Facts + Statistics: Identity theft and cybercrime

Technology

IN THIS FACTS + STATISTICS

SHARE THIS

DOWNLOAD TO PDF

The scope of identity theft

Identity theft continues to pose challenges for consumers as criminals develop new

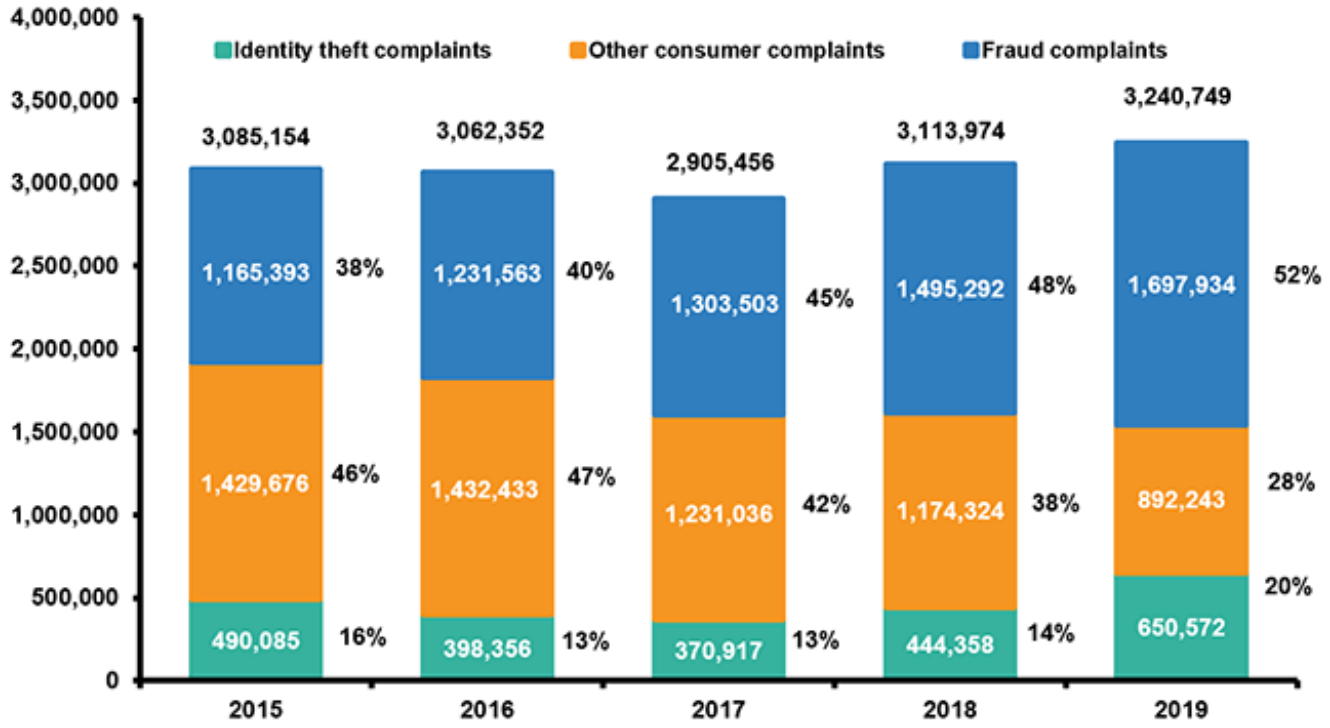
mechanisms to commit fraud. According to the 2019 Identity Fraud Study from Javelin Strategy & Research, the number of consumers who were victims of identity fraud fell to 14.4 million in 2018, down from a record high of 16.7 million in 2017. However, identity fraud victims in 2018 bore a heavier financial burden: 3.3 million people were responsible for some of the liability of the fraud committed against them, nearly three times as many as in 2016. Moreover, these victims' out-of-pocket fraud costs more than doubled from 2016 to 2018 to $1.7 billion. New account fraud losses also rose slightly, with criminals beginning to focus their attention on different financial accounts, such as loyalty and rewards programs and retirement accounts. Additionally, criminals are becoming adept at foiling authentication processes, particularly mobile phone account takeovers. These takeovers nearly doubled to 680,000 victims in 2018, compared with 380,000 in 2017. The study does note that the shift to embedded chip cards is helping to contain existing card fraud, which showed the steepest decline of any fraud type in 2018, with losses at $14.7 billion in 2018, down from $16.8 billion in 2017.

Identity theft and fraud complaints

The Consumer Sentinel Network, maintained by the Federal Trade Commission (FTC), tracks consumer fraud and identity theft complaints that have been filed with federal, state and local law enforcement agencies and private organizations. Of the 3.2 million identity theft and fraud reports received in 2019, 1.7 million were fraud-related, about 900,000 were other consumer complaints and about 651,000 were identity theft complaints. Of the 1.7 million fraud cases, 23 percent reported money was lost. In 2019 consumers reported losing more than $1.9 billion related to fraud complaints, an increase of $293 million from 2018. The median amount consumers paid in these cases was $320. Within the fraud category, imposter scams were the most reported and ranked first among the top 10 fraud categories identified by the FTC. They accounted for $667 million in losses.

In 2019, 650,570 or 20 percent of all complaints, were related to identity theft. Identity theft claims fell from 2015 to 2017 by 24 percent but began to increase again in 2018 and were up 46 percent from 2018 to 2019.

Identity Theft And Fraud Reports, 2015-2019 (1)



(1) Percentages are based on the total number of Consumer Sentinel Network reports by calendar year. These figures exclude "Do Not Call" registry complaints.

Source: Federal Trade Commission, Consumer Sentinel Network.

View Archived Graphs

Top Five Types of Identity Theft, 2019 (1)

	Number of reports	Percent of total top five
Credit card fraud—new accounts	246,763	45.7%
Miscellaneous identity theft (2)	166,875	30.9
Mobile telephone—new accounts	44,208	8.2
Business or personal loan	43,919	8.1
Auto loan or lease	38,561	7.1
Total, top five	**540,326**	**100.0%**

(1) Consumers can report multiple types of identity theft. In 2019, 18 percent of identity theft reports included more than one type of identity theft.
(2) Includes online shopping and payment account fraud, email and social media fraud, and medical services, insurance and securities account fraud, and other identity theft.

Source: Federal Trade Commission, Consumer Sentinel Network.

View Archived Tables

Identity Theft By State, 2018 (1)

State	Complaints per 100,000 population (2)	Number of complaints	Rank (3)	State	Complaints per 100,000 population (
Alabama	108	5,241	19	Montana	
Alaska	69	507	41	Nebraska	
Arizona	126	8,853	11	Nevada	1
Arkansas	73	2,197	38	New Hampshire	
California	186	73,668	3	New Jersey	1
Colorado	110	6,151	18	New Mexico	
Connecticut	108	3,864	19	New York	1
Delaware	158	1,517	7	North Carolina	
D.C.	167	1,156	5	North Dakota	
Florida	180	37,797	4	Ohio	
Georgia	229	23,871	1	Oklahoma	
Hawaii	72	1,021	40	Oregon	
Idaho	80	1,368	33	Pennsylvania	1
Illinois	127	16,296	10	Puerto Rico	
Indiana	74	4,918	36	Rhode Island	
Iowa	53	1,654	50	South Carolina	1
Kansas	74	2,142	36	South Dakota	
Kentucky	57	2,522	47	Tennessee	
Louisiana	111	5,202	17	Texas	1
Maine	56	744	48	Utah	
Maryland	145	8,747	8	Vermont	
Massachusetts	93	6,387	29	Virginia	
Michigan	140	13,952	9	Washington	1
Minnesota	73	4,070	38	West Virginia	
Mississippi	97	2,894	25	Wisconsin	
Missouri	85	5,222	32	Wyoming	

(1) Includes the District of Columbia and Puerto Rico.
(2) Population figures are based on the 2018 U.S. Census population estimates.
(3) Ranked by complaints per 100,000 population. States with the same number of complaints per 100,000 population receive the same rank.

Source: Federal Trade Commission, Consumer Sentinel Network.

View Archived Tables

See also the Identity Theft section of our Web site Click Here

Top 10 Writers Of Identity Theft Insurance By Direct Premiums Written, 2019 (1)

($000)

Rank	Group/company	Direct premiums written (2)	As a percent of total
1	State Farm Mutual Automobile Insurance	$31,492	13.4%
2	Nationwide Mutual Group	30,982	13.2
3	Travelers Companies Inc.	24,251	10.4
4	Hanover Insurance Group Inc.	12,722	5.4
5	Liberty Mutual	11,845	5.1
6	Allstate Corp.	10,863	4.6
7	American Family Insurance Group	10,119	4.3
8	Farmers Insurance Group of Companies	9,855	4.2
9	Erie Insurance Group	8,973	3.8
10	American International Group (AIG)	5,997	2.6

(1) Includes stand-alone policies and the identity theft portion of package policies. Does not include premiums from companies that cannot report premiums for identity theft coverage provided as part of package policies.
(2) Before reinsurance transactions.
(3) Includes only companies that can report premiums for stand-alone identity theft coverage and coverage provided as part of package policies.

Source: NAIC data, sourced from S&P Global Market Intelligence, Insurance Information Institute.

View Archived Tables

Cybercrime

As businesses increasingly depend on electronic data and computer networks to conduct their daily operations, growing pools of personal and financial information are being transferred and stored online. This can leave individuals exposed to privacy violations, and financial institutions and other businesses exposed to potentially enormous liability, if and when a data security breach occurs.

Interest in cyber insurance and cyberrisk continues to grow as a result of high-profile data breaches and awareness of the almost endless range of exposures businesses face. In 2019 the worst data breaches were the Capital One Financial Corp. breach in July that exposed 100 million records and the October Adobe Creative Cloud breach that exposed 7 million users. In 2017 the largest U.S. credit bureau, Equifax Inc., suffered a breach that exposed the personal data of 145 million people, including Social Security numbers. It was among the worst breaches on record because of the amount of sensitive information stolen. In 2019, ransomware attacks—a type of malware that denies access to an organization's system—more than doubled from 2018. On average, in 2019 an organization fell victim to ransomware every 14 seconds. Also troubling is that while more organizations purchase insurance to protect against the risk, ransom demands grow larger as attackers realize that the company can meet these demands.

In 2019, there were 1,473 breaches, up 17 percent from 1,257 in 2018 but below the record number of breaches in 2017, when there were 1,632 breaches. However, the number of sensitive (i.e., personal identifying information) records exposed in 2019 totaled 164.7 million, down 65 percent from 471.2 million in 2018, according to the Identity Theft Resource Center's 2019 End-of-Year Data Breach Report. The business sector again faced the highest number of breaches—644 in 2019 compared with 575 in 2018. The ITRC notes that while the business sector accounted for 44 percent of total 2019 breaches, these breaches exposed only 11 percent of all sensitive records. The medical/healthcare sector ranked second in 2019 for the number of breaches, with 525, exposing 39.4 million sensitive records. The education sector had 113 breaches, ranking third, with 2.3 million sensitive records exposed. Breaches in the banking/credit/financial sector—totaling 108—ranked fourth. However those breaches exposed 100.6 million or 61 percent of total sensitive records. The Capital One breach in July alone exposed 99 percent of the sensitive records in the banking sector.

In 2019 the ITRC reported that hacking was the most used method of breaching data, with 577 data breaches resulting in 15.3 million records exposed. This form of breach includes intrusion methods like phishing, ransomware and malware, and skimming. Unauthorized access ranked second with 538 data breaches, but this method affected the highest number of records exposed by data breach type—142 million, or 86 percent of all sensitive records exposed in 2019. Employee error or negligence, improper exposure or lost data had the third highest number of breaches, 161, with 2.9 million records exposed.

In 2020 through April 10, the ITRC tracked 269 breaches that exposed 3.3 million records. The year to date total includes the Health Share of Oregon breach that exposed 654,400 records,

reported in February. It does not include the Marriott breach, announced March 31, that may have exposed the records of 5.2 million guests. The medical/health care sector was the most affected sector by number of records exposed, with 2.2 million records exposed, or 65 percent of all records exposed so far in 2020. The sector had 113 breaches, or 42 percent of all breaches to date. The business sector had about 666,600 records exposed so far in 2020, or 20 percent of all records exposed in 110 breaches that accounted for 41 percent of all 2020 breaches.

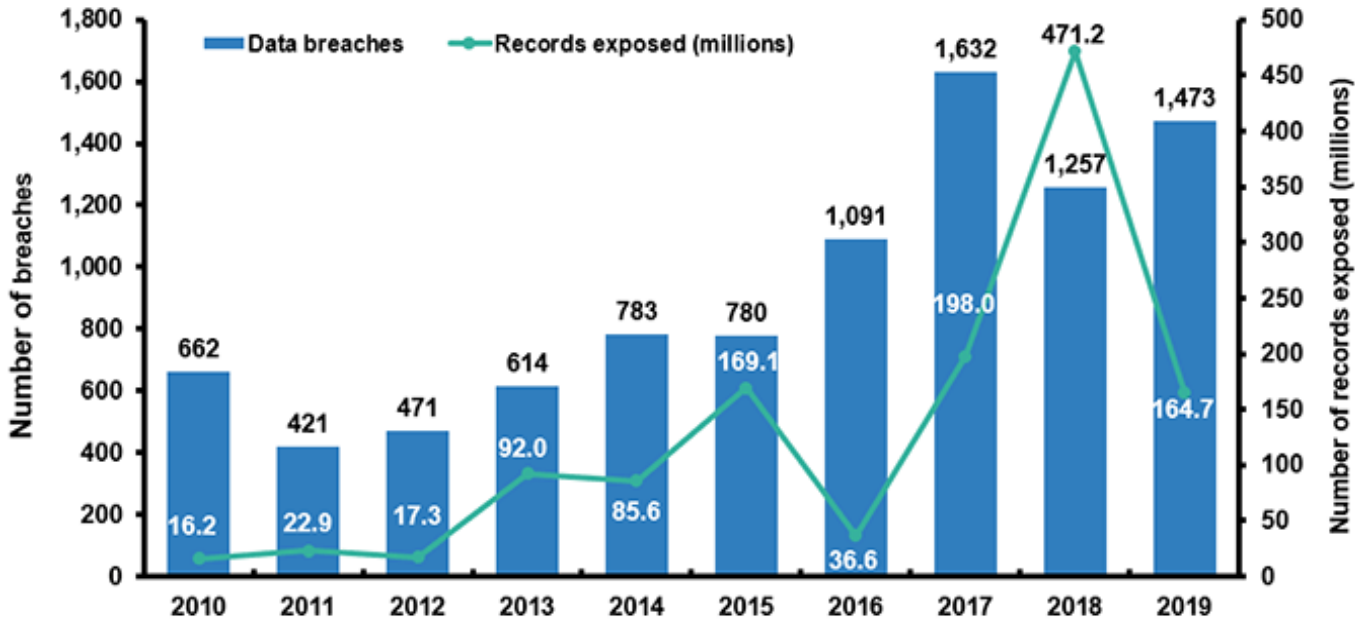
Despite conflicting analyses, the costs associated with cybercrime are increasing. McAfee and the Center for Strategic and International Studies (CSIS) estimated the likely annual cost to the global economy from cybercrime is $445 billion a year, with a range of between $375 billion and $575 billion. The average cost of a data breach globally was $13.0 million in 2018, up 12 percent from $11.7 million in 2017, according to a 2019 study from the Ponemon Institute and Accenture. Researchers polled 355 organizations located in 11 countries to determine what costs they faced after a cyberattack, such as the costs to detect, recover, investigate and manage the incident response. They also included the cost of activities that occur after the fact and efforts to reduce business interruption and loss of customers. In the United States, the average annual cost of cybercrime rose 29 percent in 2018, to $27.4 million, compared with $21.2 million in 2017. Globally, the banking industry had the highest average annual cost in 2018 —$18.4 million—up from $16.7 million in 2017, followed by utilities and software companies. By type of attack, malware incidents had the highest cost, at $2.6 million followed closely by web-based attacks at $2.3 million.

Cyber insurance evolved as a product in the United States in the mid- to late-1990s as insurers have had to expand coverage for a risk that is rapidly shifting in scope and nature. In 2018, 545 insurers reported writing cyber insurance, up from 505 in 2017, according to NAIC data sourced from S&P Global Market Intelligence. Direct premiums written totaled $2.0 billion in 2018, from companies that can report premiums for stand-alone and coverage provided as part of package policies, up from $1.86 billion in 2017.

According to the Insurance Information Institute (I.I.I.) and J.D. Power 2019 *Small Business Cyber Insurance and Security Spotlight Survey*[SM], 12 percent of businesses surveyed suffered one or more cyber incidents in the prior year, up from 10 percent in 2018. Nearly 71 percent said they are “very concerned” about cyber incidents, up from 58 percent in 2018, and 75 percent said they believe the risk of being victimized by a cyberattack is growing at an alarming rate–up from 70 percent in 2018. Among the 44 percent of respondents who said they do not currently have cyber insurance and the 21 percent who said they do not know whether they do, 64 percent said they do not plan to purchase a cyber insurance policy in the next 12 months. While this is down from 70 percent in 2018 and given small companies’ growing awareness and concerns about cyberrisk, insurers and agents and brokers might be able to increase their overall support of this market by addressing the issues of affordability and coverage limitations that seem to be an obstacle to purchasing.

Number Of Data Breaches And Records Exposed, 2010-2019

(1)



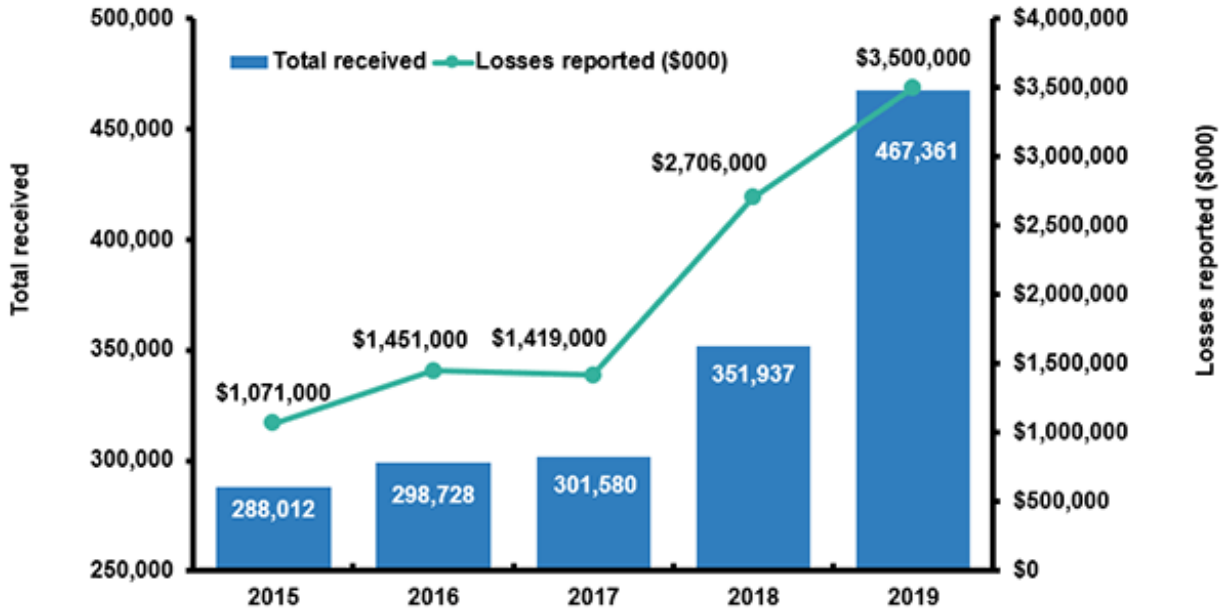
(1) As of January 7, 2019.

Source: Identity Theft Resource Center, *2019 End of Year Data Breach Report*.

View Archived Graphs

The IC3 says that 2019 complaints and dollar losses were the highest since the center began tracking cybercrime statistics in 2000. In 2019 the IC3 received and processed 467,361 complaints and losses to individuals and businesses rose to $3.5 billion from 2018. Both the number of complaints and the losses reported rose from 2018 by about 30 percent. In terms of dollar losses, business email compromise caused the most losses, with about $1.7 billion in losses, followed by confidence fraud or romance complaints, with almost half a billion dollars in losses. Business email compromise typically involves a criminal mimicking a legitimate email address, for example, an employee will receive a message that appears to be from an executive within their company requesting a payment or wire transfer that funnels money directly to a criminal. About 24,000 people were victims of email account scams. Confidence fraud occurs when a criminal deceives a victim into believing they have a trust relationship and the victim is persuaded to send money or personal and financial information. In 2019 about 20,000 people reported confidence scams.

Cybercrime Complaints, 2015-2019 (1)



(1) Based on complaints submitted to the Internet Crime Complaint Center.

Source: Internet Crime Complaint Center.

View Archived Graphs

Top 10 States By Number Of Cybercrime Victims, 2019 (1)

Rank	State	Number
1	California	50,132
2	Florida	27,178
3	Texas	27,178
4	New York	21,371
5	Washington	13,095
6	Maryland	11,709
7	Virginia	11,674
8	Pennsylvania	10,914
9	Illinois	10,337
10	Indiana	9,746

(1) Based on the total number of complaints submitted to the Internet Crime Complaint Center via its website from each state where the complainant provided state information.

Source: Internet Crime Complaint Center.

View Archived Tables

Top 10 Writers Of Cybersecurity Insurance By Direct Premiums Written, 2019 (1)

($000)

Rank	Group/company	Direct premiums written (2)	of total
1	Chubb Ltd.	$356,856	15.9%
2	AXA	229,680	10.2
3	American International Group (AIG)	225,758	10.1
4	Travelers Companies Inc.	178,526	7.9
5	Beazley Plc.	150,943	6.7
6	AXIS Capital Holdings Ltd.	97,305	4.3
7	CNA Financial Corp.	94,722	4.2
8	BCS Insurance Co.	76,062	3.4
9	Liberty Mutual	68,377	3.0
10	Fairfax Financial Holdings	65,101	2.9

(1) Includes stand-alone policies and the cybersecurity portion of package policies. Does not include premiums from companies that cannot report premiums for cybersecurity coverage provided as part of package policies.
(2) Before reinsurance transactions.
(3) Includes only companies that can report premiums for stand-alone cybersecurity coverage and coverage provided as part of package policies.

Source: NAIC data, sourced from S&P Global Market Intelligence, Insurance Information Institute.

View Archived Tables

Additional resources

Federal Trade Commission

Internet Crime Complaint Center

Back to top