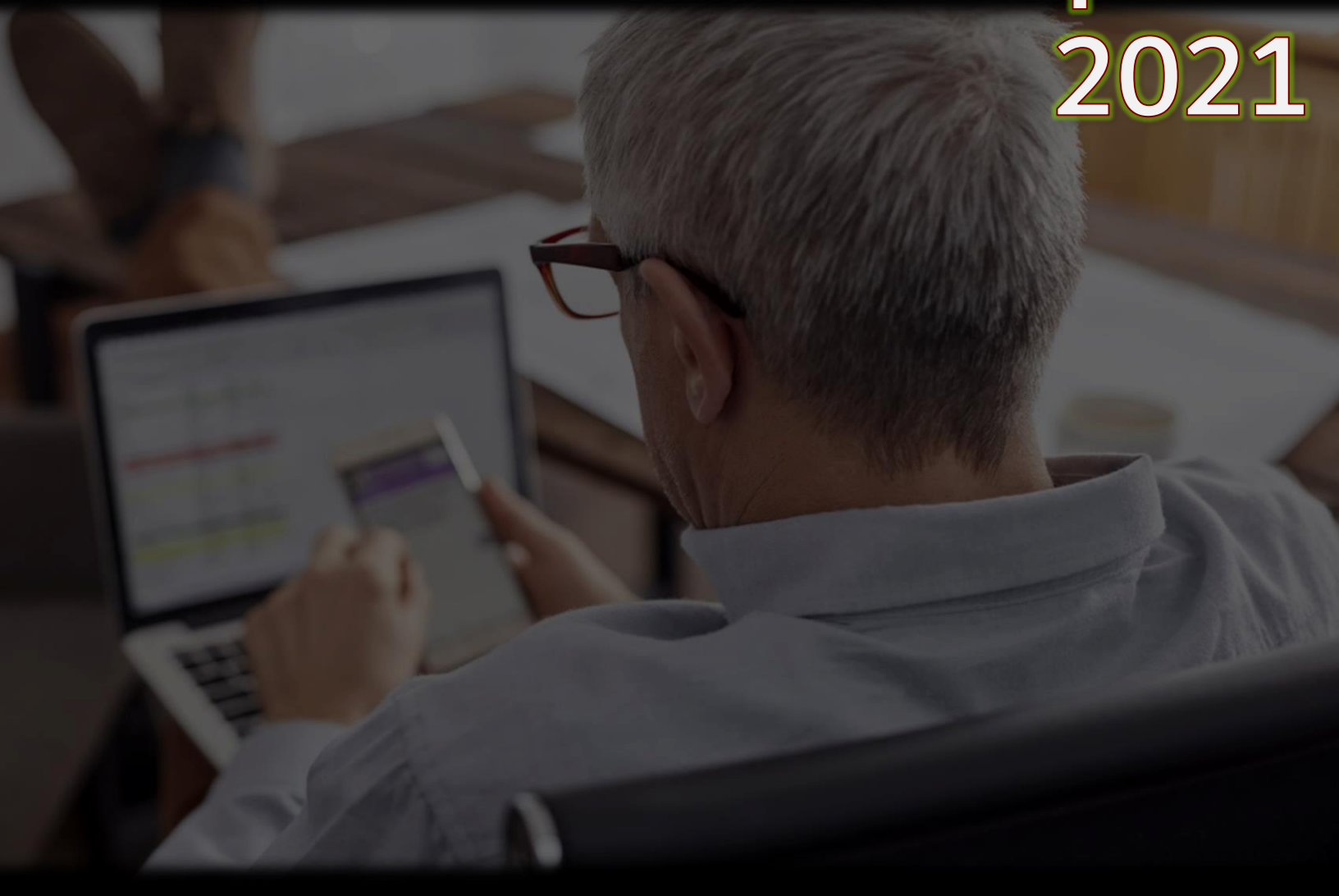
Elder Fraud Report 2021



2021 ELDER FRAUD REPORT

TABLE OF CONTENTS

Introduction 3
By the Numbers 4
2021 Victims by Age Group 5
Over 60 Victim Reporting for past five years 5
2021 – STATES BY NUMBER OF OVER 60 VICTIMS 6
2021 – STATES BY LOSSES OF OVER 60 VICTIMS 6
2021 Crime Types 7
LAST 3 YEARS COMPARISON 9
LAST 3 YEARS COMPARISON, *Continued* 10
2021 OVERALL STATE STATISTICS 11
2021 OVERALL STATE STATISTICS, *Continued* 12
COMMON FRAUDS AFFECTING OVER 60 VICTIMS 13
Tech Support Fraud 13
Confidence Fraud/Romance Scams 13
Lottery/Sweepstakes/Inheritance 15
Government Impersonation 15
Investment 16
Cryptocurrency 16
Appendix A: Definitions 17
Appendix B: Additional information about IC3 Data 20
Appendix C: 2021 – STATE VICTIMS PER CAPITA 21
2021 – STATES BY NUMBER OF OVER 60 VICTIMS PER CAPITA 23
2021 – STATES BY LOSSES OF OVER 60 VICTIMS PER CAPITA 23

INTRODUCTION

Dear Reader,

Working with the Department of Justice Elder Fraud Initiative and other internal and external partners, the FBI is committed to identifying, investigating, and prosecuting criminals who target seniors. The Internet Crime Complaint Center (IC3) is a key component in this endeavor, as it provides victims a venue to identify the subject and the fraud committed against them.

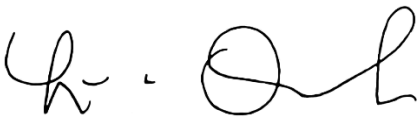
Through this voluntary submission of information, the IC3 receives and tracks thousands of complaints each day. These complaints contain the details of multiple types of schemes, including romance scams, investment fraud, government impersonation, and tech support fraud.

The number of elderly victims has risen at an alarming rate, while the loss amounts are even more staggering. In 2021, over 92,000 victims over the age of 60 reported losses of $1.7 billion to the IC3. This represents a 74 percent increase in losses over losses reported in 2020.

As a result of these trends and the emphasis by the FBI on protecting our seniors, the FBI is publishing the 2021 IC3 Elder Fraud Annual Report. This information is a companion report to the 2021 IC3 Annual Report released in March 2022. These reports, along with other publications, are available at www.ic3.gov.

The intent of this information is to educate, warn, and protect potential victims of all ages. Highlighting the crimes specifically affecting seniors will it be possible to ensure the necessary emphasis and resources are allocated to address this problem.

For those who unfortunately fall victim to these criminal tactics, please know the information you provide to the FBI is vital in bringing the criminals responsible to justice.



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

BY THE NUMBERS

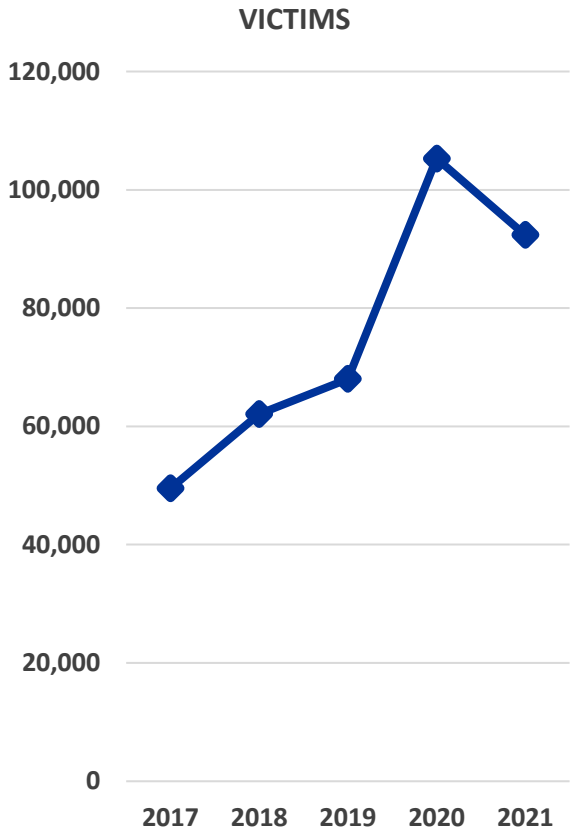
IC3 Over 60 Victims by the Numbers[1]

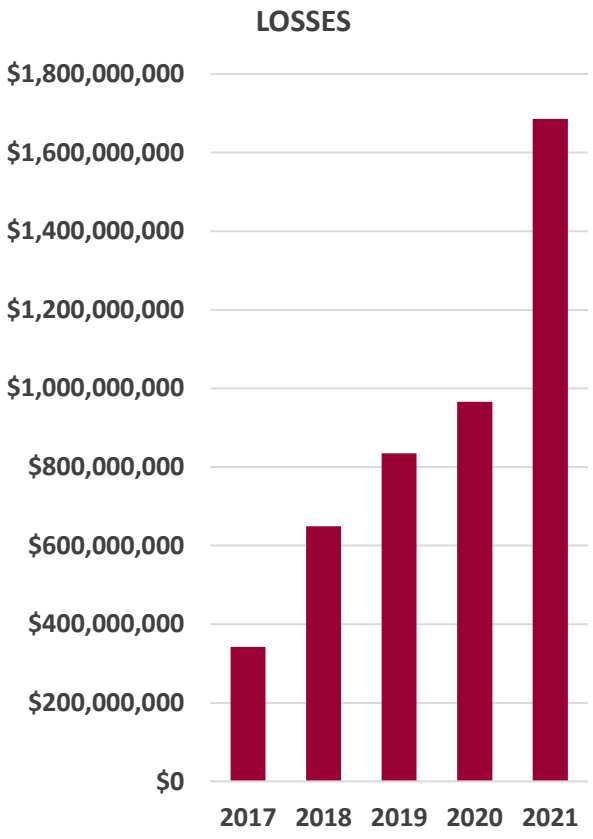
[1] Accessibility description: Image depicts key statistics regarding Over 60 complaints. The total number of complaints received in 2021 was 92,371. Total losses of $1.7 billion were reported. Over 60 victims experienced 24 percent of the total loss of all IC3 complaints received in 2021. 3,133 victims lost more than $100,000. The average loss per victim was $18,246.

2021 VICTIMS BY AGE GROUP

VICTIMS		
Age Range[2]	Total Count	Total Loss
Under 20	14,919	$101,435,178
20 - 29	69,390	$431,191,702
30 - 39	88,448	$937,386,500
40 - 49	89,184	$1,192,890,255
50 - 59	74,460	$1,261,591,978
Over 60	92,371	$1,685,017,829

OVER 60 VICTIM REPORTING FOR PAST FIVE YEARS[3]

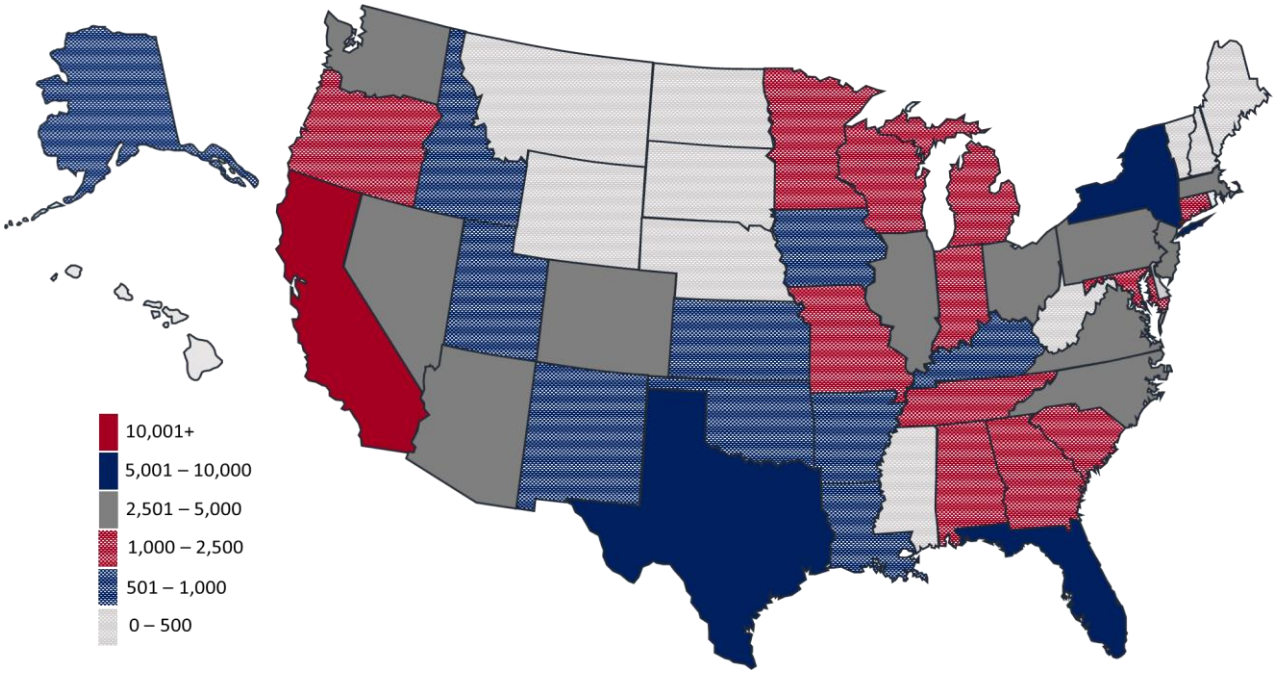




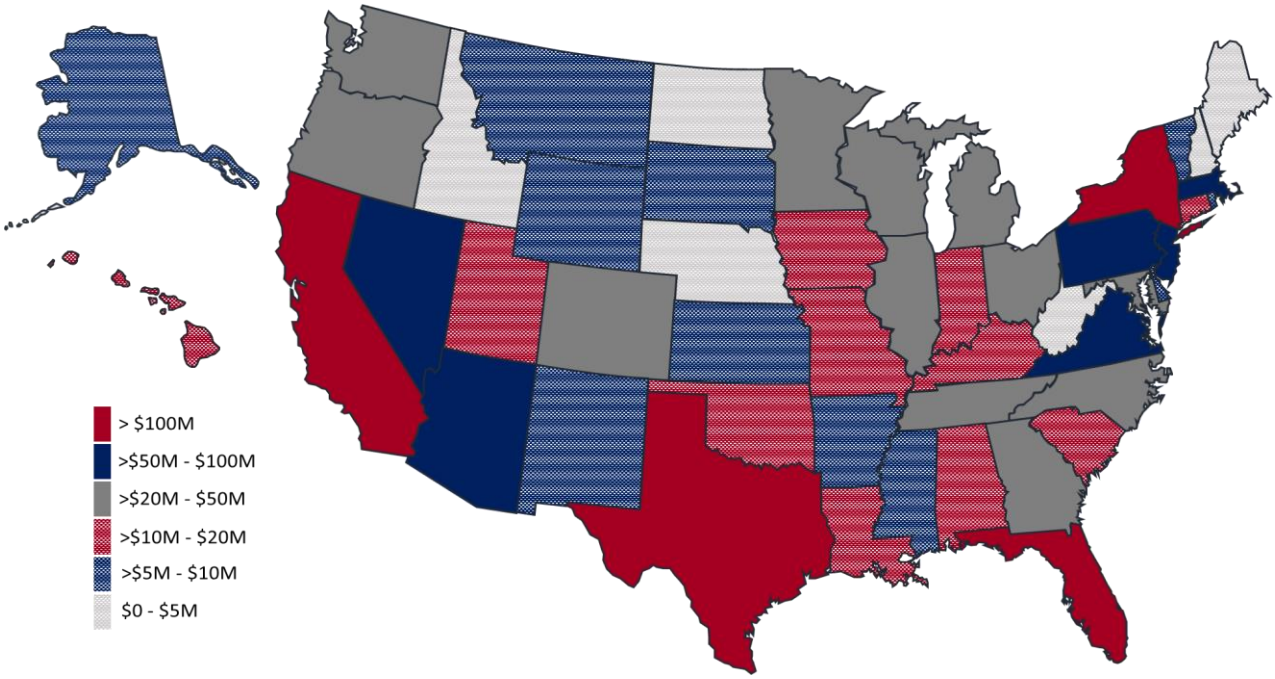
[2] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

[3] Charts describe Over 60 Victim Counts and Losses from 2017 – 2021.

2021 – STATES BY NUMBER OF OVER 60 VICTIMS[4]



2021 – STATES BY LOSSES OF OVER 60 VICTIMS



[4] Accessibility description: Image depicts a map of the United States color-coded by victim counts and losses. Please see Appendix B for more information regarding IC3 data.

2021 CRIME TYPES

OVER 60 VICTIM COUNT			
Crime Type	**Victims**	**Crime Type**	**Victims**
Tech Support	13,900	**Investment**	2,104
Non-payment/Non-Delivery	13,220	**Real Estate/Rental**	1,764
Identity Theft	8,902	**Overpayment**	1,448
Confidence Fraud/Romance	7,658	**Employment**	1,408
Personal Data Breach	6,189	**Terrorism/Threats of Violence**	719
Extortion	5,987	**IPR/Copyright and Counterfeit**	686
Phishing	5,831	**Ransomware**	365
Spoofing	3,936	**Civil Matter**	184
BEC/EAC *	3,755	**Computer Intrusion**	176
(Reporting a potential business victimization)	*2,143*	**Corporate Data Breach**	158
(Reporting a personal victimization)	*1,612*	**Malware/Scareware/Virus**	134
Government Impersonation	3,319	**Re-shipping**	76
Credit Card Fraud	3,164	**Health Care Related**	74
Advanced Fee	3,029	**Denial of Service/TDos**	61
Other	2,933	**Crimes Against Children**	42
Lottery/Sweepstakes/Inheritance	2,607	**Gambling**	19

Descriptors*	
Social Media	3,951
Virtual Currency	5,109

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 as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

***** Regarding BEC/EAC victim counts: A whole number is given to depict the overall victim count and is then broken out into separate counts to identify when an Over 60 victim may be reporting victimization on behalf of a business or personally.

2021 CRIME TYPES *Continued*

OVER 60 VICTIM LOSS			
Crime Type	**Loss**	**Crime Type**	**Loss**
Confidence Fraud/Romance	$432,081,901	**Spoofing**	$19,473,060
BEC/EAC *	$355,805,098	**Employment**	$9,610,615
(Reporting a potential business loss)	*$277,547,598*	**Overpayment**	$9,214,129
(Reporting a personal loss)	*$78,257,500*	**Phishing**	$9,166,217
Investment	$239,474,635	**Corporate Data Breach**	$7,095,746
Tech Support	$237,931,278	**Civil Matter**	$6,530,661
Personal Data Breach	$103,688,489	**IPR/Copyright and Counterfeit**	$4,954,221
Real Estate/Rental	$102,071,631	**Computer Intrusion**	$4,575,956
Government Impersonation	$69,186,858	**Health Care Related**	$1,233,632
Identity Theft	$59,022,153	**Malware/Scareware/Virus**	$1,177,864
Lottery/Sweepstakes/Inheritance	$53,557,330	**Ransomware ****	$424,852
Non-Payment/Non-Delivery	$52,023,580	**Terrorism/Threats of Violence**	$361,549
Credit Card Fraud	$39,019,072	**Re-shipping**	$360,455
Advanced Fee	$36,464,491	**Denial of Service/TDos**	$119,840
Other	$22,196,542	**Gambling**	$20,116
Extortion	$19,533,187	**Crimes Against Children**	$550

Descriptors*	
Social Media	$58,940,655
Virtual Currency	$241,143,166

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/EAC victim losses: A whole number is given to depict the overall victim loss and is then broken out into separate counts to identify when an Over 60 victim 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 3 YEARS COMPARISON

OVER 60 VICTIM COUNT			
Crime Type	**2021**	**2020**	**2019**
Advanced Fee	3,029	3,008	4,038
BEC/EAC	3,755	3,530	3,792
(Reporting a potential business loss)	*2,143*		
(Reporting a personal loss)	*1,612*		
Civil Matter	184	170	150
Computer Intrusion	176	--	--
Confidence Fraud/Romance	7,658	6,817	5,871
Corporate Data Breach	158	285	133
Credit Card Fraud	3,164	3,195	2,716
Crimes Against Children	42	58	31
Denial of Service/TDos	61	52	40
Employment	1,408	1,867	1,670
Extortion	5,987	23,100	12,242
Gambling	19	16	28
Government Impersonation	3,319	4,159	4,038
Health Care Related	74	243	72
IPR/Copyright and Counterfeit	686	552	287
Identity Theft	8,902	7,581	2,744
Investment	2104	1,062	612
Lottery/Sweepstakes/Inheritance	2,607	3,774	2,764
Malware/Scareware/Virus	134	287	622
Non-payment/Non-Delivery	13,220	14,534	7,731
Other	2,933	3,259	3,340
Overpayment	1,448	2,196	2,913
Personal Data Breach	6,189	6,121	6,725
Phishing/Vishing/Smishing/Pharming	5,831	7,353	5,383
Ransomware	365	365	337
Re-shipping	76	114	141
Real Estate/Rental	1,764	1,882	1,754
Spoofing	3,936	7,279	6,260
Tech Support	13,900	9,429	6,781
Terrorism/Threats of Violence	719	1,699	1,941

LAST 3 YEARS COMPARISON, *Continued*

OVER 60 VICTIM LOSS			
Crime Type	**2021**	**2020**	**2019**
Advanced Fee	$36,464,491	$33,184,114	$49,079,064
BEC/EAC	$355,805,098	$168,793,903	$209,597,559
(Reporting a potential business loss)	*$277,547,598*		
(Reporting a personal loss)	*$78,257,500*		
Civil Matter	$6,530,661	$1,866,788	$3,198,653
Computer Intrusion	$4,575,956	--	--
Confidence Fraud/Romance	$432,081,901	$281,134,006	$233,839,738
Corporate Data Breach	$7,095,746	$10,148,817	$3,616,996
Credit Card Fraud	$39,019,072	$20,780,800	$19,449,560
Crimes Against Children	$550	$411,349	$22,149
Denial of Service/TDos	$119,840	$180,447	$205
Employment	$9,610,615	$16,092,611	$8,920,628
Extortion	$19,533,187	$18,503,168	$30,564,053
Gambling	$20,116	$17,450	$85,457
Government Impersonation	$69,186,858	$45,909,970	$47,982,075
Health Care Related	$1,233,632	$2,652,390	$38,900
IPR/Copyright and Counterfeit	$4,954,221	$479,375	$1,146,051
Identity Theft	$59,022,153	$39,006,465	$25,739,680
Investment	$239,474,635	$98,040,940	$79,100,961
Lottery/Sweepstakes/Inheritance	$53,557,330	$38,804,343	$35,744,579
Malware/Scareware/Virus	$1,177,864	$671,667	$277,806
Non-Payment/Non-Delivery	$52,023,580	$40,377,167	$50,538,448
Other	$22,196,542	$49,689,594	$39,149,129
Overpayment	$9,214,129	$11,212,323	$13,397,602
Personal Data Breach	$103,688,489	$24,641,539	$28,470,827
Phishing/Vishing/Smishing/Pharming	$9,166,217	$18,829,999	$12,919,831
Ransomware	$424,852	$5,332,312	$723,642
Re-shipping	$360,455	$588,553	$595,352
Real Estate/Rental	$102,071,631	$50,098,565	$47,579,324
Spoofing	$19,473,060	$40,886,040	$42,218,197
Tech Support	$237,931,278	$116,415,126	$38,410,435
Terrorism/Threats of Violence	$361,549	$1,112,825	$2,363,624

2021 OVERALL STATE STATISTICS

OVER 60 VICTIMS BY STATE*

Rank	State	Victims	Rank	State	Victims
1	California	12,951	30	Utah	917
2	Florida	9,645	31	Louisiana	860
3	Texas	6,798	32	New Mexico	785
4	New York	6,223	33	Arkansas	721
5	Ohio	4,166	34	Kansas	666
6	Nevada	3,712	35	Iowa	548
7	Pennsylvania	3,627	36	Alaska	546
8	Colorado	3,569	37	Idaho	508
9	Illinois	3,499	38	Maine	475
10	Arizona	3,175	39	New Hampshire	471
11	Massachusetts	3,129	40	Hawaii	470
12	Virginia	2,956	41	Mississippi	469
13	Washington	2,853	42	Montana	406
14	New Jersey	2,665	43	Delaware	394
15	North Carolina	2,594	44	West Virginia	380
16	Michigan	2,410	45	Nebraska	353
17	Georgia	2,189	46	District of Columbia	349
18	Maryland	2,096	47	Rhode Island	260
19	Oregon	1,773	48	Vermont	244
20	Tennessee	1,686	49	Puerto Rico	229
21	Missouri	1,566	50	South Dakota	217
22	Indiana	1,536	51	Wyoming	208
23	Minnesota	1,458	52	North Dakota	151
24	South Carolina	1,447	53	Virgin Islands, U.S.	29
25	Wisconsin	1,315	54	United States Minor Outlying Islands	18
26	Alabama	1,184	55	Guam	16
27	Connecticut	1,061	56	American Samoa	7
28	Kentucky	953	57	Northern Mariana Islands	4
29	Oklahoma	923			

*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.

2021 OVERALL STATE STATISTICS, *Continued*

OVER 60 VICTIM LOSSES BY STATE*

Rank	State	Loss	Rank	State	Loss
1	California	$427,263,948	30	Kentucky	$12,767,463
2	Florida	$224,205,716	31	Hawaii	$11,693,691
3	New York	$188,052,904	32	Iowa	$10,312,324
4	Texas	$159,614,547	33	Oklahoma	$10,003,612
5	New Jersey	$87,546,156	34	Kansas	$8,488,260
6	Pennsylvania	$77,027,656	35	Mississippi	$7,907,893
7	Virginia	$60,833,227	36	District of Columbia	$7,704,848
8	Arizona	$54,441,279	37	Delaware	$7,079,040
9	Nevada	$53,320,488	38	Arkansas	$6,597,200
10	Massachusetts	$51,358,532	39	New Mexico	$6,316,971
11	Illinois	$49,956,292	40	Rhode Island	$5,671,235
12	Washington	$49,354,985	41	Vermont	$5,664,535
13	Ohio	$45,244,016	42	Montana	$5,405,855
14	North Carolina	$40,553,429	43	South Dakota	$5,372,535
15	Maryland	$37,817,082	44	Alaska	$5,166,344
16	Colorado	$33,942,278	45	Wyoming	$5,004,298
17	Georgia	$33,548,909	46	Idaho	$4,165,655
18	Tennessee	$32,520,912	47	Puerto Rico	$3,786,418
19	Michigan	$31,852,632	48	North Dakota	$3,099,693
20	Wisconsin	$22,634,486	49	West Virginia	$3,050,335
21	Oregon	$20,862,388	50	New Hampshire	$2,960,234
22	Minnesota	$20,513,323	51	Maine	$2,561,129
23	Louisiana	$19,887,674	52	Nebraska	$2,499,945
24	Utah	$19,868,020	53	Guam	$1,583,587
25	Indiana	$18,637,905	54	Virgin Islands, U.S.	$314,574
26	South Carolina	$18,331,406	55	American Samoa	$148,600
27	Alabama	$17,627,526	56	United States Minor Outlying Islands	$38,063
28	Missouri	$16,290,136	57	Northern Mariana Islands	$3,000
29	Connecticut	$15,630,551			

*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.

COMMON FRAUDS AFFECTING OVER 60 VICTIMS

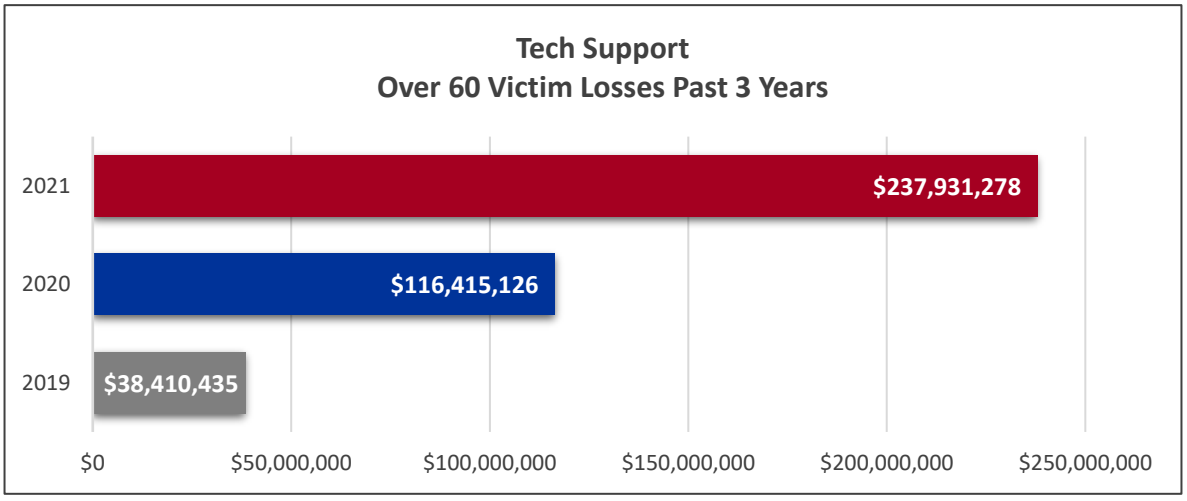
Tech Support Fraud

Tech Support Fraud is the most reported Fraud among Over 60 Victims. In 2021, the IC3 received 13,900 complaints related to Tech Support Fraud from elderly victims who experienced almost $238 million in losses. Elderly victims account for 58 percent of the total reports of tech support fraud to the IC3 and 68 percent of the total losses.

Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues or renewing fraudulent software or security subscriptions. However, in 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms, such as financial and banking institutions, utility companies, or virtual currency exchanges.

Many victims report being directed to make wire transfers to overseas accounts, purchase large amounts of prepaid cards, or mail large amounts of cash via overnight or express services.

For additional information on tech support scams, refer to IC3 Tech Support Fraud PSA, I-032818-PSA[5]

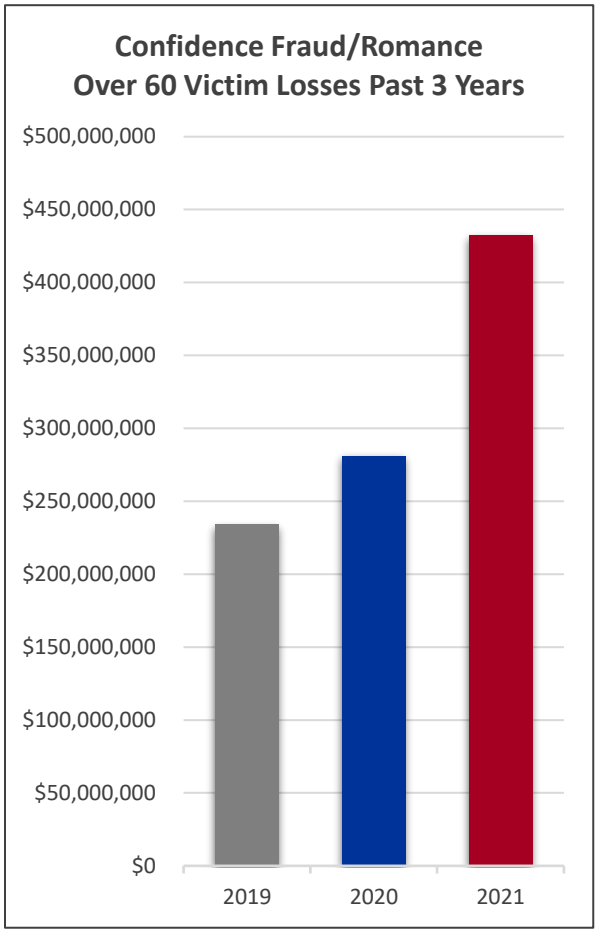


Confidence Fraud/Romance Scams

Confidence Fraud/Romance scams encompass those designed to pull on a victim's "heartstrings". In 2021, the IC3 received reports from 7,658 victims who experienced over $432 million in losses to Confidence Fraud/Romance scams. This type of fraud accounts for the highest losses reported by Over 60 victims.

[5] IC3 Tech Support Fraud PSA, I-032818-PSA, https://www.ic3.gov/Media/Y2018/PSA180328

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 himself 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 2021, over 450 Over 60 victims reported Grandparent scams, with approximate losses of $6.5 million.

Con artists are present on most dating and social media sites. In 2021, the IC3 received thousands of complaints from victims of online relationships resulting in sextortion or investment scams.

- Sextortion occurs when someone threatens to distribute your private and sensitive material if their demands are not met. In 2021, the IC3 received over 2,100 sextortion-related complaints from victims over 60, with losses over $3 million. Please see the September 2021 IC3 PSA I-090221-PSA on Sextortion for more information.[6]
- Many victims of Confidence Fraud/Romance scams also report being pressured into investment opportunities, especially utilizing cryptocurrency, called "pig butchering". This scam is most often reported among younger populations. However, in 2021, 791 over 60 victims lost almost $123 million from this scam. Additional information on "pig butchering" can be found in the September 2021 IC3 PSA I-091621-PSA.[7]

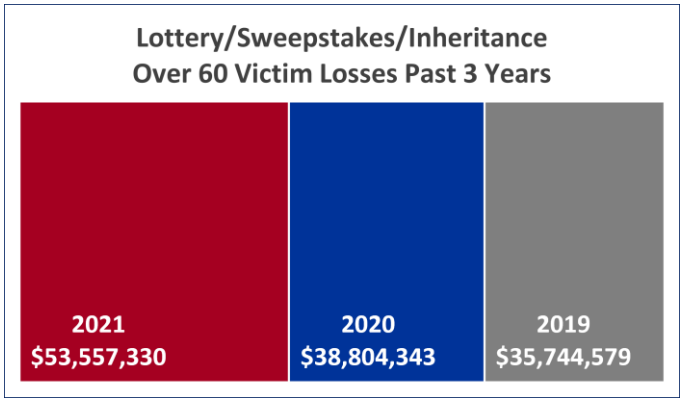
[6] FBI Warns about an Increase in Sextortion Complaints. https://www.ic3.gov/Media/Y2021/PSA210902

[7] Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams. https://www.ic3.gov/Media/Y2021/PSA210916

Lottery/Sweepstakes/Inheritance

In 2021, the IC3 received over 2,600 reports of elderly victims in Lottery/Sweepstakes/Inheritance scams. Victims lost over $53 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.

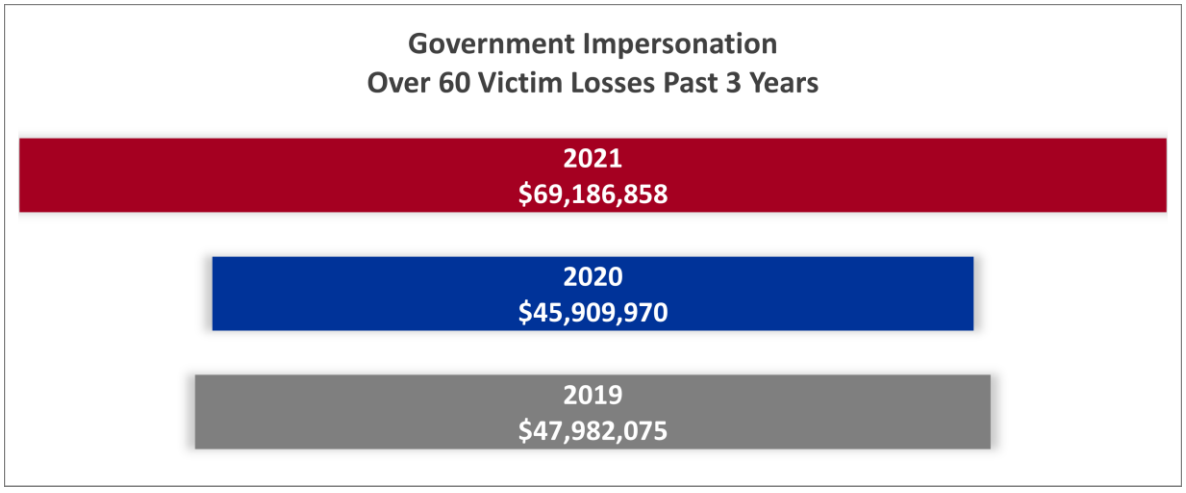


Inheritance scams function very similarly as the victim is informed an unknown, distant relative has left a large inheritance to the victim. The victim is required to pay taxes and fees to receive the inheritance money.

Government Impersonation

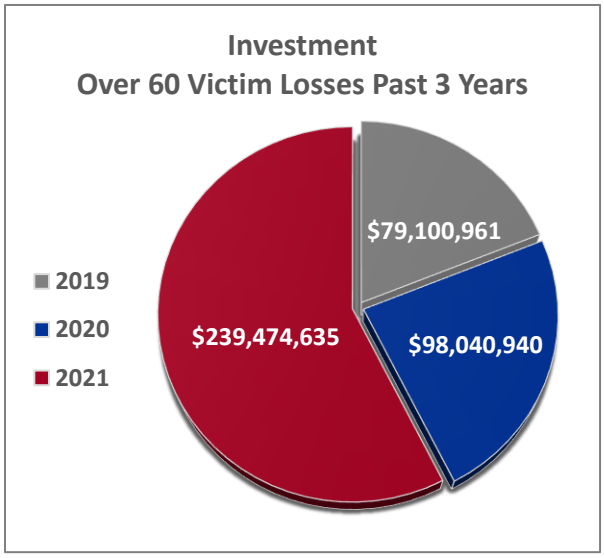
While government impersonation is not reported as often, millions of dollars are still lost by the elderly to criminals impersonating government officials. The criminals often extort victims with threats of physical or financial harm to obtain personally identifiable information.

In 2021, victims over the age of 60 reported this type of fraud over 3,300 times, with losses of $69 million. The subjects generally demand prepaid cards, wire transfers, or cash to be mailed or sent overnight.



Investment

Investment fraud involves the illegal sale or purported sale of financial instruments. The typical investment fraud schemes are characterized by offers of low or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities. Examples of investment fraud include advance fee fraud, Ponzi schemes, pyramid schemes, and market manipulation fraud.



These schemes often seek to victimize targeted individuals, such as groups with common interests, age, religion, or ethnicity, to build trust to effectively operate the investment fraud against them. The scammers' ability to foster trust makes these schemes so successful. Investors should use scrutiny and gather as much information as possible before considering any new investment opportunities.

More than 2,100 Over 60 victims reported Investment scams in 2021, with losses over $239 million.

Cryptocurrency

In 2021, the IC3 received more than 5,100 complaints from over 60 victims involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. Losses of these victims totaled over $241 million.

Cryptocurrency is becoming the preferred payment method for all types of scams – SIM Swaps, tech support fraud, employment schemes, romance scams, even some auction fraud. It is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim.

Cryptocurrency ATMs: Automated Teller Machines (ATMs) used to purchase cryptocurrency are popping up everywhere. Regulations on the machines are lax and purchases are almost instantaneous and irreversible, making this payment method lucrative to criminals. The most common scams reported were Confidence Fraud/Romance, Investment, Employment, and Government Impersonation. Read more about crypto ATM scams in IC3 PSA I-110421-PSA.[8]

[8] The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment https://www.ic3.gov/Media/Y2021/PSA211104

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/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Civil Matter: Civil litigation generally includes all disputes formally submitted to a court, about any subject in which one party is claimed to have committed a wrong but not a crime. In general, this is the legal process most people think of when the word "lawsuit" is used.

Computer Intrusion: Unauthorized access or exceeding authorized access into a protected computer system. A protected computer system is one owned or used by the US Government, a financial institution, or any business. This typically excludes personally owned systems and devices.

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".

Corporate Data Breach: A data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Credit Card 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.

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system, or a Telephony Denial of Service (TDoS) floods a voice service with multiple requests, slowing down or interrupting service.

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.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

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

Health Care Related: A scheme attempting to defraud private or government health care programs which usually involving health care providers, companies, or individuals. Schemes may include offers

for fake insurance cards, health insurance marketplace assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

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.

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.).

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/Scareware/Virus: 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/Vishing/Smishing/Pharming: 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.

Re-shipping: Individuals receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

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

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; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

Social Media: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

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

Terrorism/Threats of Violence: Terrorism is violent acts intended to create fear that are perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.

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.
- Victims are not required to provide an age range. This field is completely voluntary. Therefore, information in this report only reflects complaints where a victim provided an age range of “Over 60”

APPENDIX C: 2021 – STATE VICTIMS PER CAPITA

OVER 60 VICTIMS BY STATE *(per 100,000 People)*

Rank	State	Victims	Rank	State	Victims
1	**Nevada**	118.1	27	**Illinois**	27.6
2	**Alaska**	74.5	28	**Utah**	27.5
3	**Colorado**	61.4	29	**Idaho**	26.7
4	**District of Columbia**	52.1	30	**Minnesota**	25.5
5	**Massachusetts**	44.8	31	**Missouri**	25.4
6	**Florida**	44.3	32	**North Carolina**	24.6
7	**Arizona**	43.6	33	**South Dakota**	24.2
8	**Oregon**	41.8	34	**Tennessee**	24.2
9	**Delaware**	39.3	35	**Michigan**	24.0
10	**Vermont**	37.8	36	**Arkansas**	23.8
11	**New Mexico**	37.1	37	**Rhode Island**	23.7
12	**Washington**	36.9	38	**Alabama**	23.5
13	**Montana**	36.8	39	**Oklahoma**	23.2
14	**Wyoming**	35.9	40	**Texas**	23.0
15	**Ohio**	35.4	41	**Kansas**	22.7
16	**Maine**	34.6	42	**Indiana**	22.6
17	**Virginia**	34.2	43	**Wisconsin**	22.3
18	**Maryland**	34.0	44	**West Virginia**	21.3
19	**New Hampshire**	33.9	45	**Kentucky**	21.1
20	**California**	33.0	46	**Georgia**	20.3
21	**Hawaii**	32.6	47	**North Dakota**	19.5
22	**New York**	31.4	48	**Louisiana**	18.6
23	**Connecticut**	29.4	49	**Nebraska**	18.0
24	**New Jersey**	28.8	50	**Iowa**	17.2
25	**Pennsylvania**	28.0	51	**Mississippi**	15.9
26	**South Carolina**	27.9	52	**Puerto Rico**	7.0

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

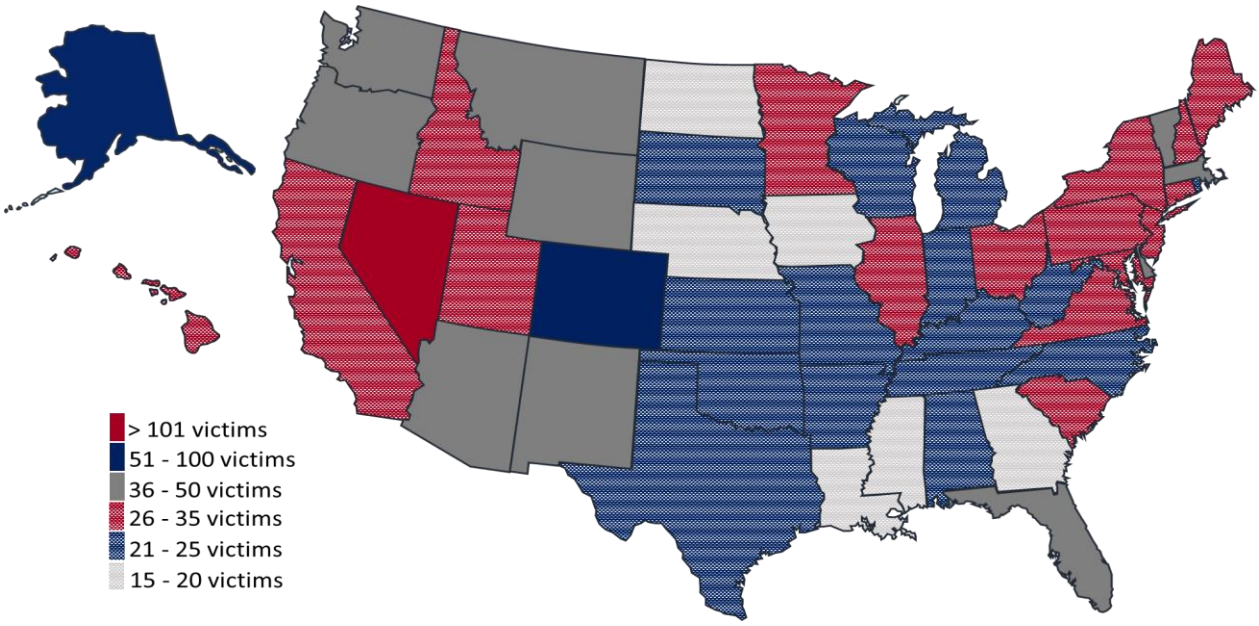
Per 100,000 people, based upon U.S. Census Bureau population estimates when available. https://www.census.gov

OVER 60 VICTIM LOSSES BY STATE *(per 100,000 People)*					
Rank	State	Loss	Rank	State	Loss
1	**Nevada**	$1,695,949	27	**Louisiana**	$430,092
2	**District of Columbia**	$1,149,892	28	**North Dakota**	$399,987
3	**California**	$1,088,908	29	**Illinois**	$394,242
4	**Florida**	$1,029,358	30	**North Carolina**	$384,350
5	**New York**	$948,043	31	**Ohio**	$384,074
6	**New Jersey**	$944,695	32	**Wisconsin**	$383,902
7	**Vermont**	$877,447	33	**Minnesota**	$359,417
8	**Wyoming**	$864,594	34	**South Carolina**	$353,158
9	**Hawaii**	$811,187	35	**Alabama**	$349,761
10	**Arizona**	$748,198	36	**Iowa**	$322,959
11	**Massachusetts**	$735,298	37	**Michigan**	$316,916
12	**Delaware**	$705,517	38	**Georgia**	$310,651
13	**Alaska**	$705,136	39	**New Mexico**	$298,551
14	**Virginia**	$703,903	40	**Kansas**	$289,249
15	**Washington**	$637,769	41	**Kentucky**	$283,130
16	**Maryland**	$613,403	42	**Indiana**	$273,846
17	**South Dakota**	$600,031	43	**Mississippi**	$268,067
18	**Utah**	$595,212	44	**Missouri**	$264,099
19	**Pennsylvania**	$594,163	45	**Oklahoma**	$250,928
20	**Colorado**	$583,996	46	**Idaho**	$219,139
21	**Texas**	$540,554	47	**Arkansas**	$218,025
22	**Rhode Island**	$517,633	48	**New Hampshire**	$213,121
23	**Oregon**	$491,324	49	**Maine**	$186,638
24	**Montana**	$489,541	50	**West Virginia**	$171,083
25	**Tennessee**	$466,235	51	**Nebraska**	$127,308
26	**Connecticut**	$433,508	52	**Puerto Rico**	$116,020

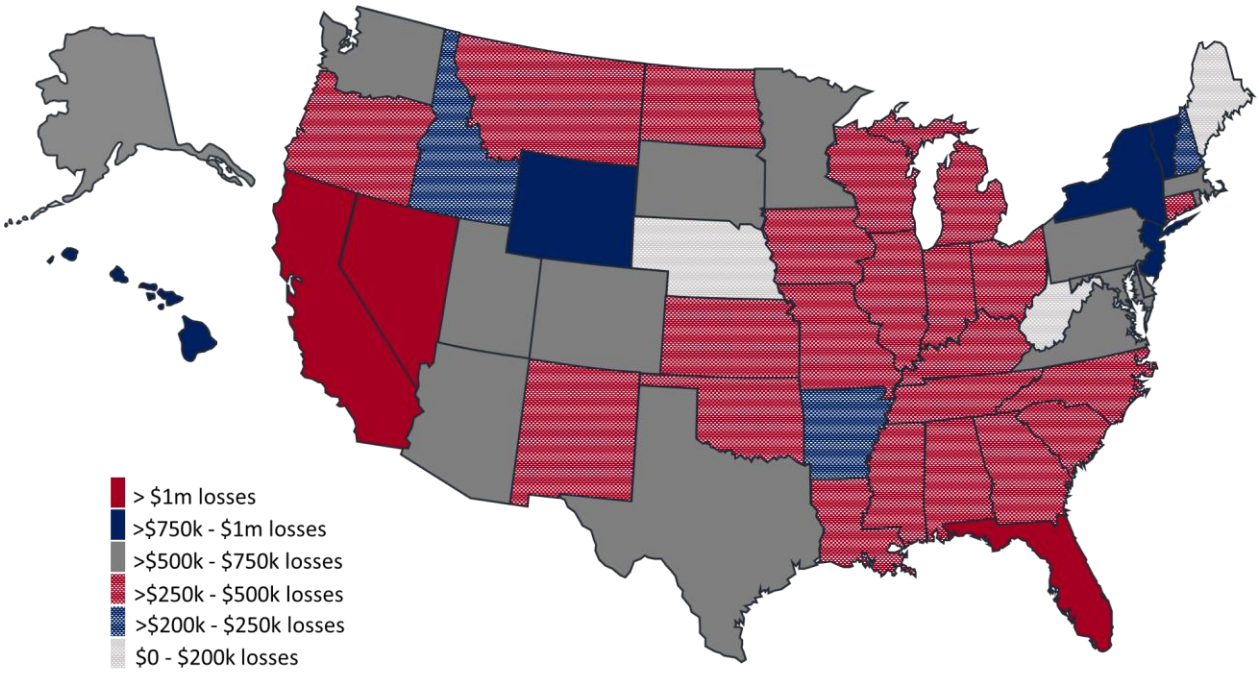
*Note: This information is based on the total number of complaints from each state, Puerto Rico, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data. Populations based on data available from the U.S. Census Bureau.

Per 100,000 people, based upon U.S. Census Bureau population estimates when available. https://www.census.gov

2021 – STATES BY NUMBER OF OVER 60 VICTIMS PER CAPITA[9]



2021 – STATES BY LOSSES OF OVER 60 VICTIMS PER CAPITA



[9]Per 100,000 people, based upon July 2021 U.S. Census Bureau population estimates. https://www.census.gov