent scheme. This can be devastating to elderly victims as their income is typically limited and many lose their entire life savings. [5]

More than 4,500 victims over 60 reported losses slightly under $1 billion.

Lottery/Sweepstakes/Inheritance

In 2022, the IC3 received over 2,300 reports of elderly victims in Lottery/Sweepstakes/Inheritance scams. Victims lost almost $70 million to these types of fraud.

The initial contact in a Lottery/Sweepstakes scam is often a call, an email, a social media notification, or a piece of mail offering congratulations for winning a big contest, lottery, or sweepstakes the victim did not enter. To claim their prize, the victim is required to pay upfront fees and taxes. The subjects will continue to call victims for months or even years, promising the big prize is only one more payment away.

Inheritance scams function very similarly as the victim is informed an unknown, distant relative has left a large inheritance to the victim. The victim is required to pay taxes and fees to receive the inheritance money.

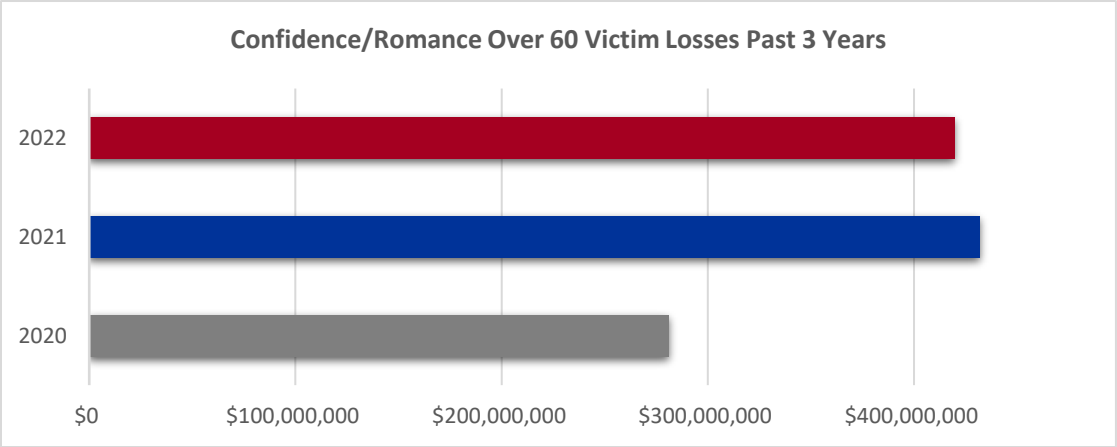
[5] See Appendix D: Referenced Publications

Confidence/Romance Scams

Confidence/Romance scams encompass those designed to pull on a victim's "heartstrings". In 2022, the IC3 received reports from 7,166 victims over 60 who experienced almost $419 million in losses to Confidence/Romance scams.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out Romance scams are experts at what they do and will seem genuine, caring, and believable. The scammer's intention is to quickly establish a relationship, endear themselves to the victim, gain trust, and eventually ask for money. Scam artists often say they are in the military, or a trades-based industry engaged in projects outside the U.S. That 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.

Grandparent Scams also fall into this category, where criminals impersonate a panicked loved one, usually a grandchild, nephew, or niece of an elderly person. The loved one claims to be in trouble and needs money immediately. In 2022, almost 400 victims over 60 reported Grandparent scams, with approximate losses of $3.8 million.



Extortion

Extortion occurs when a criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is used in various schemes reported to the IC3, including email extortion attacks, hitman schemes, government extortion, and sextortion. In 2022, over 4,200 victims over 60 reported incidences of extortion, with losses over $15.5 million.

Almost half of extortion victims over 60 reported to be victims of sextortion. Most believed they were in a relationship with the victim and shared sensitive photos or information which were then later used to sextort them.

Non-Payment/Non-Delivery

Elderly victims filed almost 8,000 Non-Payment/Non-Delivery complaints experiencing losses over $51 million in 2022, making Non-Delivery of products the second most reported fraud among the elderly.

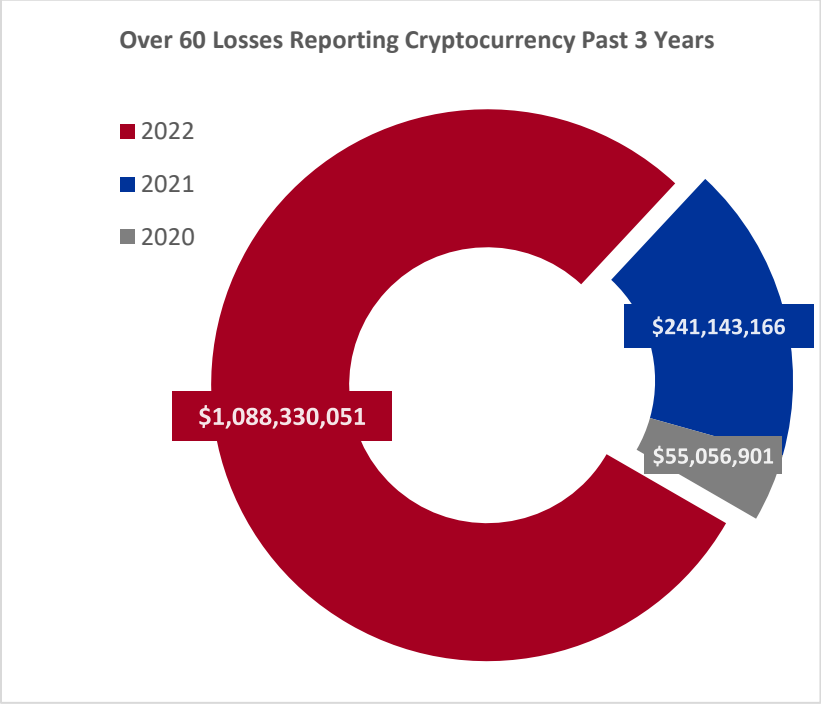
More elderly people are joining social media outlets to connect with others. The combination of online shopping and social media creates easy venues for scammers to post false advertisements. Many victims report ordering items from links advertised on social media and either receiving nothing at all or receiving something completely unlike the advertised item.

Cryptocurrency

In 2022, the IC3 received almost 10,000 complaints from victims over 60 involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. Losses of these victims totaled over $1 billion.

Cryptocurrency is becoming a preferred payment method for all types of scams – SIM Swaps, Tech/Customer Support fraud, Employment schemes, Romance scams, and even some Auction fraud. It is extremely pervasive in Investment scams, where losses can reach into the hundreds of thousands of dollars per victim.

The largest losses among victims over 60 are cryptocurrency-related Investment scams, which accounts for approximately 66% 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 15% of losses associated to cryptocurrency.



The IC3 published multiple PSAs depicting how cryptocurrency is exploited in frauds and scams, particularly the use of cryptocurrency ATMs, crypto investments, and crypto support impersonations.[6]

[6] [6] See Appendix D: Referenced Publications

VICTIMS OVER 60 WITH A CRYPTOCURRENCY NEXUS			
Crime Type	**Victims**	**Crime Type**	**Victims**
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		

VICTIM 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 Fraud: 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 the victims 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: 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.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; or, forged websites used to mislead and gather personal information. Often used in connection with other crime types.

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

- Each complaint is reviewed by an IC3 analyst. The analyst categorizes the complaint according to the crime type(s) that are appropriate. Additionally, the analyst will adjust the loss amount if the complaint data does not support the loss amount reported.
- One complaint may have multiple crime types.
- 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.
- Victim is identified as the individual filing a complaint.
- Subject is identified as the individual perpetrating the scam as reported by the victim.
- “Count by Subject per state” is the number of subjects per state, as reported by victims.
- “Subject earnings per Destination State” is the amount swindled by the subject, as reported by the victim, per state.

APPENDIX C: TIPS FOR PROTECTION

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Resist the pressure to act quickly. Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Be cautious of unsolicited phone calls, mailings, and door-to-door service offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- Make sure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.
- Legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals; nor, demand immediate payment or require payment via prepaid cards, wire transfers, cryptocurrency, or mailed cash.
- Never give unknown, unverified persons remote access to devices or accounts.
- Be careful what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.
- Take precautions to protect your identity if a criminal gains access to your device or account. Immediately contact your financial institutions to place protections on your accounts and monitor your accounts and personal information for suspicious activity.
- Legitimate lotteries and beneficiaries do not need to pay upfront taxes and fees to claim a prize or inheritance. Playing foreign lotteries in any form is a violation of federal law.
- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Government or law enforcement officials will not demand payment by cryptocurrency, prepaid cards, wire transfers, or overnight mailed cash, nor contact a subject by phone to notify they are under investigation.

APPENDIX D: REFERENCED PUBLICATIONS

Internet Crime Complaint Center (IC3) | FBI Warns of the Impersonation of Law Enforcement and Government Officials, published 03/07/2022.

Internet Crime Complaint Center (IC3) | Technical and Customer Support Fraud, published 03/16/2022.

Internet Crime Complaint Center (IC3) | Cryptocurrency Investment Schemes, published 10/03/2022.

Internet Crime Complaint Center (IC3) | The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment, published 11/04/2021.

Internet Crime Complaint Center (IC3) | Scammers Using Computer-Technical Support Impersonation Scams to Target Victims and Conduct Wire Transfers, published 11/10/2022.

Inside the FBI Podcast: Hanging Up on Tech Support Scams — FBI, published 11/22/2022.