June 2019 | U.S. Attorney's Office for the Eastern District of Kentucky |

FCBA Bench and Bar CLE

Cybercrime

Cybercrime

In recent years, the Department of Justice has ramped up efforts to combat cybercrime. Cybercrime encompasses a vast and ever-changing array of criminality. Hackers attack computer systems to obtain information, extort money, or otherwise cause disarray. Perpetrators all over the world target U.S.-based victims through phishing, tech fraud, and hundreds of other scams, in order to defraud U.S. citizens of substantial sums of money. Cybercriminals also have at their disposal online mechanisms for money transfer and laundering at a speed and rate previously unseen in the law enforcement community.

What makes matters more difficult is the anonymity that cybercrime affords criminals. Sophisticated masking tools, available on the open internet and dark web, obfuscate the identity and location of criminals. Encrypted platforms shield communications between coconspirators from law enforcement.

While cybercrime is certainly trending upwards and law enforcement is working diligently to combat cybercrime, members of society must be cautious when it comes to their own online activity. Recognizing a scam or a potential breach is as important in fighting cybercrime as law enforcement's efforts to bring justice to the perpetrators.

Spotlight Cyber Stalking and Threats

The U.S. Attorney's Office for the Eastern District of Kentucky has recently brought a focus on cybercrimes targeting individuals. It has prosecuted individuals for communicating threats over the internet, cyberbullying, and cyber stalking.

Contents

ABOUT THE INTERNET CRIME COMPLAINT CENTER

The mission of the FBI is to protect the American people and uphold the Constitution of the United States.

The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners. Information is analyzed and disseminated for investigative and intelligence purposes, for law enforcement, and for public awareness.

In an effort to promote public awareness, the IC3 produces this annual report to aggregate and highlight the data provided by the general public. The quality of the data is directly attributable to the information ingested via the public interface www.ic3.gov. The IC3 attempts to standardize the data by categorizing each complaint based on the information provided. The IC3 staff analyzes the data to identify trends in Internet-facilitated crimes and what those trends may represent in the coming year.

In 2018, the Victim Services Division (VSD) collaborated with the IC3 to develop a new position – Victim Specialists -Internet Crimes (VSIC). VSD secured approval and funding for three positions to be placed at the IC3. These VSIC positions are able to contact victims, provide crisis intervention, conduct needs assessments, and refer victims to resources and referrals when appropriate. In many circumstances, complaints involving cyberbullying, harassment, ID theft, and confidence scams may never rise to the level of a Federal investigation. Due to the nature of the system through which these complaints are vetted and then filtered down to local law enforcement officers, victims may not get the help they need in time. The FBI is obligated to try and triage these victims as their first line of defense. VSICs positioned at IC3 facilitate the necessary support services for victims that reach out. The key component in this process of assistance is to ensure timely support and services are provided to prevent further victimization and to engage the recovery process as quickly as possible.

The benefit from VSICs positioned at IC3 is that they are able to quickly reach out and call these victims to intervene and offer assistance. Many victims do not believe they have been compromised and genuinely want to help the perpetrator. Skilled VSICs can help navigate those feelings for the victim, allow them to come to terms with what has happened, and provide them the resources and steps necessary to get their life back together.

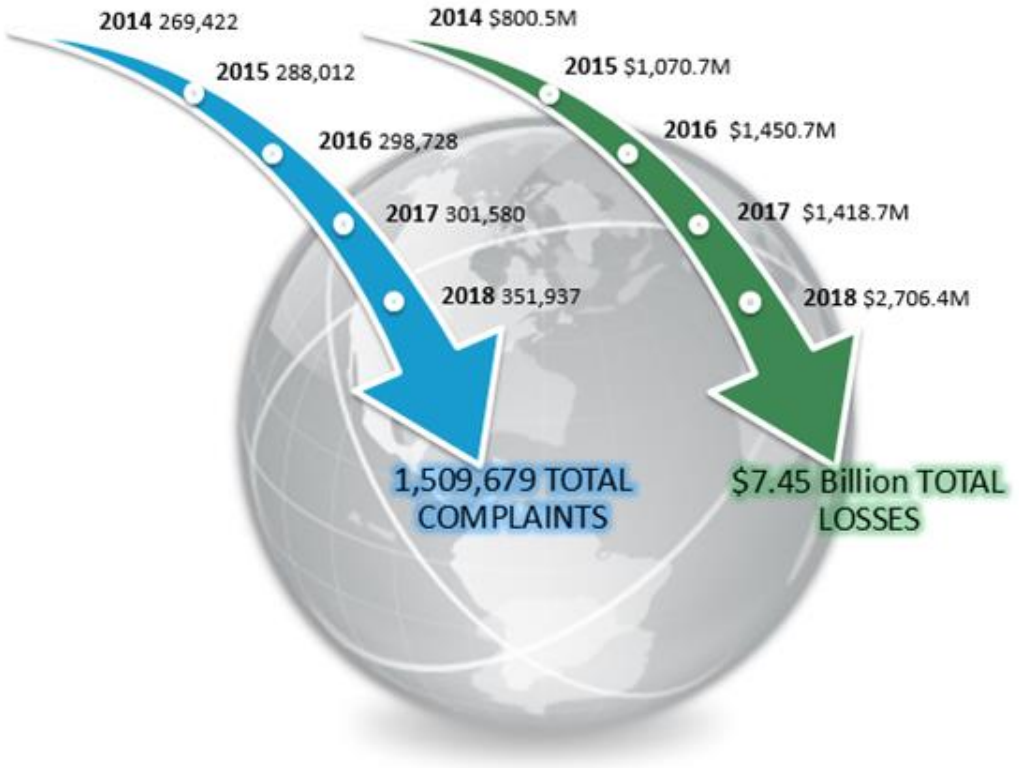
These positions also lead to a greater coordination of services. VSICs at IC3 work with the victim's local field office Victim Specialist (VS) to coordinate in-person services and support. VSICs at IC3 have the opportunity to liaison with their counterparts in the field and, should the situation warrant, they can work with the VS in the victim's area to facilitate a follow up meeting. This tremendously benefits VSs in the field in that the IC3 VSICs have developed much of the preliminary information the VS would try to assess in their first meeting with the victim. The field VS is able to work more efficiently with greater background information available prior to their first encounter. Timely victim assistance and support can further victimization and can start the victim instead on a path towards recovery.

IC3 HISTORY

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. There have been 4,415,870 complaints reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of almost 300,000 complaints per year. The complaints address a wide array of Internet scams affecting victims across the globe.[1]

IC3 Complaint Statistics

2014-2018



[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2014 to 2018. Over that time period, IC3 received a total of 1,509,679 complaints, and a total loss of $7.45 billion.

THE IC3 ROLE IN COMBATING CYBER CRIME[2]

WHAT WE DO

Central Hub to Alert the Public

Victims Report Internet Crime Via

www.IC3.gov

Partner with Private Sector and with Local, State, Federal, and International Agencies

Increase Victim Reporting via Outreach

Host Remote Access Database for all Law Enforcement via the FBI's LEEP website

[2] Accessibility description - images depicts what IC3 does to include providing a central hub to alert the public; victim reporting at www.ic3.gov; partner with private sector and with local, state, federal, and international agencies; increase victim reporting via outreach; host a remote access database for all law enforcement via the FBI's LEEP website

IC3 CORE FUNCTIONS

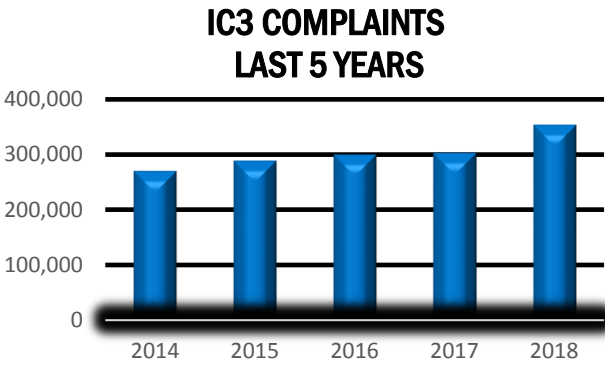
COLLECTION	ANALYSIS	PUBLIC AWARENESS	REFERRALS
The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to Internet crime, as well as any other relevant information necessary to support the complaint.	The IC3 reviews and analyzes data submitted through its website and produces intelligence products to highlight emerging threats and new trends.	Public service announcements (PSAs), scam alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of Internet crimes and the methods used to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.	The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement conducts an investigation and determines a crime has been committed, legal action may be brought against the perpetrator.

IC3 Core Functions[3]

[3] Accessibility description: image contains a table and wheel with the core functions. Core functions are listed in individual blocks- Collection, Analysis, Public Awareness, and Referrals as components of an ongoing process.

2018 Overall Statistics[13]

IMPORTANT STATS



 # Of Complaints Reported Since Inception ('00)
4,415,870

Approximately 300,000
Complaints Received Per Year On Average

$2.71 Billion
Victim Losses in **2018**

Over 900
Complaints Received Per Day On Average

2018 VICTIMS BY AGE GROUP

Victims		
Age Range[14]	Total Count	Total Loss
Under 20	9,129	$12,553,082
20 - 29	40,924	$134,485,965
30 - 39	46,342	$305,699,977
40 - 49	50,545	$405,612,455
50 - 59	48,642	$494,926,300
Over 60	62,085	$649,227,724

[13] Accessibility description: image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints for the years 2014 to 2018. The total number of complaints received since the year 2000 is 4,415,870. IC3 receives approximately 300,000 complaints each year, or more than 900 per day.
[14] Not all complaints include an associated age range—those without this information are excluded from this table.

2018 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

Descriptors*

Social Media	40,198
Virtual Currency	36,477

*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.

2018 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,297,803,489	Tech Support	$38,697,026
Confidence Fraud/Romance	$362,500,761	Harassment/Threats of Violence	$21,903,829
Investment	$252,955,320	Misrepresentation	$20,000,713
Non-Payment/Non-Delivery	$183,826,809	IPR/Copyright and Counterfeit	$15,802,011
Real Estate/Rental	$149,458,114	Civil Matter	$15,172,692
Personal Data Breach	$148,892,403	Malware/Scareware/ Virus	$7,411,651
Corporate Data Breach	$117,711,989	Health Care Related	$4,474,792
Identity Theft	$100,429,691	Ransomware	*$3,621,857
Advanced Fee	$92,271,682	Denial of Service/TDos	$2,052,340
Credit Card Fraud	$88,991,436	Re-Shipping	$1,684,179
Extortion	$83,357,901	Charity	$1,006,379
Spoofing	$70,000,248	Gambling	$926,953
Government Impersonation	$64,211,765	Crimes Against Children	$265,996
Other	$63,126,929	Hacktivist	$77,612
Lottery/Sweepstakes	$60,214,814	Terrorism	$10,193
Overpayment	$53,225,507	No Lead Value	$0.00
Phishing/Vishing/Smishing/Pharming	$48,241,748		
Employment	$45,487,120		

Descriptors*

Social Media	$101,045,973	*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.
Virtual Currency	$182,106,976	

***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 ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.**

2018 OVERALL STATE STATISTICS

Count by Victim per State*

Rank	State	Victims	Rank	State	Victims
1	California	49,031	30	Kentucky	2,813
2	Texas	25,589	31	Oklahoma	2,644
3	Florida	23,984	32	New Mexico	2,127
4	New York	18,124	33	Kansas	2,098
5	Virginia	14,800	34	Iowa	1,983
6	Washington	10,775	35	Mississippi	1,882
7	Pennsylvania	10,554	36	Arkansas	1,849
8	Illinois	10,087	37	Alaska	1,603
9	Colorado	9,328	38	Idaho	1,513
10	Georgia	9,095	39	District of Columbia	1,364
11	Maryland	8,777	40	Nebraska	1,205
12	New Jersey	8,440	41	West Virginia	1,109
13	Arizona	8,027	42	Hawaii	1,100
14	Ohio	7,812	43	New Hampshire	1,056
15	Michigan	7,533	44	Rhode Island	1,028
16	North Carolina	7,523	45	Delaware	897
17	Wisconsin	6,621	46	Maine	832
18	Massachusetts	6,173	47	Montana	787
19	Tennessee	5,584	48	Puerto Rico	704
20	Missouri	5,508	49	Vermont	525
21	Nevada	5,228	50	Wyoming	497
22	Indiana	4,676	51	South Dakota	465
23	Alabama	4,585	52	North Dakota	459
24	Oregon	4,511	53	U.S. Virgin Islands	65
25	Minnesota	4,304	54	Guam	52
26	South Carolina	3,575	55	U.S. Minor Outlying Islands	47
27	Louisiana	3,469	56	American Samoa	16
28	Connecticut	3,134	57	Northern Marina Islands	15
29	Utah	3,041			

***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.**

2018 Overall State Statistics *Continued*

Total Losses by Victim per State*

Rank	State	Loss	Rank	State	Loss
1	California	$450,482,128	30	Louisiana	$16,396,262
2	New York	$201,090,065	31	Iowa	$15,337,975
3	Texas	$195,611,047	32	Oklahoma	$11,587,907
4	Florida	$178,141,470	33	Nebraska	$9,426,684
5	North Carolina	$137,230,988	34	Kentucky	$9,352,781
6	Ohio	$97,730,046	35	District of Columbia	$8,899,830
7	Illinois	$82,849,726	36	New Mexico	$8,617,772
8	Michigan	$80,929,815	37	West Virginia	$8,298,753
9	New Jersey	$79,711,752	38	Arkansas	$6,971,524
10	Massachusetts	$68,242,216	39	Rhode Island	$6,929,001
11	Pennsylvania	$62,692,761	40	Idaho	$6,853,195
12	Georgia	$61,466,974	41	Montana	$6,612,063
13	Washington	$60,513,117	42	Hawaii	$6,460,785
14	Minnesota	$48,814,059	43	New Hampshire	$6,084,633
15	Maryland	$47,180,259	44	Mississippi	$5,725,032
16	Arizona	$45,166,115	45	Puerto Rico	$5,219,087
17	Virginia	$43,792,436	46	Wyoming	$4,517,128
18	Connecticut	$37,859,918	47	Alaska	$3,616,856
19	Colorado	$34,082,849	48	Delaware	$3,141,393
20	Indiana	$29,577,716	49	U.S. Virgin Islands	$2,723,790
21	Nevada	$28,920,936	50	Maine	$2,699,746
22	Oregon	$28,599,963	51	North Dakota	$2,296,789
23	Tennessee	$28,590,404	52	Vermont	$2,127,317
24	Missouri	$25,577,740	53	South Dakota	$1,733,826
25	Wisconsin	$24,649,284	54	Guam	$155,055
26	Utah	$20,617,421	55	U.S. Minor Outlying Islands	$96,346
27	South Carolina	$19,567,920	56	American Samoa	$18,537
28	Kansas	$17,474,768	57	Northern Mariana Islands	$13,865
29	Alabama	$16,911,098			

***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.**

2018 Overall State Statistics *Continued*

Count by Subject per State*

Rank	State	Subjects	Rank	State	Subjects
1	California	15,975	30	Wisconsin	858
2	Texas	10,252	31	District of Columbia	845
3	Florida	9,141	32	Utah	843
4	Virginia	7,569	33	Delaware	825
5	New York	7,352	34	Kentucky	783
6	Maryland	4,279	35	Montana	739
7	Illinois	3,919	36	Mississippi	710
8	New Jersey	3,645	37	Connecticut	624
9	Georgia	3,081	38	Iowa	600
10	Washington	2,819	39	Arkansas	498
11	Pennsylvania	2,601	40	New Mexico	428
12	Michigan	2,309	41	North Dakota	352
13	Ohio	2,258	42	Idaho	348
14	Nevada	2,251	43	Hawaii	300
15	Arizona	2,089	44	Rhode Island	297
16	Tennessee	2,016	45	Alaska	268
17	North Carolina	1,997	46	West Virginia	261
18	Colorado	1,707	47	New Hampshire	242
19	Nebraska	1,653	48	Maine	240
20	Massachusetts	1,485	49	South Dakota	166
21	Missouri	1,375	50	Vermont	140
22	Oregon	1,257	51	Wyoming	140
23	Indiana	1,209	52	Puerto Rico	115
24	South Carolina	1,124	53	U.S. Minor Outlying Islands	16
25	Alabama	1,059	54	U.S. Virgin Islands	15
26	Minnesota	969	55	Guam	4
27	Louisiana	935	56	American Samoa	3
28	Oklahoma	872	57	Northern Mariana Islands	3
29	Kansas	866			

***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.**

2018 Overall State Statistics *Continued*

Subject Earnings per Destination State*

Rank	State	Loss	Rank	State	Loss
1	California	$181,698,326	30	Louisiana	$5,395,827
2	Florida	$93,294,872	31	Hawaii	$4,997,730
3	Maryland	$85,984,642	32	Utah	$4,953,576
4	New York	$84,538,779	33	Alabama	$4,411,596
5	Texas	$79,616,314	34	Wisconsin	$4,171,769
6	Georgia	$45,325,413	35	Iowa	$4,133,227
7	Illinois	$23,843,582	36	Kentucky	$3,995,141
8	New Jersey	$23,499,992	37	Arkansas	$3,687,941
9	Nevada	$23,398,329	38	Puerto Rico	$3,617,864
10	Michigan	$20,486,316	39	Mississippi	$3,562,790
11	Pennsylvania	$19,479,628	40	New Mexico	$3,477,718
12	North Carolina	$17,481,764	41	Delaware	$3,241,823
13	Colorado	$16,371,194	42	Idaho	$3,235,557
14	Virginia	$15,427,366	43	Kansas	$2,489,295
15	Missouri	$14,273,141	44	Montana	$2,090,337
16	Arizona	$13,737,455	45	Wyoming	$2,052,206
17	Washington	$13,587,420	46	Alaska	$1,936,162
18	Tennessee	$11,485,660	47	Rhode Island	$1,668,834
19	Massachusetts	$9,787,562	48	North Dakota	$920,577
20	Indiana	$9,317,973	49	Maine	$772,482
21	Oklahoma	$8,579,862	50	West Virginia	$731,691
22	Ohio	$8,413,509	51	South Dakota	$482,016
23	South Carolina	$7,294,220	52	Vermont	$244,045
24	Connecticut	$7,030,105	53	U.S. Minor Outlying Islands	$23,402
25	District of Columbia	$6,877,801	54	U.S. Virgin Islands	$12,597
26	Minnesota	$6,604,137	55	Guam	$10,613
27	New Hampshire	$5,612,713	56	American Samoa	$7,000
28	Nebraska	$5,475,575	57	Northern Mariana Islands	$0.00
29	Oregon	$5,472,776			

***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.**

Select a state: **Kentucky**

Crime Type by Victim Count			
Crime Type	*Victim Count*	*Crime Type*	*Victim Count*
Advanced Fee	172	Identity Theft	124
BEC/EAC	152	Investment	6
Charity	3	Lottery/Sweepstakes/Inheritance	92
Civil Matter	4	Malware/Scareware/Virus	20
Confidence Fraud/Romance	210	Misrepresentation	53
Corporate Data Breach	28	No Lead Value	99
Credit Card Fraud	150	Non-payment/Non-Delivery	601
Crimes Against Children	14	Other	81
Denial of Service/TDos	5	Overpayment	128
Employment	112	Personal Data Breach	434
Extortion	373	Phishing/Vishing/Smishing/Pharming	179
Gambling	4	Ransomware	17
Government Impersonation	106	Re-shipping	9
Hacktivist	0	Real Estate/Rental	76
Harassment/Threats of Violence	187	Spoofing	136
Health Care Related	2	Tech Support	143
IPR/Copyright and Counterfeit	11	Terrorism	2
Descriptors*			
Social Media	363	Virtual Currency	214

*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.

Crime Type by Victim Loss			
Crime Type	*Loss Amount*	*Crime Type*	*Loss Amount*
Advanced Fee	$472,212	Identity Theft	$68,497
BEC/EAC	$3,399,040	Investment	$1,133,857
Charity	$25	Lottery/Sweepstakes/Inheritance	$373,097
Civil Matter	$0	Malware/Scareware/Virus	$30,425

Confidence Fraud/Romance	$1,527,974	Misrepresentation	$76,016
Corporate Data Breach	$237,024	No Lead Value	$0
Credit Card Fraud	$594,410	Non-payment/Non-Delivery	$1,446,743
Crimes Against Children	$0	Other	$57,134
Denial of Service/TDos	$0	Overpayment	$301,818
Employment	$1,250,869	Personal Data Breach	$245,630
Extortion	$160,293	Phishing/Vishing/Smishing/Pharming	$116,551
Gambling	$400	Ransomware	$3,650
Government Impersonation	$129,546	Re-shipping	$0
Hacktivist	$0	Real Estate/Rental	$210,421
Harassment/Threats of Violence	$553,745	Spoofing	$431,544
Health Care Related	$386	Tech Support	$122,304
IPR/Copyright and Counterfeit	$679	Terrorism	$0
Descriptors*			
Social Media	$1,906,805	Virtual Currency	$90,932

*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.

Crime Type by Subject Count			
Crime Type	*Subject Count*	*Crime Type*	*Subject Count*
Advanced Fee	38	Identity Theft	32
BEC/EAC	21	Investment	13
Charity	3	Lottery/Sweepstakes/Inheritance	19
Civil Matter	2	Malware/Scareware/Virus	2
Confidence Fraud/Romance	71	Misrepresentation	22
Corporate Data Breach	7	No Lead Value	20
Credit Card Fraud	40	Non-payment/Non-Delivery	215
Crimes Against Children	3	Other	28
Denial of Service/TDos	1	Overpayment	59
Employment	29	Personal Data Breach	132
Extortion	73	Phishing/Vishing/Smishing/Pharming	30

Gambling	6	Ransomware	2
Government Impersonation	15	Re-shipping	1
Hacktivist	0	Real Estate/Rental	14
Harassment/Threats of Violence	73	Spoofing	30
Health Care Related	0	Tech Support	13
IPR/Copyright and Counterfeit	7	Terrorism	0
Descriptors*			
Social Media	101	Virtual Currency	42

*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.

Crime Type by Subject Loss			
Crime Type	*Loss Amount*	*Crime Type*	*Loss Amount*
Advanced Fee	$189,595	Identity Theft	$6,625
BEC/EAC	$760,154	Investment	$203,671
Charity	$0	Lottery/Sweepstakes/Inheritance	$152,994
Civil Matter	$5,000	Malware/Scareware/Virus	$500
Confidence Fraud/Romance	$803,478	Misrepresentation	$179,787
Corporate Data Breach	$0	No Lead Value	$0
Credit Card Fraud	$579,601	Non-payment/Non-Delivery	$1,358,607
Crimes Against Children	$0	Other	$22,801
Denial of Service/TDos	$0	Overpayment	$71,554
Employment	$57,058	Personal Data Breach	$19,427
Extortion	$3,350	Phishing/Vishing/Smishing/Pharming	$16,050
Gambling	$1,347	Ransomware	$0
Government Impersonation	$1,200	Re-shipping	$0
Hacktivist	$0	Real Estate/Rental	$72,832
Harassment/Threats of Violence	$18,620	Spoofing	$63,557
Health Care Related	$0	Tech Support	$4,900
IPR/Copyright and Counterfeit	$94	Terrorism	$0
Descriptors*			

Social Media	$221,123	Virtual Currency	$17,482

*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.

Victims by Age Group		
Age Range	*Count*	*Amount Loss*
Under 20	84	$48,822
20 - 29	303	$891,773
30 - 39	423	$430,809
40 - 49	418	$1,636,303
50 - 59	432	$2,425,810
Over 60	521	$2,903,545

Federal Bureau of Investigation

Addressing Threats to the Nation's Cybersecurity

As the primary investigative agency of the federal government for more than a hundred years, the responsibilities of the Federal Bureau of Investigation (FBI) have kept pace with ever-emerging threats and crime trends affecting the United States. From the notorious gangsters of the early 20th century, to espionage and sabotage during World War II, through the Cold War years and the global war on terrorism, the FBI has protected our nation. The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences. While the FBI must adapt to meet these challenges, addressing the broad range of threats to the nation's cybersecurity is squarely within its mandate. *Why the FBI?*

It's our job.

The FBI has a unique dual responsibility, to prevent harm to national security as the nation's domestic intelligence agency and to enforce federal laws as the nation's principal law enforcement agency. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred.

The FBI's unified mission brings all lawful investigative techniques and legal tools together in combating these threats. This approach facilitates information sharing and ensures responsible stewardship of resources by collocating talent, tools, and institutional knowledge in a single organization.

- **Domestic Coordination within the U.S. Intelligence Community**

  As a member of the U.S. Intelligence Community (USIC), the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF). Located in the Washington, D.C. metro area, the NCIJTF serves by Presidential Directive as the national focal point for coordinating cyber threat investigations. Representatives from the USIC member agencies, as well as select federal law enforcement partners, are present at the center and collaborate in identifying, mitigating, and disrupting cybersecurity threats.

- **Support to the Homeland Security Enterprise**

  As part of the homeland security enterprise, the FBI supports the Department of Homeland Security's (DHS) mission by investigating threats and incidents which affect the security of protected computers and networks. The results of these investigations increase collective knowledge which can be leveraged to improve the nation's security posture, such as providing effective mitigation strategies to potential victims. Additionally, actions taken by the FBI have succeeded in disrupting and dismantling threats. With the entire homeland security enterprise working together, and through a balanced approach employing both defensive measures and directed action against adversaries, our nation is safer.

Roles and Authorities in Brief

The FBI has the authority and responsibility to investigate and enforce all violations of federal law that are not exclusively assigned to another federal agency.
- Title 28, USC Section 533 & 28 CFR 0.85

"The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime."
- The President's National Strategy to Secure Cyberspace, 2003

"The FBI is vested by law with the primary role in carrying out investigations within the United States of threats to the nation's security. This includes the lead domestic role in the investigation of international terrorist threats…and in the conduction of counterintelligence activities against foreign espionage and intelligence efforts directed against the U.S."
- Attorney General Guidelines for Domestic FBI Operations

"Intelligence elements of the FBI…shall collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence…"
- Executive Order 12333 and pursuant to Title 50, USC Section 401

- **Leadership within U.S. Law Enforcement**

  The FBI's capacity to respond to cyber incidents and emergencies in communities nationwide is enhanced through task force partnerships with other law enforcement agencies. Key federal, state, and local cyber investigative and forensic personnel, sworn and civilian, are teamed together in this endeavor. The FBI is enhancing the capabilities of each of its cyber task forces to address the full range of cybersecurity threats and function as extensions of the NCIJTF. No other agency can match this broad and robust presence, which is crucial for timely and effective incident response.

In the U.S. and abroad, we are where you need us.

Domestic — Whether you live and work in a large city or small town, chances are that the FBI has an office nearby. FBI field offices are located in 56 cities, with satellite offices in some 380 additional locations. Cyber agents at each field office are equipped to respond to events ranging from a significant data breach to a national cyber emergency. And, to supplement this standing capability, the FBI also maintains a rapid deployment team of highly specialized cyber agents.

International — Not only does 21st century technology enable global communication and commerce, it enables threat actors to apply their craft from anywhere in the world. For nearly 70 years, the FBI has stationed personnel overseas to build relationships that protect Americans at home. Today, the FBI maintains legal attaché offices within 75 U.S. Embassies globally, covering over 200 countries. Additionally, cyber agents have been embedded with foreign law enforcement partners in several key countries, fulfilling a liaison role to foster cooperation and mutual legal assistance.

We acknowledge the unique capabilities of private industry and academia, and the need for constant collaboration.

The U.S. Government cannot address cybersecurity threats alone. Ongoing collaboration with affected industries, security researchers, and academia is indispensible. The FBI maintains a presence and close partnership with the National Cyber Forensics and Training Alliance (NCFTA), and shares intelligence with the private sector through FBI-led InfraGard chapters and through various industry-specific Information Sharing and Analysis Centers (ISACs). In partnership with the National White Collar Crime Center (NW3C), the FBI offers the Internet Crime Complaint Center (IC3) as a means to receive cyber crime complaints from consumers and businesses for action by authorities, and to disseminate fraud alerts to the public.

FBI Headquarters, J. Edgar Hoover Building

We defend the Constitution by upholding the law, while protecting privacy and civil liberties.

Roles and responsibilities within the Executive Branch agencies are divided to ensure mission focus and clarity in regard to authorities. As a component of the Department of Justice, the FBI is responsible for investigations and intelligence collection within the territorial jurisdiction of the United States and relating to U.S. persons overseas.

Bound by the U.S. Constitution, relevant laws, and guidelines provided by the Attorney General, the FBI is governed by the principle of employing the least intrusive method necessary to further an investigation. When an investigative method would infringe upon an individual's reasonable expectation of privacy, approval and oversight by a U.S. District Court or the Foreign Intelligence Surveillance Court is required.

In its role as a protector and defender of the U.S. Constitution and enforcer of federal law, the FBI regularly takes action on behalf of victims whose privacy has been violated, such as through a computer intrusion or identity theft.

We care.

In the last decade, the FBI has assembled a team of hundreds of cyber experts with diverse and highly skilled information technology backgrounds. Our people are committed to serving the public by meeting cyber challenges head on and imposing consequences on those who victimize the American people through the misuse of computers and networks.

REPORTING COMPUTER HACKING, FRAUD AND OTHER INTERNET-RELATED CRIME

The primary federal law enforcement agencies that investigate domestic crime on the Internet include: the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE) , the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF) . Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. In general, federal crime may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the "Duty Complaint Agent.

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases.

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, please refer to the following table:

Type of Crime	**Appropriate federal investigative law enforcement agencies**
Computer intrusion (i.e. hacking)	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Password trafficking	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Counterfeiting of currency	• U.S. Secret Service
Child Pornography or Exploitation	• FBI local office • if imported, U.S. Immigration and Customs Enforcement • Internet Crime Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	• U.S. Postal Inspection Service • Internet Crime Complaint Center
Internet fraud and SPAM	• FBI local office • U.S. Secret Service • Federal Trade Commission (online complaint)

	• if securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint) • Internet Crime Complaint Center
Internet harassment	• FBI local office
Internet bomb threats	• FBI local office • ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	• FBI local office • ATF local office

Other Cybercrime Reporting Resources

- **The Internet Crime Complaint Center (IC3)**

  The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

  The Internet Crime Complaint Center

- Department of Homeland Security's National Infrastructure Coordinating Center: (202) 282-9201 (report incidents relating to national security and infrastructure issues)
- U.S. Computer Emergency Readiness Team (U.S. CERT) (online reporting for technicians)

devices when they are given access to them. This includes communicating with others online and sending photos. Parents may want to maintain their child's online account access information with the child's understanding that the parent can log in at any time.

Communicate with your children.

Have age-appropriate discussions with your child about the dangers associated with communicating with unknown people online, sending photos, or engaging in other risky behavior online. In an effort to protect children from online predators, it's important to educate them about sextortion and the motivations of those who extort children. Let your children know they can come to you without fear of reprisal, and that you have a genuine interest in their safety and online activities. Those exploited through these crimes are victims, no matter what they did or how they responded to the threat.

Layer security.

Employ basic technology security measures. Use strong passwords and update software regularly. Never open attachments to e-mails unless you are certain of the sender. Use a firewall, anti-malware software, and consider use of encryption for your hard drive. Keep in mind that some malware attacks are targeted, meaning criminals may customize their tools so that more simplistic anti-malware programs do not detect them and victims are more apt to take the bait. Do not assume technology alone will protect you; you must also do your part to protect yourself.

For Children:

- Turn off your computer when you are not using it.
- Cover webcams with a removable sticker or tape when you are not using them.
- Don't open attachments when you're not confident of the sender.
- Never send compromising images of yourself to anyone, no matter who they are or who they say they are.
- If someone you know is being victimized through sextortion, report it to your parents and encourage the victim to talk to their parents and report it to the FBI.
- If you are receiving sextortion threats, don't be afraid to talk to your parents or to call the FBI.

How do I Report a Suspected Incidence of Sextortion?

Report sextortion to the FBI.

It is important to report all instances to law enforcement. While in some cases the person committing sextortion is also a teenager, it is more likely that the perpetrator is an adult masquerading as a teenager. Law enforcement can make that determination and take steps to help minimize further distribution of sensitive material. A parent's report may result in the rescue of dozens or even hundreds of other children.

To report suspected sextortion crimes or to get help from law enforcement, call your local FBI office or toll-free, at 1-800-CALL-FBI (225-5324).

Resources:

- The National Center for Missing and Exploited Children (www.missingkids.com)
- FBI Cyber Alerts for Parents and Kids: Be Prudent When Posting Images Online (http://www.fbi.gov/news/stories/2011/december/cyber_122211/cyber_122211)
- FBI Cyber Alerts for Parents and Kids: Be Aware of 'Sextortion' (http://www.fbi.gov/news/stories/2012/february/sextortion_021012)

July 2015

U.S. Department of Justice
Federal Bureau of Investigation

SEXTORTION OF CHILDREN IN THE UNITED STATES

A Fact Sheet for Parents and Children

What is Sextortion?

Sextortion is a criminal act that occurs when someone demands something of value, typically images of a sexual nature, sexual favors, or money, from a person by either:

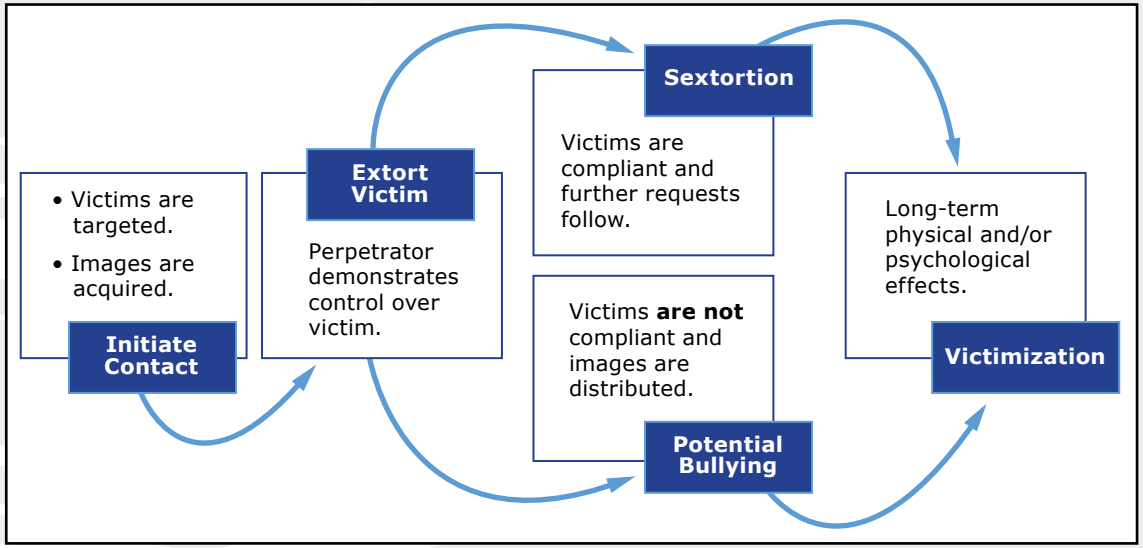
- Threatening to release or distribute material the victim seeks to keep private. This material often includes sexually explicit images, videos, e-mail, and text messages
- Threatening to financially harm friends or relatives of the victim by using information obtained from the victim's computer unless they comply with demands
- Withholding something the victim needs or wants unless they comply with demands. This is usually perpetrated by someone in a position of power or authority, such as a government official, educator, or employer

How Does Sextortion Happen?

Sextortion can be facilitated in many ways by those seeking to exploit vulnerable individuals sexually or for financial gain. They typically begin by obtaining sensitive material pertaining to their victims. Some of the methods include:

- Hacking or use of malware to assume control of a victim's computer, gaining access to the victim's files, and/or control of the computer's webcam and microphone
- Theft of personal electronic devices that contain sensitive material
- Social engineering -- leading the victim to believe the perpetrator can be trusted as the perpetrator represents himself/herself as a business (i.e. modeling agency), friend, or even the victim's boyfriend or girlfriend. This results in the victim releasing sensitive material to the perpetrator
- Identity theft

These tactics are typically conducted over the Internet or cellular networks using social networking sites (SNS), instant messaging, and e-mail. The diagram below illustrates a typical sextortion process:



How is Sextortion Related to "Sexting" and Bullying?

Sexting is the sending of sexually explicit images from one person to another using mobile devices. Sexting is one way images come into the possession of a perpetrator who could use them to facilitate the sextortion. When sexually explicit images of a student are distributed to their peers, those images often become the basis of intense bullying in a school environment.

Who is at Risk and What is the Impact?

Sextortion affects children across all demographics. Victims of sextortion withdraw from family members and can experience anxiety; psychological, physical and emotional trauma; bullying; increased risk for suicide; and increased dropout rates.

Examples of Sextortion Cases:

- ***In November, 2014***, Lucas Michael Chansler, 30, of Jacksonville, Florida, was sentenced to 105 years in prison for producing child pornography. During a four-year period, Chansler is believed to have sexually extorted approximately 350 victims in 26 states, three Canadian provinces, and the United Kingdom.
- ***In March, 2014***, Jared James Abrahams, a computer science student, was sentenced to serve 18 months in federal prison after pleading guilty to three counts of extortion and one count of unauthorized access of a computer. Abrahams targeted dozens of victims around the globe, including Miss Teen USA Cassidy Wolf. Abrahams used malicious software to disguise his identity in order to capture nude photos or videos of female victims through remote operation of their webcams without their consent.
- ***Between 2005 and 2009***, Ivory Dickerson and Patrick Connolly victimized more than 3,800 children through sextortion. Using malware, Dickerson and Connolly were able to assume control of the victims' computers and then demanded the victims send sexually explicit images of themselves. Dickerson was sentenced to 110 years in prison while Connolly was sentenced to 30 years in prison.

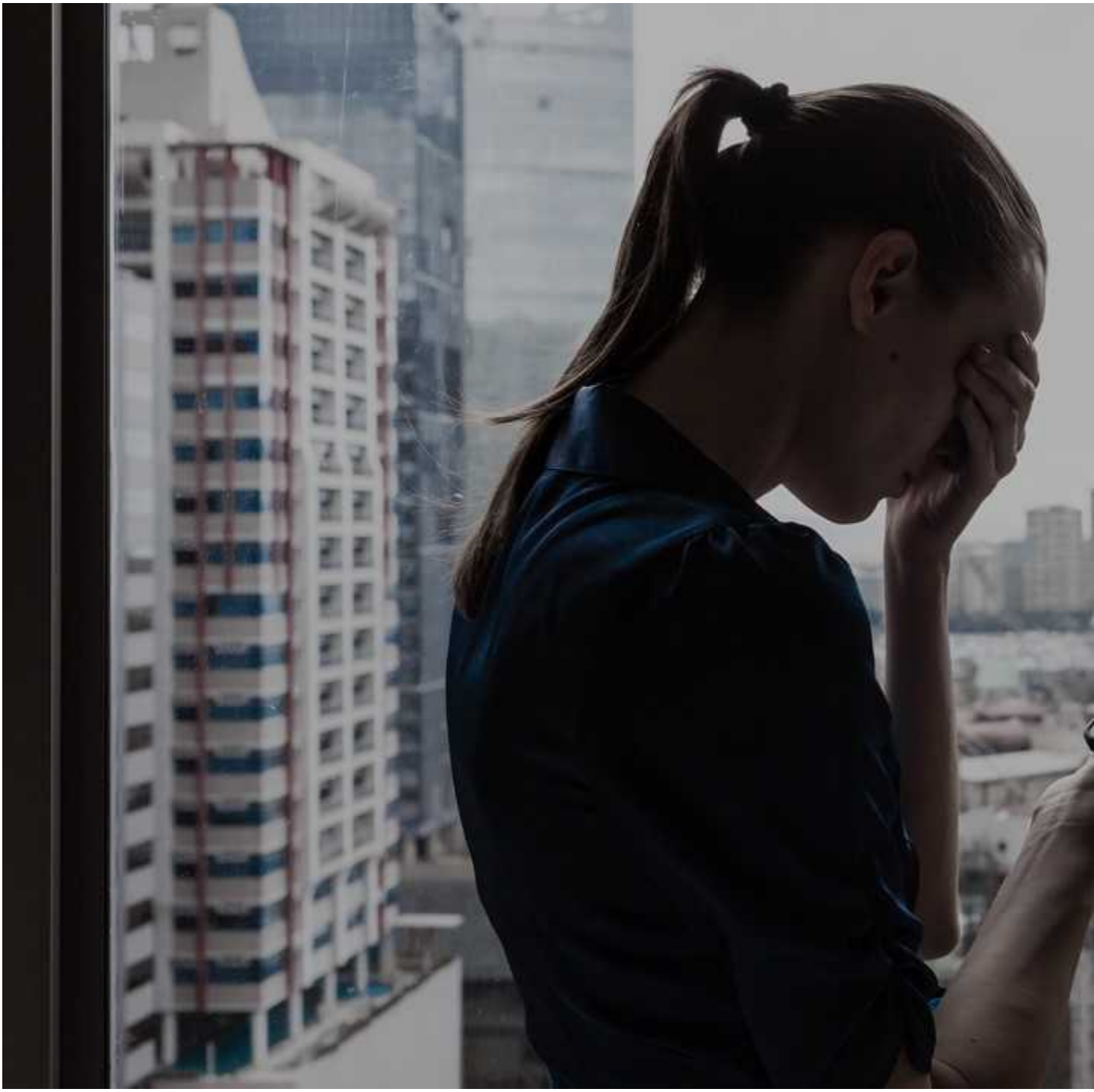
How Can I Protect Against Sextortion?

For Parents:

Supervise children's computer or mobile device usage. Devices like smartphones are more difficult to manage due to their mobility and technical capabilities. As teenagers' brains are not yet fully developed, they often struggle with anticipating consequences or impulse control. It's important to discuss with your children appropriate uses for

Cyberstalking

Two Federal Cases Illustrate the Consequences of Sextortion



Children and young adults seem particularly susceptible to sextortion—when a victim is threatened with the release of private and sensitive information unless sexual favors, nude photos, or other demands are met.

But two unrelated cyberstalking crimes committed months apart and hundreds of miles away from each other serve as a reminder of the dangers of compromising personal photos being in the wrong hands, no matter the age of the victim.

In Houston, Heriberto Latigo repeatedly used nude photos of his ex-girlfriend to coerce her to have sex with him. In Crescent, Oklahoma, Troy Allen Martin similarly blackmailed his victim for $50,000.

Both men were eventually convicted and sentenced to prison for their crimes under federal cyberstalking statutes. The harm they caused their victims, however, may never be undone. Such crimes are occurring more frequently, especially among younger victims.

Latigo not only demanded sex, he also sent his victim horrible images and threatening messages. He sent the nude photos to the victim’s sister and male co-workers, and created a disturbing Facebook page that included deeply personal information about the victim.

“It’s a violent crime; he just used cyber tools to carry it out,” said Special Agent Christopher Petrowski of the FBI’s Houston office, who worked the Latigo case.

Latigo’s victim approached local police several times. The case was complicated and the victim’s story changed a number of times, in part because of pressure from Latigo, Petrowski said, making it difficult for local authorities to help effectively. She turned to the FBI, visiting the Houston office in person in spring 2015.

“When someone walks in with a story like that, it’s very emotional and difficult to figure out right away,” Petrowski said. “They’re hurting. This went on for more than a year.”

It took some time for the FBI and federal prosecutors to determine that Latigo had likely violated federal cyberstalking laws. The FBI sent letters to social media companies to preserve certain records in order to prevent Latigo from

covering his tracks. Agents also served search warrants, seizing computer equipment from his home.

“By taking this one guy off the street, we may have prevented countless future sexual assaults. We also gave past victims some closure, which local authorities legitimately couldn’t do.”

Christopher Petrowski, special agent, FBI Houston

Members of Houston’s Innocent Images Task Force—which investigates child pornography—helped search Latigo’s electronics. They uncovered photos and were able to document that Latigo accessed social media sites from the machines.

During the course of the investigation, Petrowski discovered that other victims had filed similar complaints with local police. Although Latigo wasn’t charged in other cases, it was important to the investigation that his name was mentioned in other police reports, Petrowski said. “These other victims, who did not know each other and have never met, effectively corroborated this pattern of behavior,” he said.

Latigo was arrested in June 2015 and convicted on a federal stalking charge—using the Internet to cause substantial emotional distress—in October 2017. He was sentenced to 60 months in prison in March.

“This guy is a predator, and he targeted her from the first time they met. He had a pattern,” Petrowski said. “By taking this one guy off the street, we may have prevented countless future sexual assaults. We also gave past victims some closure, which local authorities legitimately couldn’t do.”

“He was just harassing this lady, causing severe emotional distress. He was relentless.”

Ken Western, special agent, FBI Oklahoma City

The FBI got involved in the Oklahoma case after bank employees in Ardmore noted concerning behavior surrounding the victim's attempt to wire Martin $40,000.

The victim was on the phone with Martin when she arrived at the bank. When asked for a destination bank for the wire transfer, Martin refused to tell his victim and insisted on speaking to the teller instead. The bank refused to handle the transaction.

When the wire transfer was denied, Martin told his victim to withdraw $50,000 in cash. The bank complied with the victim's request, but urged her to speak to police about the obvious coercion.

"That's a significant amount of money," said Special Agent Ken Western, who worked the case from the FBI's Oklahoma City office. "The bank thought if he was requesting money by phone, maybe it was a threatening communication. So they reported it."

The FBI reached out to the victim, who showed agents numerous text messages and played voicemails from Martin. He repeatedly said he would share nude photos he had taken of her unless she gave him money. Despite receiving $50,000, Martin also demanded a relationship and sex with the victim.

"He was just harassing this lady, causing severe emotional distress. He was relentless," Western said.

As in the Latigo case, Martin had other victims as well. He even sent the nude photos of his victim to another victim to show he was serious.

Investigators found victims through protection orders that had been filed against Martin. That information helped show a pattern of behavior. Martin found several of his victims through a dating site for divorced adults.

Martin pleaded guilty to one count of cyberstalking in October 2017. A federal judge sentenced him to 33 months' imprisonment in April.

"This goes on a lot," Western said, adding that people should not share intimate photos over the Internet or social media sites. "This lady lost $50,000, and she was extremely distressed. I hope other people will think twice about it."

Victims in both cases received support through the FBI's Victim Services Division.

What is Cyberstalking?

It is a specific federal crime and falls under a federal stalking statute as part of the Violence Against Women Act of 2005. The law was amended in 2013 to include stalking by the Internet or by telephone and no longer requires that the perpetrator and victim live in different legal jurisdictions.

The amended law in part makes it illegal to use “any interactive computer service or electronic communication service” to conduct activity that places a person “in reasonable fear” of death or serious bodily injury, or that causes or could cause “substantial emotional distress.” The law states the actions must be intentional.

Cyberstalking is punishable by up to five years in prison and a fine of $250,000. A life sentence can be imposed if the cyberstalking results in the death of a victim.

What is Sextortion?

It is a form of cyber extortion. It occurs when individuals demand their victims provide them with sexual images, sexual favors, or other things of value. There is no specific federal sextortion offense, but it falls under the federal cyberstalking law.

https://www.fbi.gov/news/stories/sentences-in-separate-cyberstalking-cases-103018