ELDER FRAUD REPORT

2020

2020 Elder Fraud Report

TABLE OF CONTENTS

Introduction 3
2020 Victims by Age Group 5
Over 60 Victim Reporting for Past Five Years 5
2020 – States By Number of Over 60 Victims 6
2020 – States By Loss of Over 60 Victims 6
2020 Crime Types 7
Last 3 Year Complaint Count Comparison 9
2020 Overall State Statistics 11
COMMON FRAUDS AFFECTING OVER 60 VICTIMS 13
Non-Payment/Non-Delivery, Fraudulent Products 13
Lottery/Sweepstakes/Inheritance 14
Confidence Fraud/Romance Scams 15
Tech Support Fraud 16
Extortion 17
Government Impersonation 17
Investment 18
Appendix A: Definitions 19
Appendix B: Additional information about IC3 Data 22

INTRODUCTION

Dear Reader,

The mission of the FBI is to protect the American people and uphold the Constitution of the United States. This mission includes our efforts to combat financial crimes targeting seniors. The FBI, in alignment with the Department of Justice Elder Fraud Initiative and the efforts of our internal and external partners, is committed to this mission. It is from this commitment to the American people that the FBI provides the public an avenue to report fraud through the Internet Crime Complaint Center (IC3).

The IC3 receives and tracks thousands of complaints daily, reported by victims of fraud. This reporting is key to identifying, investigating, and holding those responsible accountable for their actions. Victims of fraud have the option to identify their age range when submitting a complaint to IC3; the information contained in this report is derived from complaints submitted by or on behalf of victims aged 60 and over.

Each year, millions of elderly Americans fall victim to some type of financial fraud or internet scheme, such as romance scams, tech support fraud, and lottery or sweepstake scams. Criminals gain their targets' trust or use tactics of intimidation and threats to take advantage of their victims. Once successful, scammers are likely to keep a scheme going because of the prospect of significant financial gain.

In 2020, IC3 received a total of 791,790 complaints with reported losses exceeding $4.1 billion. Based on the information provided in the complaints, approximately 28% of the total fraud losses were sustained by victims over the age of 60, resulting in approximately $1 billion in losses to seniors. This represents an increase of approximately $300 million in losses reported in 2020 versus what was reported by victims over 60 in 2019.

To educate the public and provide as much information on the types of frauds targeting seniors as possible, the IC3 is offering its first publication of the 2020 IC3 Elder Fraud Annual Report. This report is a companion report to the 2020 IC3 Annual Report released in March 2021. These reports, along with other publications, are available at www.IC3.gov.

It is only by victims reporting fraud that we can identify trends, educate the public, and support investigations, and nowhere is this more important than crimes against seniors.

Calvin Shivers
Assistant Director
Federal Bureau of Investigation
Criminal Investigative Division

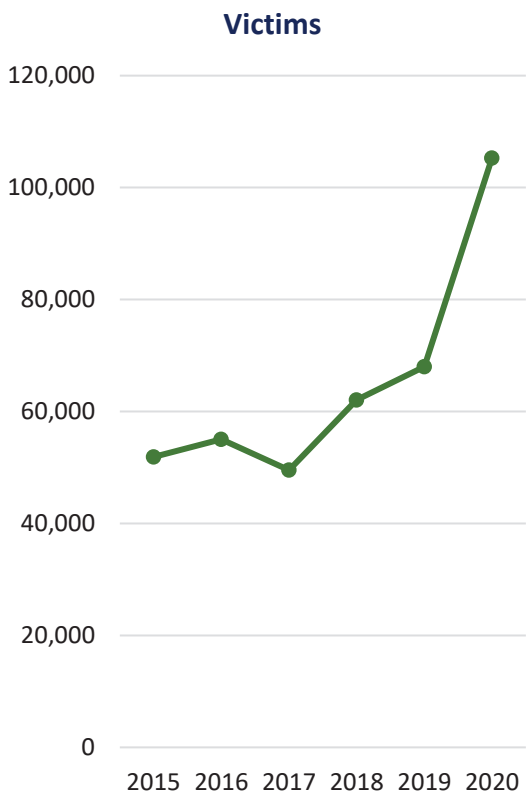
IC3 Over 60 Victims by the Numbers[1]

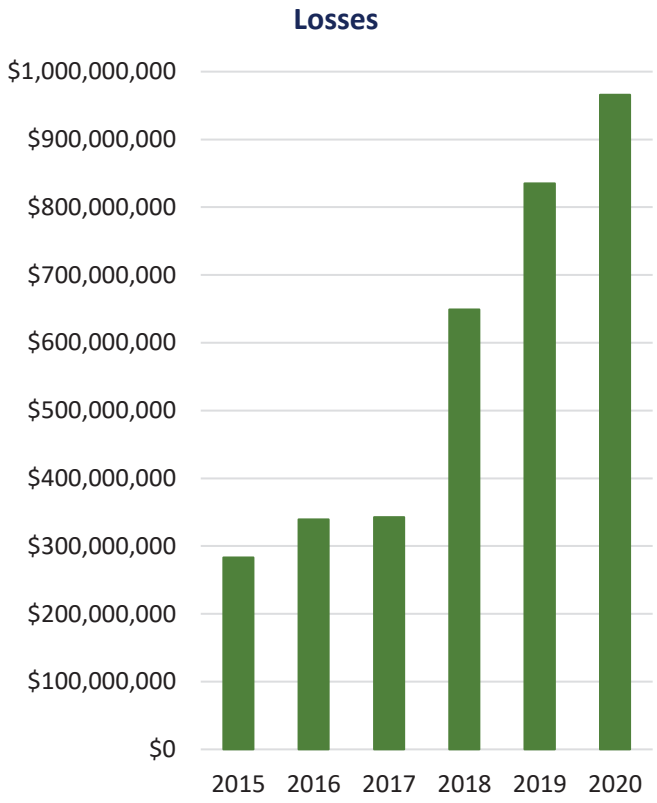
[1] Accessibility description: Image depicts key statistics regarding Over 60 complaints. The total number of complaints received in 2020 was 105,301. Total losses of $1 billion were reported. Over 60 victims experienced 28 percent of the total loss of all IC3 complaints received in 2020. 1,921 victims lost more than $100,000. The average loss per victim was $9,175.

2020 VICTIMS BY AGE GROUP

Victims		
Age Range[2]	**Total Count**	**Total Loss**
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

OVER 60 VICTIM REPORTING FOR PAST FIVE YEARS[3]

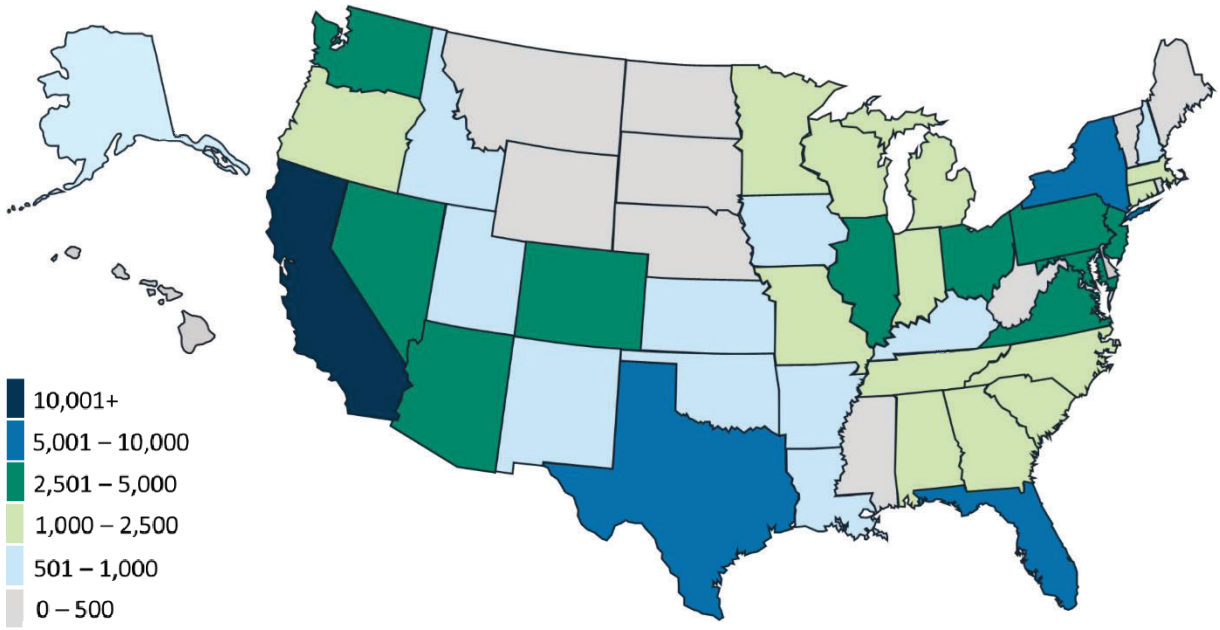




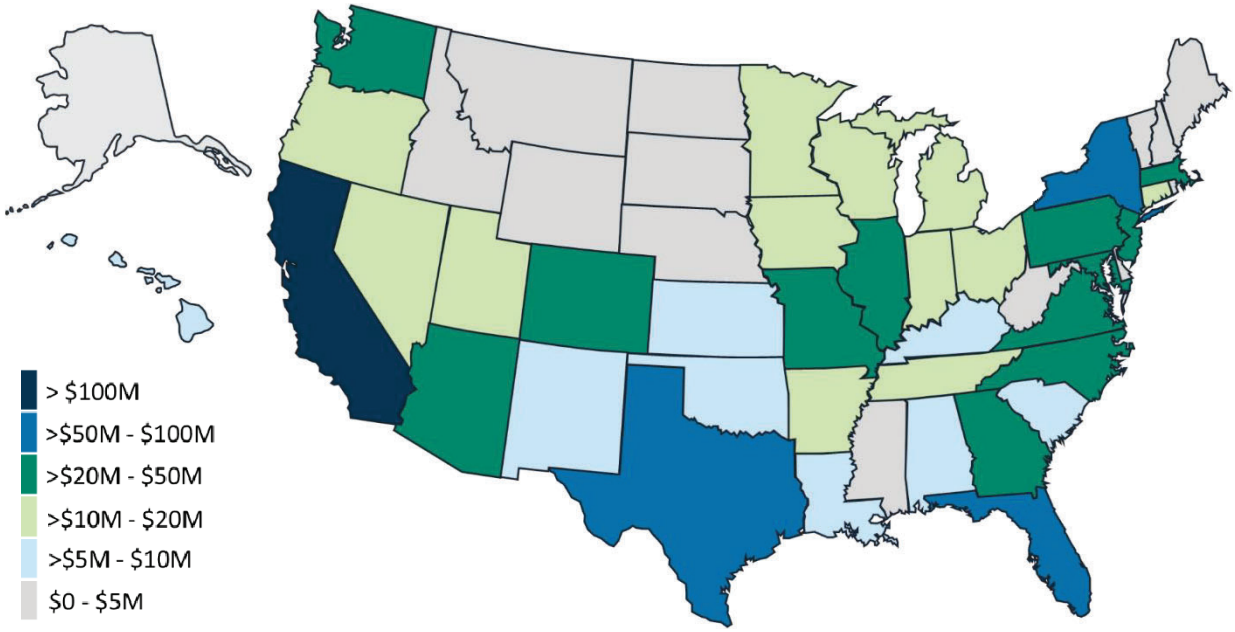
[2] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

[3] Charts describe Over 60 Victim Counts and Losses from 2015 – 2020.

2020 – STATES BY NUMBER OF OVER 60 VICTIMS[4]



2020 – 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.

2020 CRIME TYPES

Over 60 Victim Count

Crime Type	Victims	Crime Type	Victims
Extortion	23,100	Employment	1,867
Non-Payment/Non-Delivery	14,534	Terrorism/Threats of Violence	1,692
Tech Support	9,429	Investment	1,062
Identity Theft	7,581	IPR/Copyright and Counterfeit	552
Phishing/Vishing/Smishing/Pharming	7,353	Ransomware	365
Spoofing	7,279	Malware/Scareware/Virus	287
Confidence Fraud/Romance	6,817	Corporate Data Breach	285
Personal Data Breach	6,121	Health Care Related	243
Misrepresentation	4,735	Civil Matter	170
Government Impersonation	4,159	Re-shipping	114
Lottery/Sweepstakes/Inheritance	3,774	Charity	105
BEC/EAC *	3,530	Crimes Against Children	58
Other	3,259	Denial of Service/TDos	52
Credit Card Fraud	3,195	Gambling	16
Advanced Fee	3,008	Terrorism	7
Overpayment	2,196	Hacktivist	5
Real Estate/Rental	1,882		

Descriptors*

Social Media	4,533
Virtual Currency	9,447

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: This number also includes complaints in which an Over 60 person may be filing on behalf of a business who is the actual victim of a BEC scam.

2020 Crime Types *Continued*

Over 60 Victim Loss

Crime Type	Loss	Crime Type	Loss
Confidence Fraud/Romance	$281,134,006	Overpayment	$11,212,323
BEC/EAC *	$168,793,903	Corporate Data Breach	$10,148,817
Tech Support	$116,415,126	Ransomware **	$5,332,312
Investment	$98,040,940	Health Care Related	$2,652,390
Real Estate/Rental	$50,098,565	Civil Matter	$1,866,788
Other	$49,689,594	Misrepresentation	$1,815,552
Government Impersonation	$45,909,970	Terrorism/Threats of Violence	$1,112,825
Spoofing	$40,886,040	Malware/Scareware/Virus	$671,667
Non-Payment/Non-Delivery	$40,377,167	Charity	$629,295
Identity Theft	$39,006,465	Re-shipping	$588,553
Lottery/Sweepstakes/Inheritance	$38,804,343	IPR/Copyright and Counterfeit	$479,375
Advanced Fee	$33,184,114	Crimes Against Children	$411,349
Personal Data Breach	$24,641,539	Denial of Service/TDos	$180,447
Credit Card Fraud	$20,780,800	Gambling	$17,450
Phishing/Vishing/Smishing/Pharming	$18,829,999	Terrorism	$0
Extortion	$18,503,168	Hacktivist	$0
Employment	$16,092,611		

Descriptors*		
Social Media	$35,344,786	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.
Virtual Currency	$55,056,901	

***** Regarding BEC/EAC adjusted losses: This number also includes complaints in which an Over 60 person may be filing on behalf of a business who is the actual victim of a BEC scam.

****** 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 Year Complaint Count Comparison

Over 60 Victim Count

Crime Type	2020	2019	2018
Advanced Fee	3,008	4,038	3,988
BEC/EAC	3,530	3,792	3,174
Charity	105	72	114
Civil Matter	170	150	130
Confidence Fraud/Romance	6,817	5,871	5,492
Corporate Data Breach	285	133	311
Credit Card Fraud	3,195	2,716	2,841
Crimes Against Children	58	31	42
Denial of Service/TDos	52	40	48
Employment	1,867	1,670	1,873
Extortion	23,100	12,242	13,600
Gambling	16	28	19
Government Impersonation	4,159	4,038	2,983
Hacktivist	5	2	15
Health Care Related	243	72	77
IPR/Copyright and Counterfeit	552	287	260
Identity Theft	7,581	2,744	2,644
Investment	1,062	612	583
Lottery/Sweepstakes/Inheritance	3,774	2,764	2,607
Malware/Scareware/Virus	287	622	813
Misrepresentation	4,735	768	718
Non-Payment/Non-Delivery	14,534	7,731	7,328
Other	3,259	3,340	2,610
Overpayment	2,196	2,913	3,005
Personal Data Breach	6,121	6,725	10,439
Phishing/Vishing/Smishing/Pharming	7,353	5,383	5,368
Ransomware	365	337	276
Re-shipping	114	141	118
Real Estate/Rental	1,882	1,754	1,539
Spoofing	7,279	6,260	2,497
Tech Support	9,429	6,781	6,731
Terrorism/Threats of Violence	1,699	1,941	2,217

Last 3 Year Complaint Loss Comparison *Continued*

Over 60 Victim Loss			
Crime Type	**2020**	**2019**	**2018**
Advanced Fee	$33,184,114	$49,079,064	$41,949,417
BEC/EAC	$168,793,903	$209,597,559	$170,154,145
Charity	$629,295	$230,852	$319,693
Civil Matter	$1,866,788	$3,198,653	$914,407
Confidence Fraud/Romance	$281,134,006	$233,839,738	$169,735,151
Corporate Data Breach	$10,148,817	$3,616,996	$5,526,672
Credit Card Fraud	$20,780,800	$19,449,560	$20,904,793
Crimes Against Children	$411,349	$22,149	$0
Denial of Service/TDos	$180,447	$205	$292,798
Employment	$16,092,611	$8,920,628	$10,430,324
Extortion	$18,503,168	$30,564,053	$24,045,912
Gambling	$17,450	$85,457	$26,265
Government Impersonation	$45,909,970	$47,982,075	$20,676,302
Hacktivist	$0	$0	$57,012
Health Care Related	$2,652,390	$38,900	$13,415
IPR/Copyright and Counterfeit	$479,375	$1,146,051	$480,799
Identity Theft	$39,006,465	$25,739,680	$14,520,820
Investment	$98,040,940	$79,100,961	$114,851,158
Lottery/Sweepstakes/Inheritance	$38,804,343	$35,744,579	$41,924,351
Malware/Scareware/Virus	$671,667	$277,806	$872,424
Misrepresentation	$1,815,552	$1,396,206	$2,959,581
Non-Payment/Non-Delivery	$40,377,167	$50,538,448	$37,047,889
Other	$49,689,594	$39,149,129	$9,415,288
Overpayment	$11,212,323	$13,397,602	$14,768,236
Personal Data Breach	$24,641,539	$28,470,827	$24,779,324
Phishing/Vishing/Smishing/Pharming	$18,829,999	$12,919,831	$9,639,156
Ransomware	$5,332,312	$723,642	$594,469
Re-shipping	$588,553	$595,352	$734,014
Real Estate/Rental	$50,098,565	$47,579,324	$36,116,817
Spoofing	$40,886,040	$42,218,197	$12,624,158
Tech Support	$116,415,126	$38,410,435	$23,828,362
Terrorism/Threats of Violence	$1,112,825	$2,363,624	$7,409,855

2020 Overall State Statistics

Over 60 Victims per State*					
Rank	**State**	**Victims**	**Rank**	**State**	**Victims**
1	California	12,534	30	Louisiana	855
2	Florida	9,252	31	New Mexico	837
3	Texas	6,342	32	Kentucky	782
4	New York	6,021	33	Kansas	728
5	Colorado	4,335	34	Arkansas	636
6	Illinois	4,227	35	Iowa	570
7	Pennsylvania	3,543	36	Alaska	563
8	Washington	3,301	37	Idaho	550
9	Arizona	3,053	38	New Hampshire	543
10	Virginia	2,779	39	Mississippi	461
11	Nevada	2,767	40	Hawaii	452
12	Ohio	2,711	41	Nebraska	404
13	New Jersey	2,671	42	West Virginia	403
14	Michigan	2,499	43	Delaware	371
15	North Carolina	2,472	44	Maine	368
16	Massachusetts	2,309	45	Montana	335
17	Georgia	2,145	46	Rhode Island	323
18	Maryland	2,067	47	District of Columbia	252
19	Tennessee	1,881	48	Vermont	235
20	Oregon	1,775	49	Puerto Rico	207
21	Missouri	1,578	50	Wyoming	174
22	Minnesota	1,542	51	South Dakota	169
23	Indiana	1,519	52	North Dakota	104
24	South Carolina	1,350	53	Virgin Islands, U.S.	29
25	Wisconsin	1,226	54	Guam	18
26	Connecticut	1,057	55	U.S. Minor Outlying Islands	16
27	Alabama	1,040	56	Northern Mariana Islands	5
28	Oklahoma	897	57	American Samoa	2
29	Utah	893			

***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.**

2020 Overall State Statistics *Continued*

Over 60 Victim Losses by State*

Rank	State	Loss	Rank	State	Loss
1	California	$152,644,032	30	Kansas	$7,314,673
2	Florida	$84,649,328	31	New Mexico	$7,127,910
3	Texas	$69,759,993	32	Louisiana	$5,857,104
4	New York	$55,314,852	33	Hawaii	$5,436,326
5	Illinois	$32,143,412	34	District of Columbia	$5,136,728
6	North Carolina	$27,854,588	35	Idaho	$4,600,473
7	New Jersey	$27,505,005	36	Montana	$4,131,902
8	Arizona	$27,038,828	37	Iowa	$4,085,790
9	Washington	$26,541,727	38	Kentucky	$4,056,091
10	Georgia	$25,799,082	39	Nebraska	$4,048,483
11	Virginia	$24,836,467	40	Arkansas	$3,497,078
12	Utah	$23,652,577	41	Wyoming	$3,105,323
13	Pennsylvania	$23,335,992	42	Rhode Island	$2,792,854
14	Maryland	$21,177,890	43	Alaska	$2,561,387
15	Colorado	$20,852,509	44	Maine	$2,471,681
16	Massachusetts	$20,447,349	45	Delaware	$2,276,129
17	Ohio	$19,189,241	46	Mississippi	$2,213,731
18	Michigan	$18,844,350	47	Puerto Rico	$2,004,618
19	Missouri	$16,236,719	48	New Hampshire	$1,722,542
20	Minnesota	$15,730,641	49	Vermont	$1,629,726
21	Oregon	$12,787,393	50	West Virginia	$1,483,058
22	Nevada	$11,580,787	51	South Dakota	$1,396,978
23	Tennessee	$10,846,194	52	North Dakota	$1,008,768
24	Connecticut	$10,645,305	53	Virgin Islands, U.S.	$509,203
25	Wisconsin	$10,227,553	54	U.S. Minor Outlying Islands	$85,659
26	Indiana	$10,049,923	55	Northern Mariana Islands	$66,000
27	South Carolina	$9,987,360	56	Guam	$55,428
28	Alabama	$7,863,338	57	American Samoa	$0
29	Oklahoma	$7,613,157			

***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

Non-Payment/Non-Delivery, Fraudulent Products

The pandemic required many elderly victims to shop online for the first time ever. Elderly victims filed over 14,000 Non-Payment/Non-Delivery complaints experiencing losses over $40 million in 2020, making Non-Delivery of products the second most reported fraud among the elderly.

Additionally, more elderly 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.

The volume of counterfeit health and beauty products also continues to increase. Online shopping gives consumers widespread access to health and beauty products they do not realize are fake. Counterfeiters of personal care products increasingly view dealing in these fake items as a low-risk crime since many of them are located outside the U.S.

Government and industry studies and testing have discovered dangerous ingredients within counterfeit cosmetic products. Fraudulent cosmetics may contain poisonous substances and dangerous levels of bacteria from unknown sources. Some of these products have caused serious health conditions.

Protect Against Non-Delivery of Merchandise

If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong. Ensure transactions are secure when electronically sending credit card numbers.

Ensure the purchase is made from a reputable source.

Do your homework on the individual or company to ensure they are legitimate.

Obtain a physical address rather than a post office box and a telephone number and call the seller to see if the telephone number is correct and working.

Send an e-mail to the seller to make sure the e-mail address is active and be wary of those that utilize free e-mail services where a credit card wasn’t required to open the account.

Consider not purchasing from sellers who will not provide you with this type of information.

Check with the Better Business Bureau from the seller’s area.

Check out other websites regarding this person/company.

Don’t judge a person or company by their website; flashy websites can be set up quickly.

Be cautious when responding to special investment offers, especially through unsolicited e-mail.

Be cautious when dealing with foreign individuals/companies.

Inquire about returns and warranties.

Protect Against Fraudulent Products

If it sounds too good to be true, it probably is. Watch out for “secret formulas” or “breakthroughs.”

Do not be afraid to ask questions about the product—find out exactly what it should and should not do for you.

Research a product thoroughly before buying it. Call the Better Business Bureau to find out if other people have complained about the product.

Be wary of products that claim to cure a wide variety of illnesses—particularly serious ones—that do not appear to be related.

Be aware that testimonials and/or celebrity endorsements are often misleading.

Be very careful of products claiming to have no side effects.

Question products that advertise as making visits to a physician unnecessary.

Always consult your doctor before taking any dietary or nutritional supplement.

Lottery/Sweepstakes/Inheritance

In 2020, the IC3 received over 3,700 reports of elderly victims in Lottery/Sweepstakes/Inheritance scams. Victims lost over $38 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. Subjects often request the payments be made via wire transfers or prepaid cards. Often, the scammers will ask for a victim’s banking information to transfer their winnings.

The subjects will continue to call victims for months or even years, promising the big prize is only one more payment away. If the victim stops paying or cuts off contact, the subjects may threaten harm to the victim or a loved one or to report you to authorities.

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.

Protect Against Lottery/Sweepstakes/Inheritance Scams

Lottery/Sweepstakes/Inheritance scams are generally identified by unsolicited calls or notifications claiming entry into a sweepstakes the victim has never heard of before or inheriting money from a relative the victim has never heard of before. The victim is told to make upfront payments to collect the prize or inheritance. Legitimate beneficiaries do not need to pay up front taxes and fees to claim a prize or inheritance.

Playing foreign lotteries in any form is a violation of federal law.

Never provide banking or personal information.

Confidence Fraud/Romance Scams

Confidence Fraud/Romance scams encompasses those which are designed to pull on a victim's "heartstrings". In 2020, the IC3 received reports from 6,817 elderly victims who experienced over $281 million in losses to Confidence Fraud/Romance scams. This type of fraud accounts for the highest losses reported by Over 60 victims.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. Often, the scammer will utilize religion to garner trust with the victim. 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. Con artists are present on most dating and social media sites. The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will 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 ask for money for a medical emergency or unexpected legal fee.

Many victims of Romance scams also report being pressured into investment opportunities, especially utilizing virtual currency. In 2020, the IC3 received 403 complaints, losses of $29 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and virtual currencies.

Also included in the Confidence Fraud category are Grandparent Scams in which 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.

Protect Against Confidence Fraud/Romance Scams

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.

Go slowly and ask lots of questions.

For Romance scams, research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.

Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.

Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.

Beware if the individual promises to meet in person but then always comes up with an excuse why he or she cannot. If you have not met the person after a few months, for whatever reason, you have good reason to be suspicious.

Never send money to anyone you have only communicated with online or by phone.

Tech Support Fraud

Tech Support Fraud is the third most reported fraud among the elderly behind Extortion and Non-Payment/Non-Delivery. In 2020, the IC3 received 9,429 complaints related to Tech Support Fraud from elderly victims who experienced over $116 million in losses. Elderly victims account for 66 percent of the total reports of tech support fraud to the IC3 and 84 percent of the total losses.

This scheme involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal.

In 2020, the IC3 saw a large increase in the number of complaints involving criminals posing as customer support for financial institutions, utility companies, or virtual currency exchanges. Many complaints report an upsurge in the impersonation of popular online shopping companies and electronic commerce companies.

Initial contact can occur in various ways. 1) Telephone: Victim receives an unsolicited telephone call from a criminal impersonating computer support, bank representatives/support, and utility companies. 2) Search Engine Advertising: Victim searches online to find support numbers. Criminals pay to have their fraudulent company's link show higher in search results hoping victims will choose one of the top links in search results. 3) Pop-up message: Victim receives an on-screen pop-up message claiming a virus has been found on their computer. The message requests the victim call a phone number associated with the fraudulent tech support company. 4) Email: Victim receives an email warning of support subscription expiration or a potential fraudulent charge on their account. The victim is encouraged to contact the fraudulent support via phone.

A twist on Tech Support Fraud occurs when a victim is contacted and offered a refund. The criminal convinces the victim to provide access to their computer and bank account, then appears to accidentally refund too much to the victim. The criminal then demands return of the "extra" funds.

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.

Protect Against Tech Support Fraud

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, or mailed cash.

Install ad-blocking software that eliminates or reduces pop-ups and malvertising. Ensure all computer anti-virus, security, and malware protection is up to date.

Be cautious of customer support numbers obtained via open-source searching. Phone numbers listed in a "sponsored" results section are likely boosted as a result of Search Engine Advertising.

Resist the pressure to act quickly. Criminals will urge the victim to act fast to protect their device. Legitimate companies will allow time for a person to process and research any questions.

Never give unknown, unverified persons remote access to devices or accounts.

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.

Virtual currency is commonly demanded as the payment mechanism because it provides the criminal an additional layer of anonymity when perpetrating these schemes. Most extortion complaints received in 2020 were part of an email extortion campaign in which victims received an email threatening to tell all their contacts they were infected with COVID or threatening to infect the recipient with COVID unless a virtual currency payoff was made.

Over 60 victims reported over 21,000 incidents of Extortion in 2020, with losses over $18 million.

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 2020, victims over the age of 60 reported this type of fraud over 4,100 times, with losses of almost $46 million.

Victims often receive a phone call from someone impersonating a member of government or law enforcement. Impersonated agencies range from local law enforcement to large federal agencies, including the Social Security Administration, the Internal Revenue Service, the Drug Enforcement Agency, and the FBI.

The impersonator often claims a crime has been committed using the victim's identity and threatens arrest. The subject demands money to help clear the victim's name or to assist in the investigation into who may be committing the crimes using the stolen identity.

Medical professionals have reported an increase in impersonations of State Medical Boards and Boards of Health. The impersonators claim the professional's license was used in a crime or to fraudulently purchase illegal drugs or medications.

The subjects generally demand prepaid cards, wire transfers, or cash to be mailed or sent overnight.

Protect Against Government Impersonation

Government or law enforcement officials will not demand payment by prepaid cards, wire transfers, or overnight mailed cash, nor contact a subject by phone to notify they are under investigation.

Legitimate government or law enforcement actions will likely occur in person or by official letters.

Phone numbers can be spoofed easily. Do not always trust the number on your caller ID.

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 a common interests, age, religion, or ethnicity—to utilize the common interests to build trust to effectively operate the investment fraud against them. The perpetrators range from professional investment advisers to persons trusted and interacted with daily, such as a neighbor, sports coach, or online relationship. The fraudster's ability to foster trust makes these schemes so successful. Investors should use scrutiny and gather as much information as possible before entering any new investment opportunities.

Confidence Fraud/Romance scammers often manipulate victims to convince them to support fraudulent investments. Criminals utilize the apparent relationship to encourage the victim to invest into ventures which the victim knows little about such as virtual currency. Trusting their online relationship, the victim begins sending funds via virtual currency to non-existent investments. Elderly victim losses in 2020 related to this type of investment fraud exceed $20 million.

Protect Against Investment Fraud

Do not judge a person or company by their website; flashy websites can be set up quickly.

Do not invest in anything you are not sure about. Do your homework on the investment and the company to ensure that they are legitimate.

Check out other websites regarding this person/company.

Be cautious when responding to special investment offers, especially through unsolicited e-mail.

Be cautious when dealing with foreign individuals/companies.

Inquire about all the terms and conditions.

If it sounds too good to be true, it likely is. Watch out for "get rich quick" promises.

APPENDIX A: DEFINITIONS

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.

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.

Charity: Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.

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.

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 leak or spill of business data that is released from a secure location to an untrusted environment. It may also refer to 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.

Hacktivist: A computer hacker whose activity is aimed at promoting a social or political cause.

Harassment/Threats of Violence: Harassment occurs when a perpetrator uses false accusations or statements of fact to intimidate a victim. 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.

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 on the basis of 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.

Misrepresentation: Merchandise or services were purchased or contracted by individuals online for which the purchasers provided payment. The goods or services received were of a measurably lesser quality or quantity than was described by the seller.

Non-Payment/Non-Delivery: In non-payment situations, goods and services are shipped, but payment is never rendered. In non-delivery situations, payment is sent, but goods and services are never received.

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: 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.

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”.