Introduction

Data collection

Data analysis

Conclusion

Appendix

Computer Crime Statistics—2019

Dr. Michael A. Crain/ Florida Atlantic University/ Center for Forensic Accounting

I am grateful to Maria Gutierrez for research assistance.

Introduction

This research report by Florida Atlantic University's Center for Forensic Accounting is the result of compiling FBI internet crime statistics from 2015 through 2019. It shows trends in internet crimes across those U.S. states with the highest reported victim losses or number of victims. This information can be used for public awareness and by government for law enforcement and policy making.

The U.S. Federal Bureau of Investigation (FBI) created the Internet Crime Complaint Center (IC3) in 2000 to receive internet crime complaints from the public. Once someone files a complaint, FBI classifies it into a crime type so that data can be sorted and disseminated to law enforcement agencies and the public. Every year, FBI's IC3 publishes general data with victim numbers and loss amounts for each type of internet crime. Separately, IC3 publishes annual data for each of the U.S. states and territories.

Over the years, FBI data show some internet crimes persist and others have disappeared. Yet, new and more sophisticated types of crimes now prevail. Our report shows online crime trends over the last five years for states having higher internet crime activity with a focus on the trend from 2018 to 2019. The states selected for our 2019 report are: California, Florida, New York, Ohio, Texas, and Washington. We have identified these top states as having the largest victim monetary losses or number of victims in 2019. Ohio and Washington are new to the 2019 report while North Carolina and Virginia in the 2018 report dropped out. We also identified ten top internet crimes with high victim losses. We added three new crimes to the 2019 report: Extortion, Government Impersonation, and Spoofing. These online crimes had large increases in victim losses.

Business Email Compromise/Email Account Compromise (BEC/EAC) is once more the top online crime with reported victim losses in 2019 of $1.8 billion.[1] BEC/EAC explained about 30% to 90% of all victim losses during 2019 across the top states. This scam accounted for 92% of all online victim

losses in Ohio, 57% in New York, 56% in Texas, 47% in Washington, 46% in California, and 33% in Florida.

The second top internet crime is Confidence Fraud/Romance where losses and number of victims continued to increase in 2019 with $475 million in victim losses.[2] In 2019 the ratio of Confidence Fraud/Romance victim losses to all online crime losses was 26% in Washington, 19% in California, 15% in Florida and Texas, 10% in New York, and 2% in Ohio. Ohio was the only top state with a decline in the ratio in 2019. The ratio fell from 9% in 2018 to 2% in 2019.

Spoofing became the third highest online crime in 2019 with victim losses of $300 million.[3] Online Investment fraud was fourth highest followed by Real Estate/ Rental.

In Florida, Identity Theft was the third highest online crime for victim losses after BEC/EAC and Confidence Fraud/Romance. Online Investment fraud and Real Estate/Rental also continued to be predominant crimes in Florida during 2019.

On the other hand, Corporate Data Breach victim losses declined in all the top states during 2019 especially in Florida. Online Credit Card Fraud declined in victim losses in five of six the top states but continues to be a significant online crime.

Data collection

The FBI, through its Internet Crime Complaint Center IC3, has been receiving internet related fraud complaints from victims since 2000. The IC3's website www.IC3.gov is a website for victims to file suspected internet related crimes. Filing a complaint requires the victim or complainant to provide detailed information on the internet crime. Detailed information requested when filling a complaint includes:[4]

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on the person was victimized
- Email header(s)
- Any other relevant information believed necessary to support the complaint

After the information in the complaint is gathered, it gets classified by crime type and analyzed to identify present and future crime trends. Intelligence reports are prepared with these data and are disseminated to law enforcement.

It is important to bear in mind that the FBI reports only include reported internet crimes, which are only a portion of the real number of internet crimes committed every year in the United States.

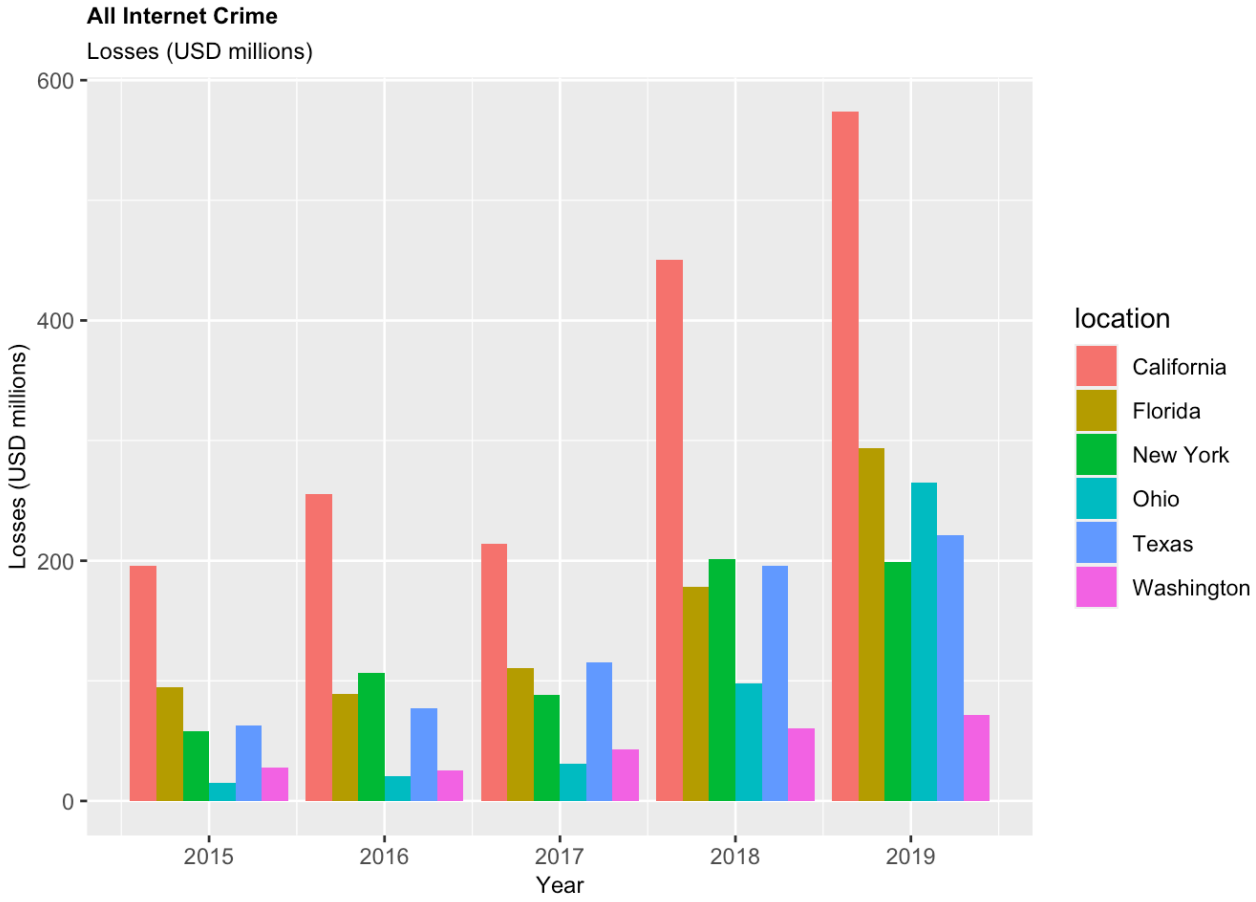
Data analysis

All Internet Crime

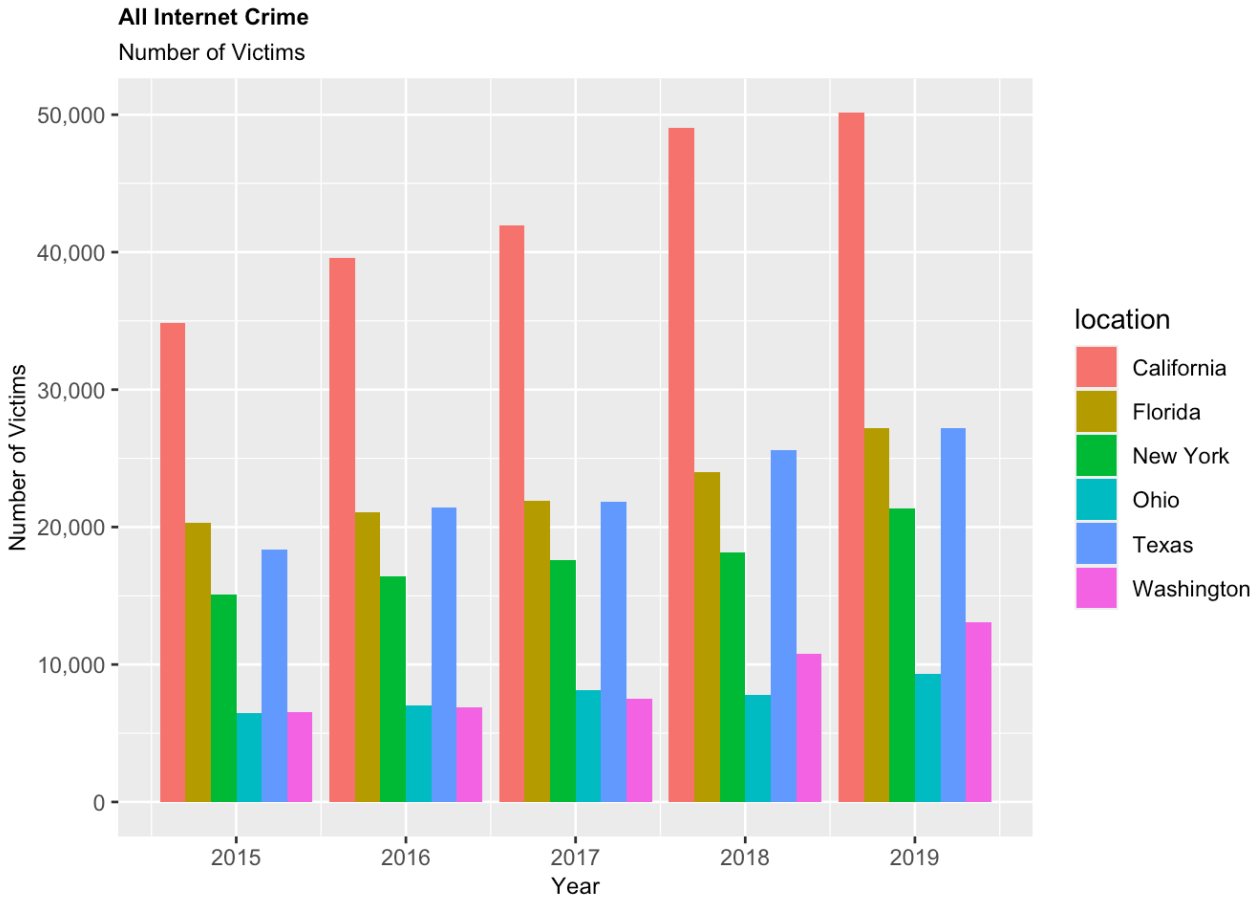
This report covers five years from 2015 to 2019 as these years contain comparable information for crime types in FBI data. The agency used different data formats in earlier years. Our report herein shows the reported internet crime in absolute numbers of victim losses and numbers of victims, and relative loss rates and victim rates accounting for population. Loss rate is defined as the amount of

total monetary victim losses divided by the population in millions. Similarly, victim rate is defined as the total number of victims divided by the population in millions. Further, our report uses internet crime and internet fraud interchangeably.

Six top states were selected for the analysis based on the highest victim losses or number of victims in 2019. The six top states are: California, Florida, New York, Ohio, Texas, and Washington.

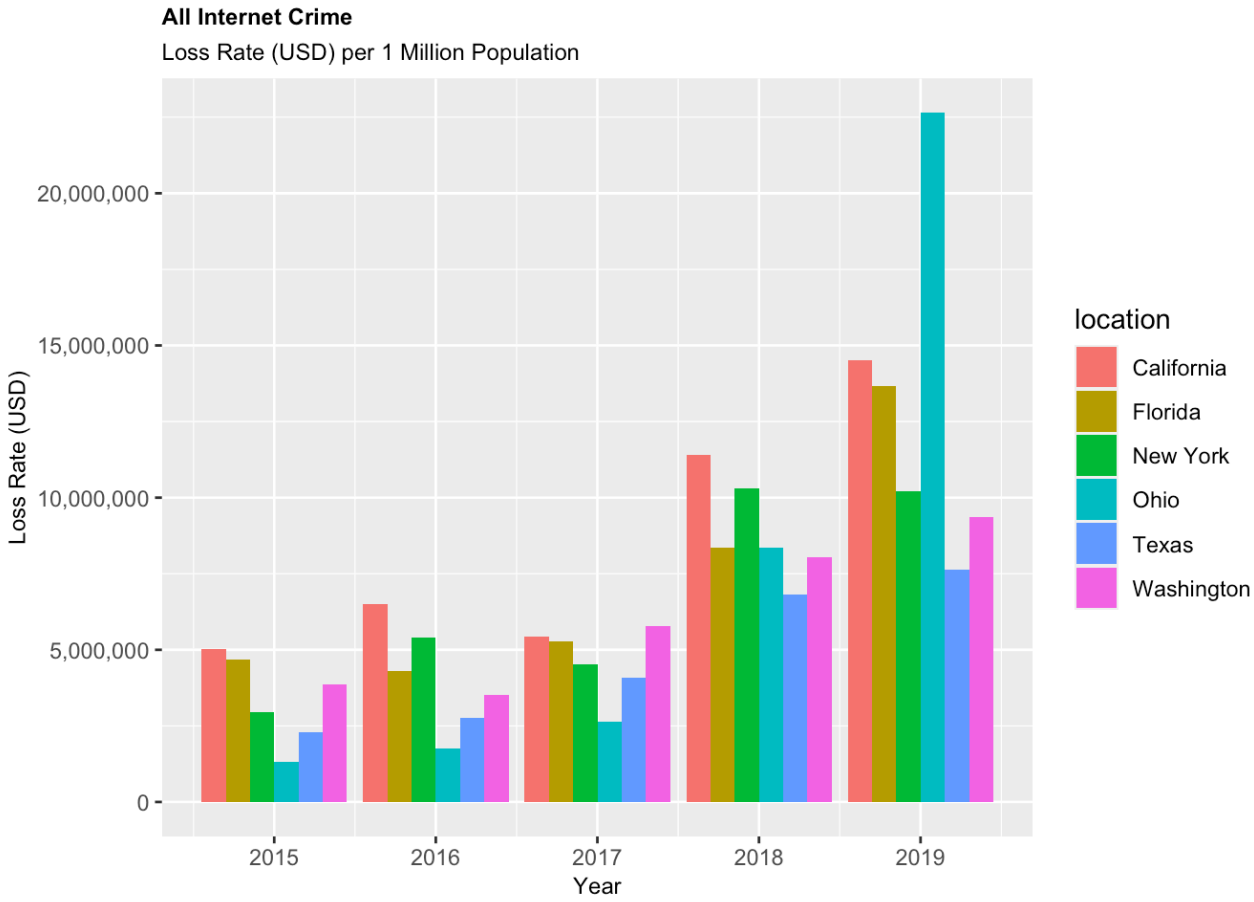


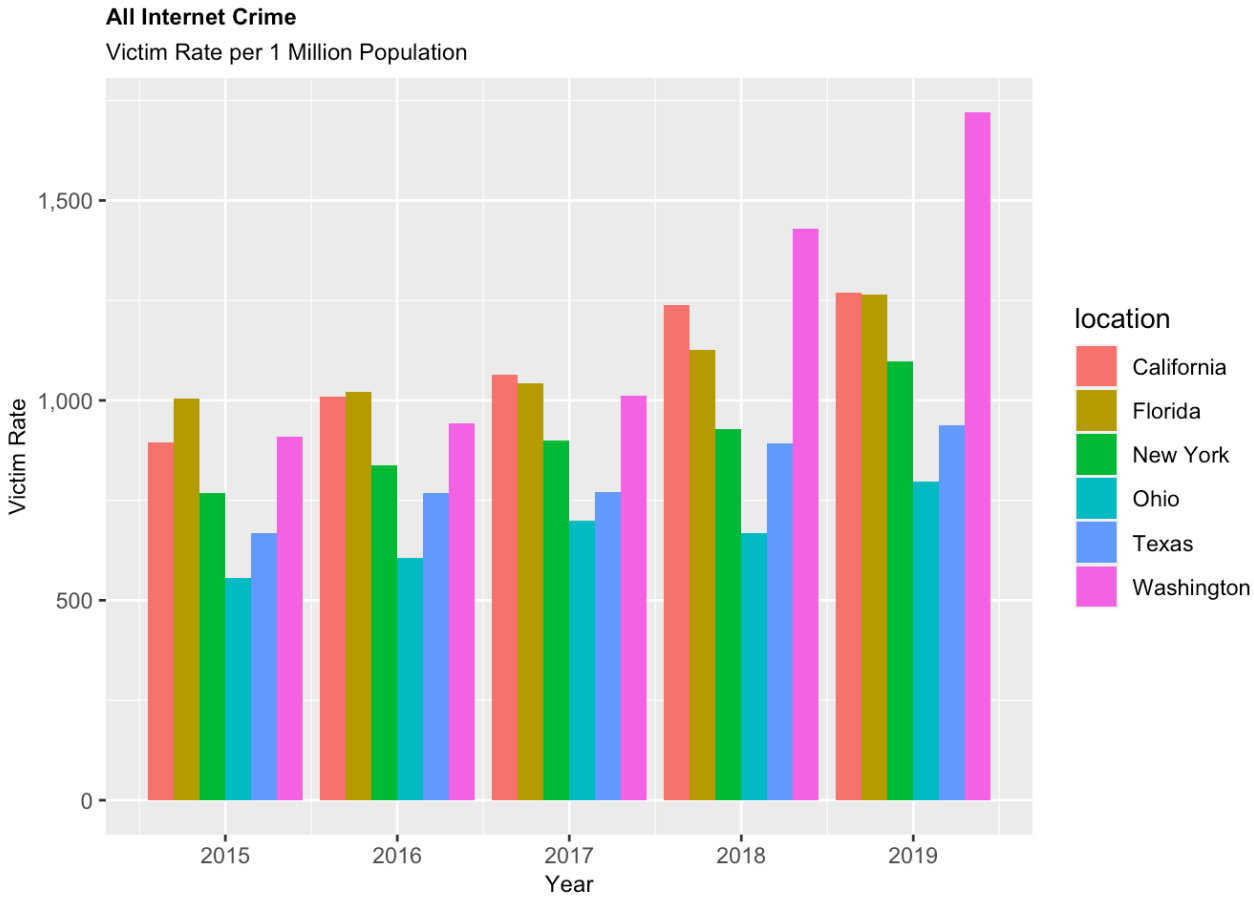
California continued to be the top state with highest victim losses and largest number of victims for all years from 2015 through 2019. California had an increase of 27% in victim losses, $123 million, from $450.5 million in 2018 to $573.6 million in 2019. In contrast, the number of victims in California only increased 2%.



While in absolute numbers California had the largest victim losses and number of victims, Ohio had the largest loss rate in 2019 of $22.6 million per one million in population, growing significantly from $8.4 million in 2018. From 2015 through 2017, Ohio ranked sixth in loss rates among the six top states. Its loss rate jumped in 2018 and again in 2019. Florida had the third highest loss rate in 2019 of $13.7 million per one million in population. Its loss rate had jumped from $8.4 million in 2018, a 63% increase for 2019.

Washington had the highest number of victims adjusted for population in 2019. Its victim rate in 2019 was 1,720 per one million in population while California and Florida had the next highest victim rates of 1,269 and 1,265, respectively.

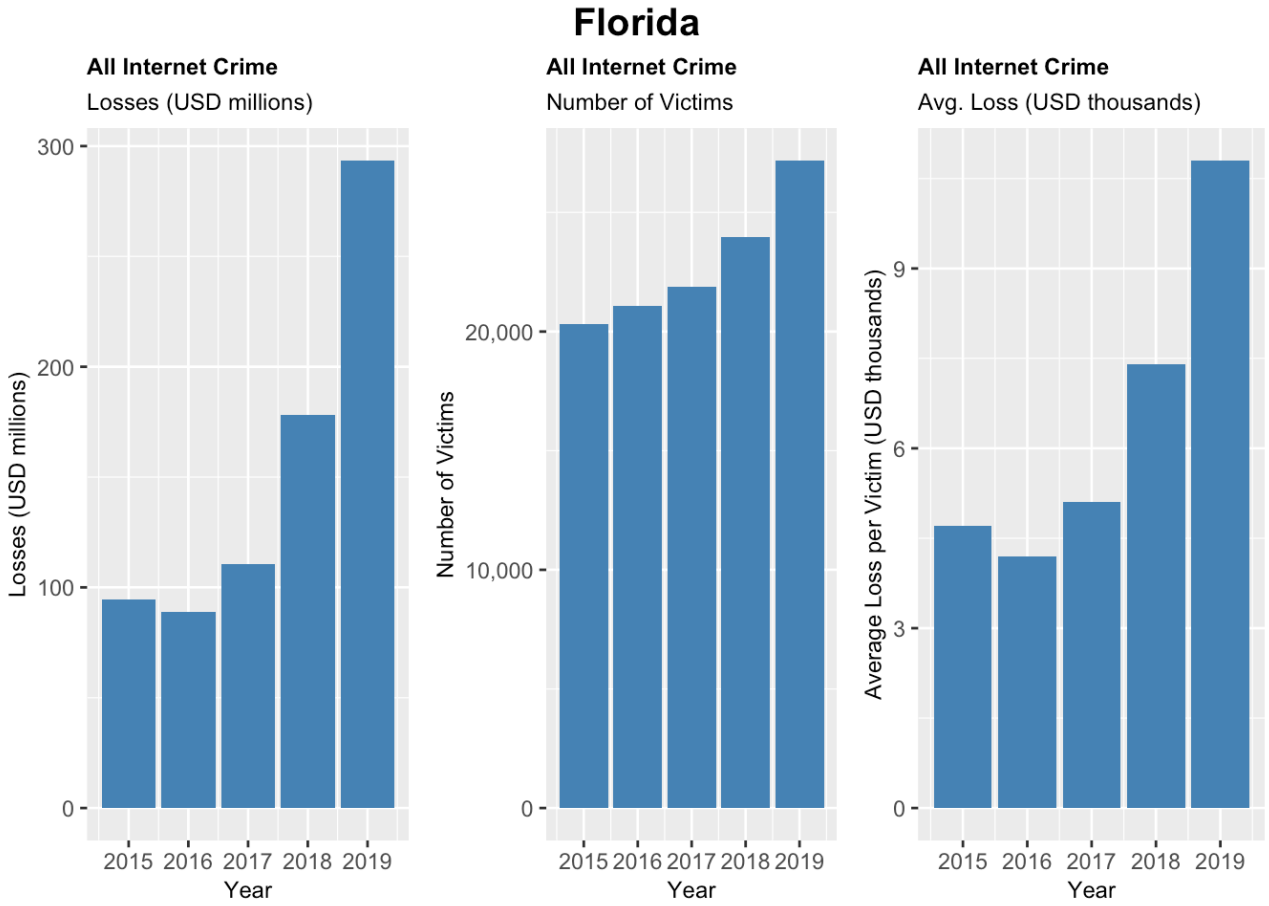

All Internet Crime
Loss Rate (USD) per 1 Million Population
Loss Rate (USD)
20,000,000
15,000,000
10,000,000
5,000,000
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


All Internet Crime
Victim Rate per 1 Million Population
Victim Rate
1,500
1,000
500
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington

Going back to absolute numbers, in 2018 Florida was behind California, New York, and Texas in victim losses, but in 2019 Florida became the second highest state in losses with $293.4 million. From 2018 through 2019, Florida's victim losses increased 65%, the largest percentage increase among the six top states, growing from $178.1 million to $293.4 million.

Although Florida and Texas had similar numbers of victims in 2019, Florida had a 13% increase and Texas increased 6% from 2018.

In Florida, 2019 was the year of the largest annual increase in both victim losses and number of victims over the past five years. The average loss per victim in Florida has grown over the past five years from $4,700 in 2015 to $10,800 in 2019. The average victim loss jumped from $7,400 in 2018 to $10,800 in 2019, a 46% increase.



Over the last five years, victim losses in the six top states have increased more than 150% with Ohio having the highest growth of 1,600%. Washington had the highest growth rate in number of victims of 100%, while Florida had the lowest of 34%.

Top types of internet crimes

Business Email Compromise/Email Account Compromise as well as Confidence Fraud/Romance continued to be top internet crimes in 2019. In addition, crimes such as Extortion, Government Impersonation, and Spoofing became prominent in 2019 for their increase in victim losses and victim numbers.

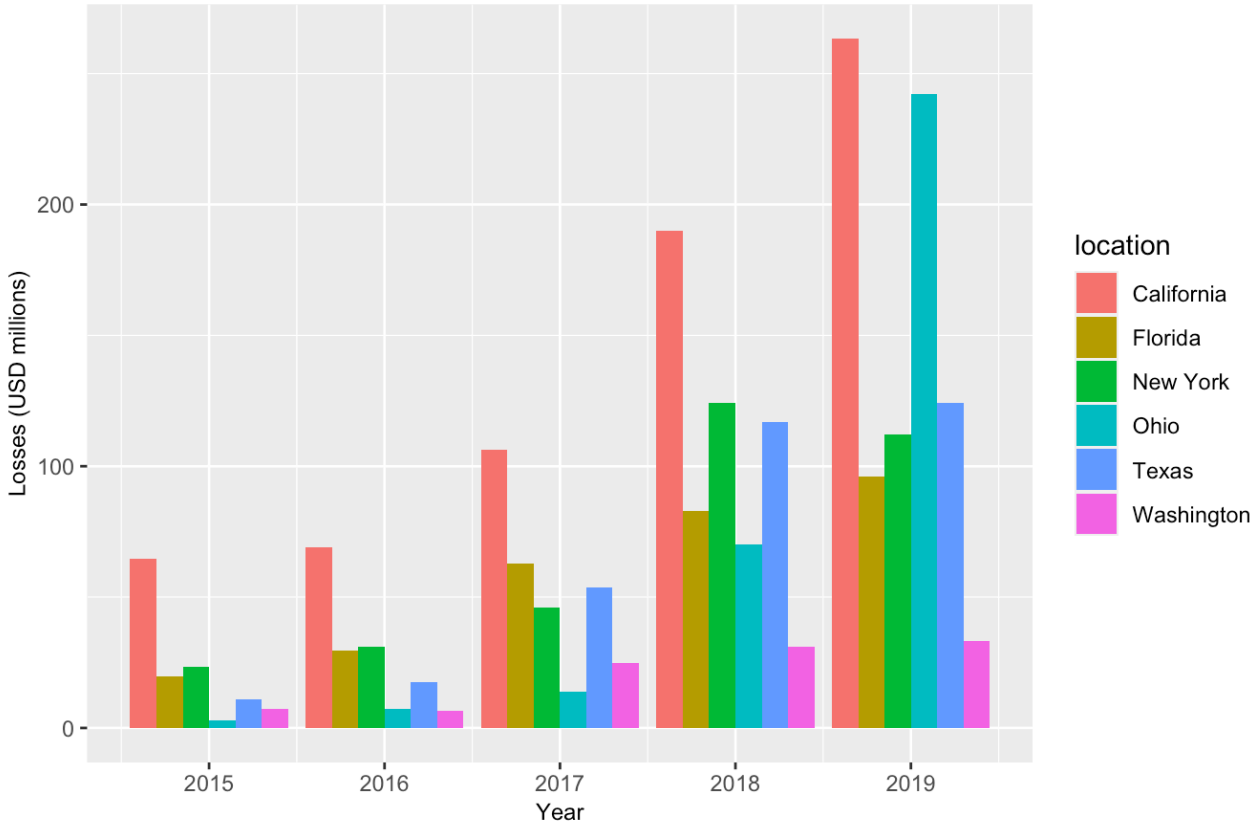
Business email compromise/ Email account compromise

Business Email Compromise/Email Account Compromise (BEC/EAC) takes place when business or personal email accounts are hacked or spoofed with the purpose of diverting and requesting electronic wire transfers to fraudulent money accounts. This scheme perhaps started with the hacking of CEO emails accounts and requesting fraudulent wire transfers. Throughout the years it has expanded to hacking and spoofing personal emails accounts and obtaining sensitive information to divert funds from other kinds of victims including lawyers, vendors, and the real estate sector. In addition, the FBI's IC3 has received increasing complaints where victims receive seemingly credible emails or text messages from their bosses or others in a position of trust requesting their victims buy gift cards.

According to the FBI report, BEC/EAC was the top online crime in 2019 with reported losses of $1.8 Billion[5]. This scheme has grown at varying rates in five of the six top states while declining 10% in New York. From 2018 through 2019, Ohio victim losses increased by 245%, but only 6% in Texas.

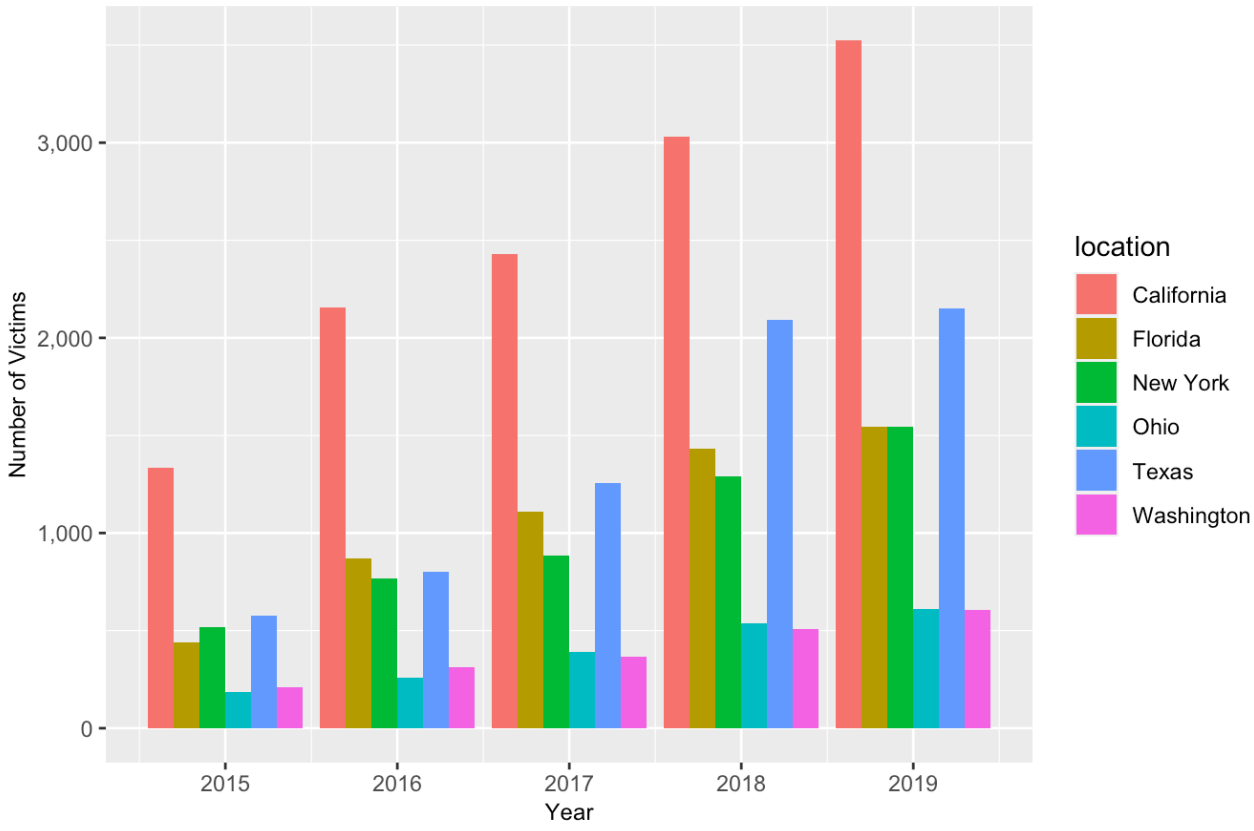
Business Email Compromise/Email Account Compromise

Losses (USD millions)



Business Email Compromise/Email Account Compromise

Number of Victims



Even though California had the highest victim losses to BEC/EAC of $263.2 million in 2019, Ohio had nearly as much with $242.1 million. Additionally, Ohio's victim losses jumped in 2019 by 245% over the previous year. BEC/EAC accounted for 92% of total victim losses to internet crime in Ohio during 2019. Ohio's BEC/EAC losses has increased rapidly since 2015 when this scheme represented 18% of its total internet crime victim losses, jumping to 46% in 2017, 72% in 2018, and, as stated, 92% in 2019.

In 2019, California had the highest number of victims reaching 3,523 victims, up 16% from 2018. Ohio had the second highest number of victims, up 14% from 2018 to 613.

In Florida, victim losses increased 16% from $83.0 million in 2018 to $96.2 million in 2019. Victim numbers, like in some of the other top states, increased at a much slower pace than victim losses, 8%, from 1,433 in 2018 to 1,546 in 2019.

In contrast to the other top states where victim losses grew faster than number of victims, Washington victim losses grew 8%, from $31.0 million in 2018 to $33.3 million in 2019 while victims numbers grew 20% from 507 to 606.

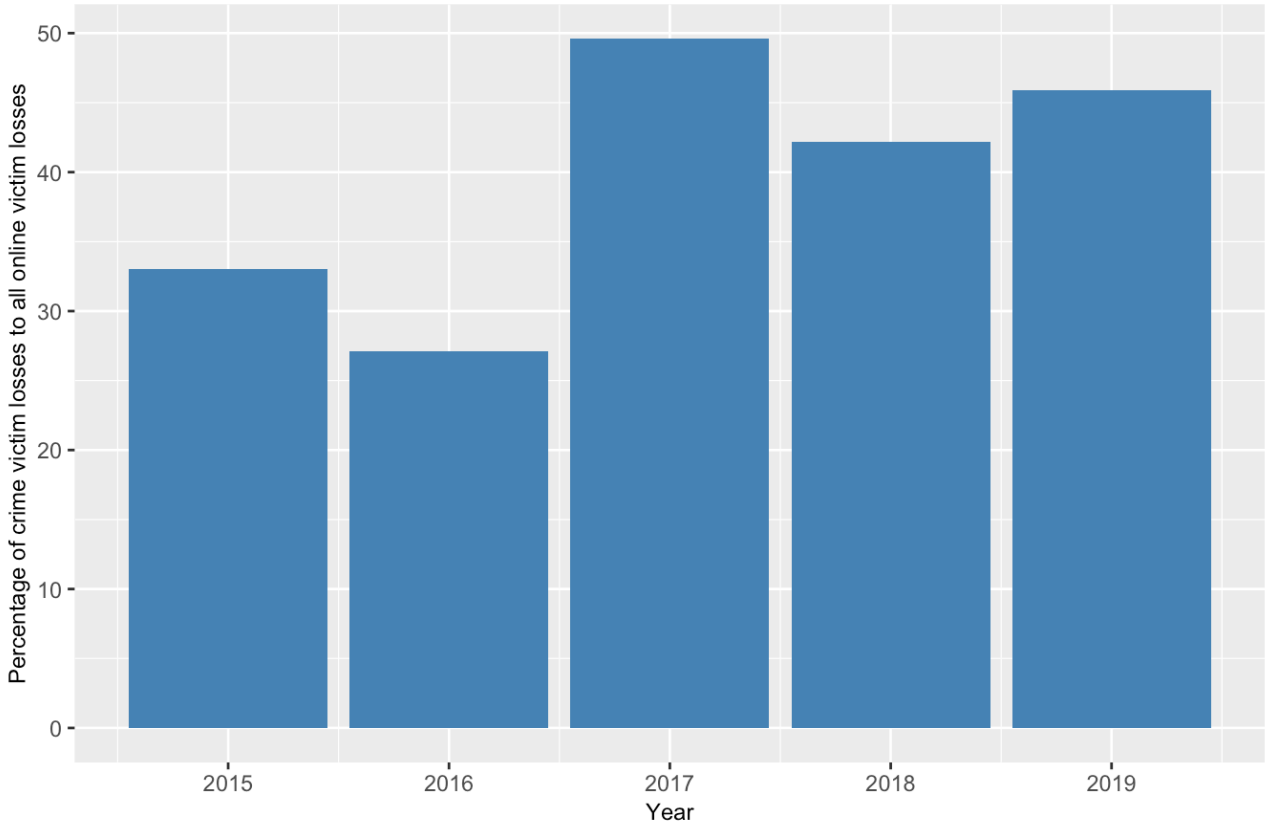
In Texas, growth in both victim losses and the number of victims were the lowest among the top states. Texas victim losses increased 6%, from $117.0 million in 2018 to $124.2 million in 2019 and victim numbers increased 3%.

New York, on the other hand, was the only top state to experience a decline in BEC/EAC victim losses from 2018 through 2019 of 10%, from $124.0 million to $112.2 million. Although losses in New York went down, the number of victims increased 20%.

In terms of the ratio of victim losses from BEC/EAC to all internet crime losses during 2019, Ohio had the highest ratio of 92%. In New York and Texas, BEC/EAC accounted for 57% and 56%, respectively, while Washington was 47%, and California 46%. Florida, on the other hand, had the lowest 2019 ratio among the top states of 33%.

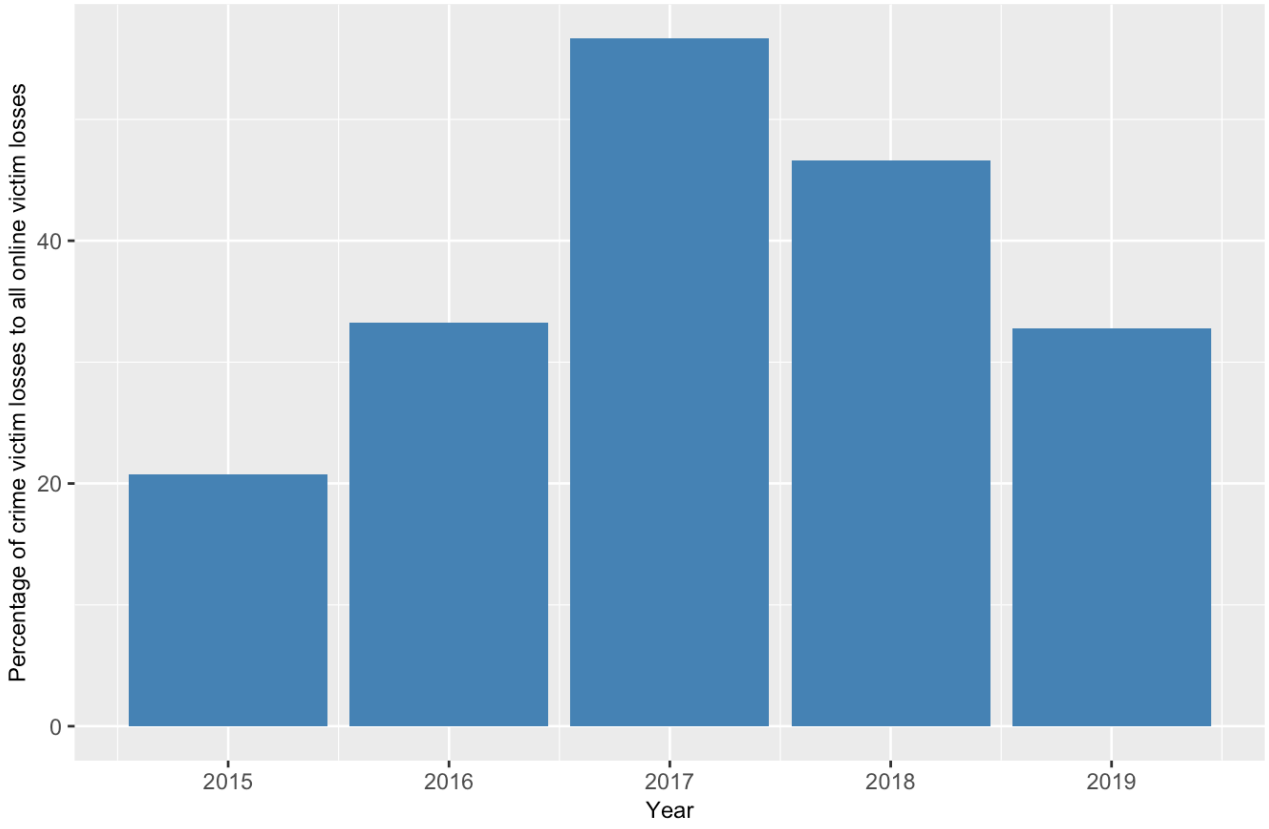
California --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



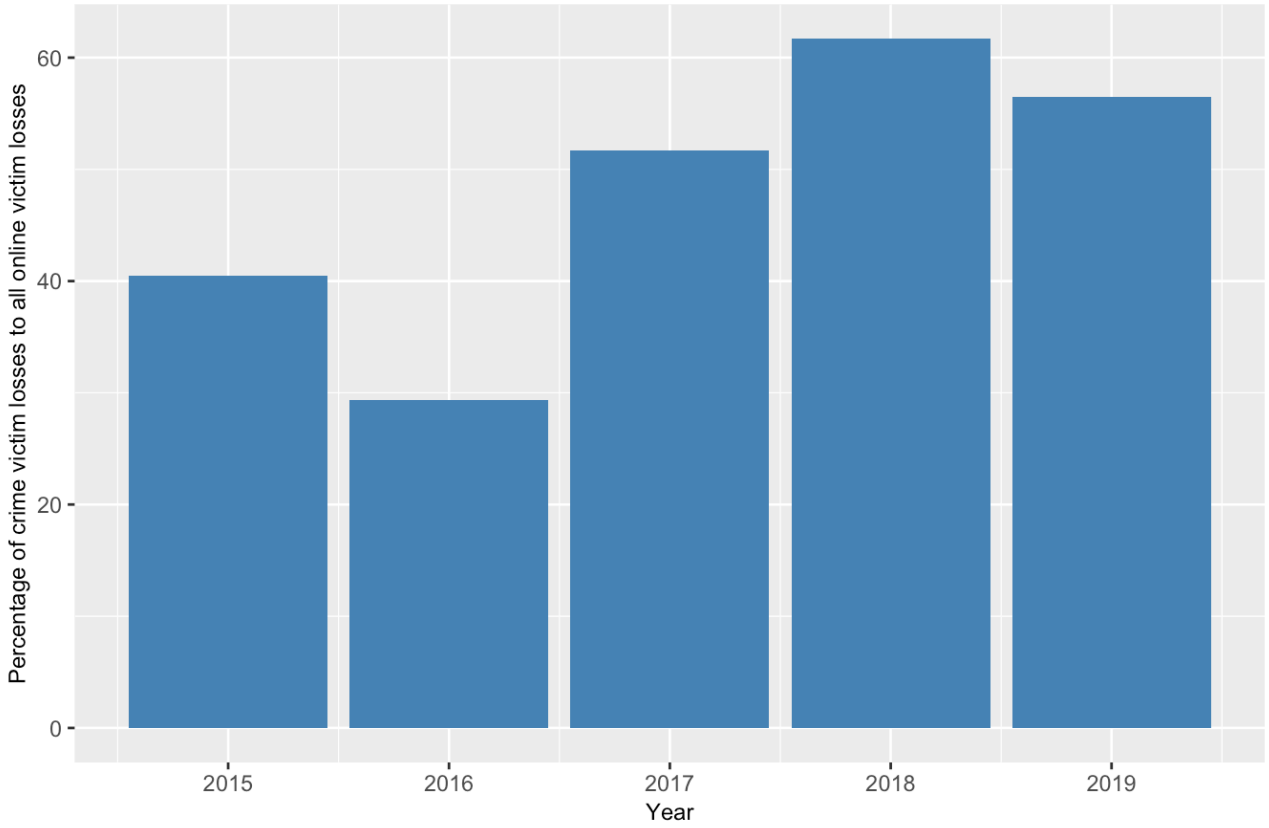
Florida --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



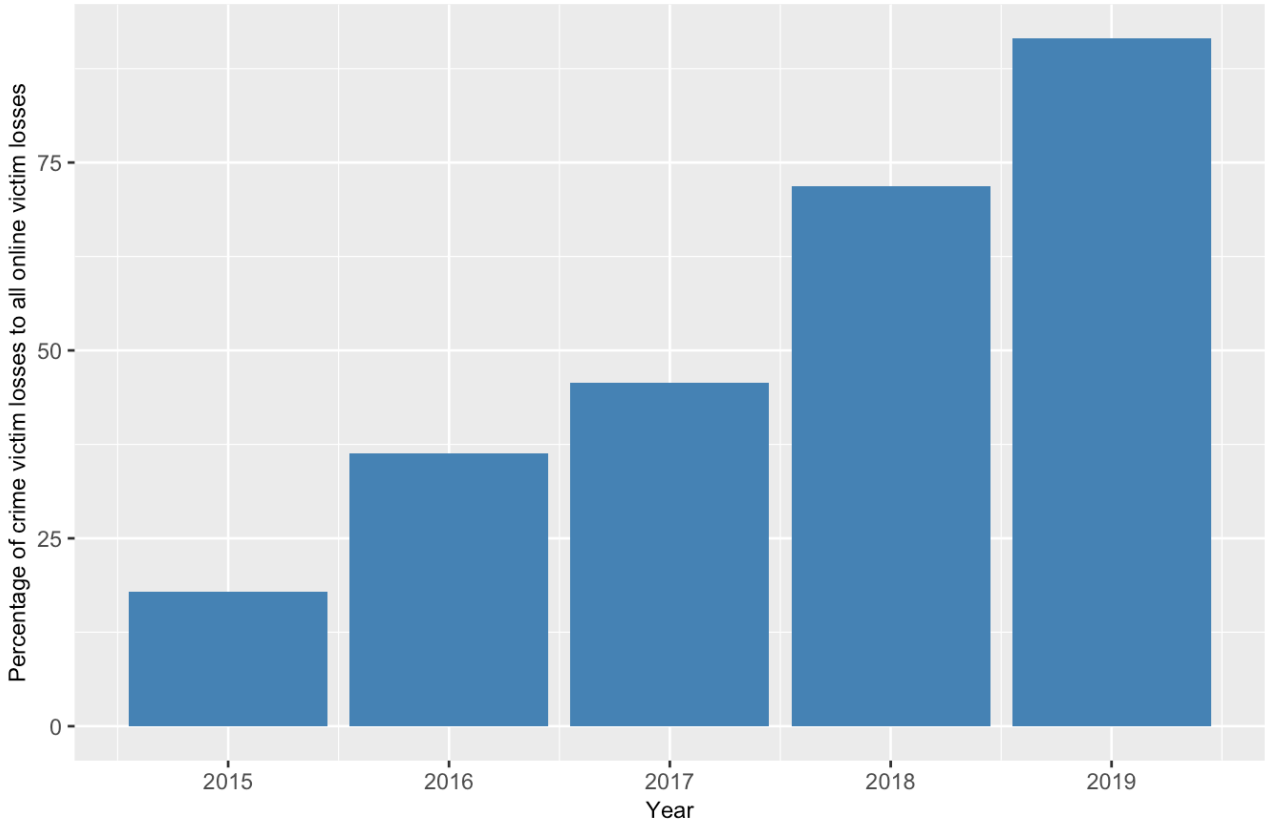
New York --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



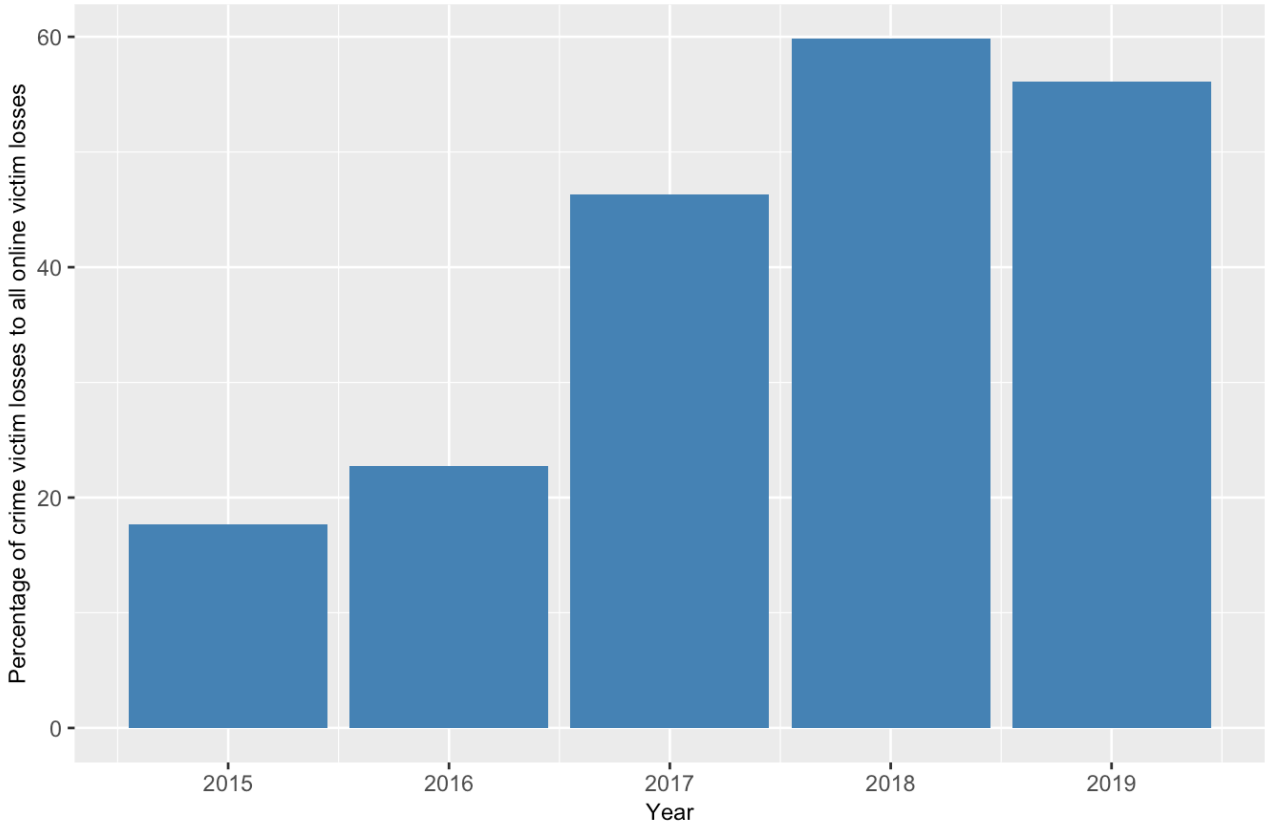
Ohio --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



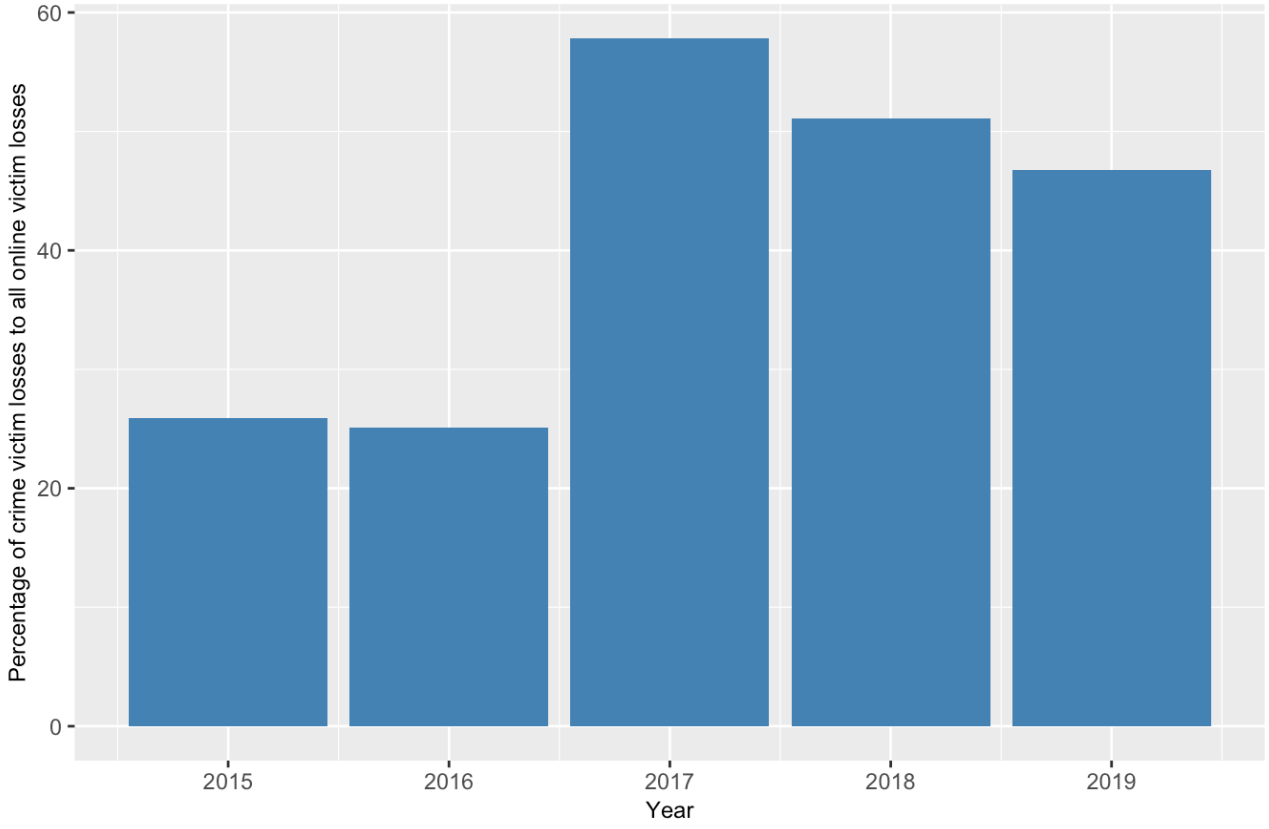
Texas --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



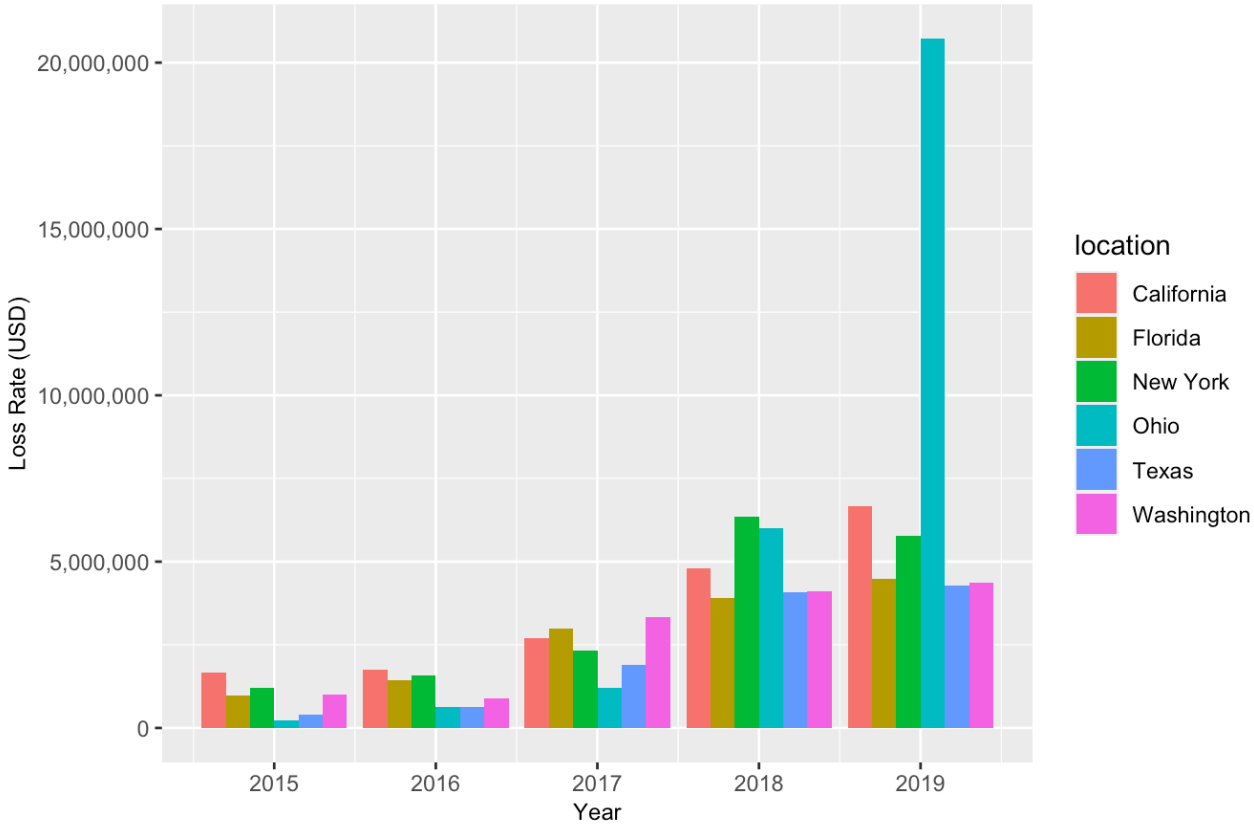
Washington --- Business Email Compromise/Email Account Compromise

Percentage of victim losses from this crime to all online victim losses



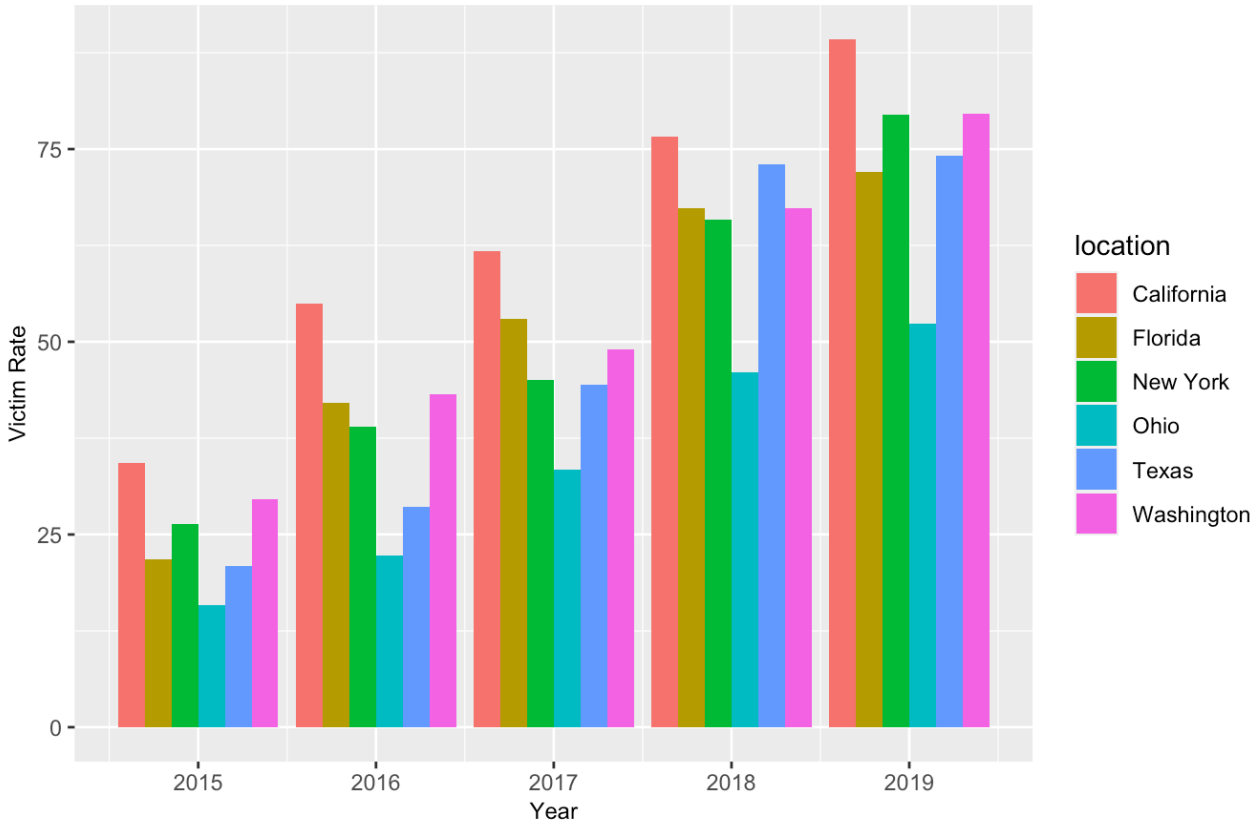
Business Email Compromise/Email Account Compromise

Loss Rate (USD) per 1 Million Population



Business Email Compromise/Email Account Compromise

Victim Rate per 1 Million Population



In relative terms, Ohio experienced victim losses of $20.7 million per one million in population in 2019 from BEC/EAC scams while victims in California, second highest, lost $6.7 million, and New York, third highest, $5.8 million.

Meanwhile, in Texas and Washington, the states with lowest loss rates among the top states, the 2019 loss rates were $4.3 million and $4.4 million per one million in population, respectively.

Victim rates in 2019 showed a different story from loss rates, where California had the highest rate of 89 victims per one million in population. Washington and New York followed with 80 and 79, respectively.

Texas and Florida were fourth and fifth highest with victim rates of 74 and 72, respectively, and Ohio, last with 52 victims per one million in population.

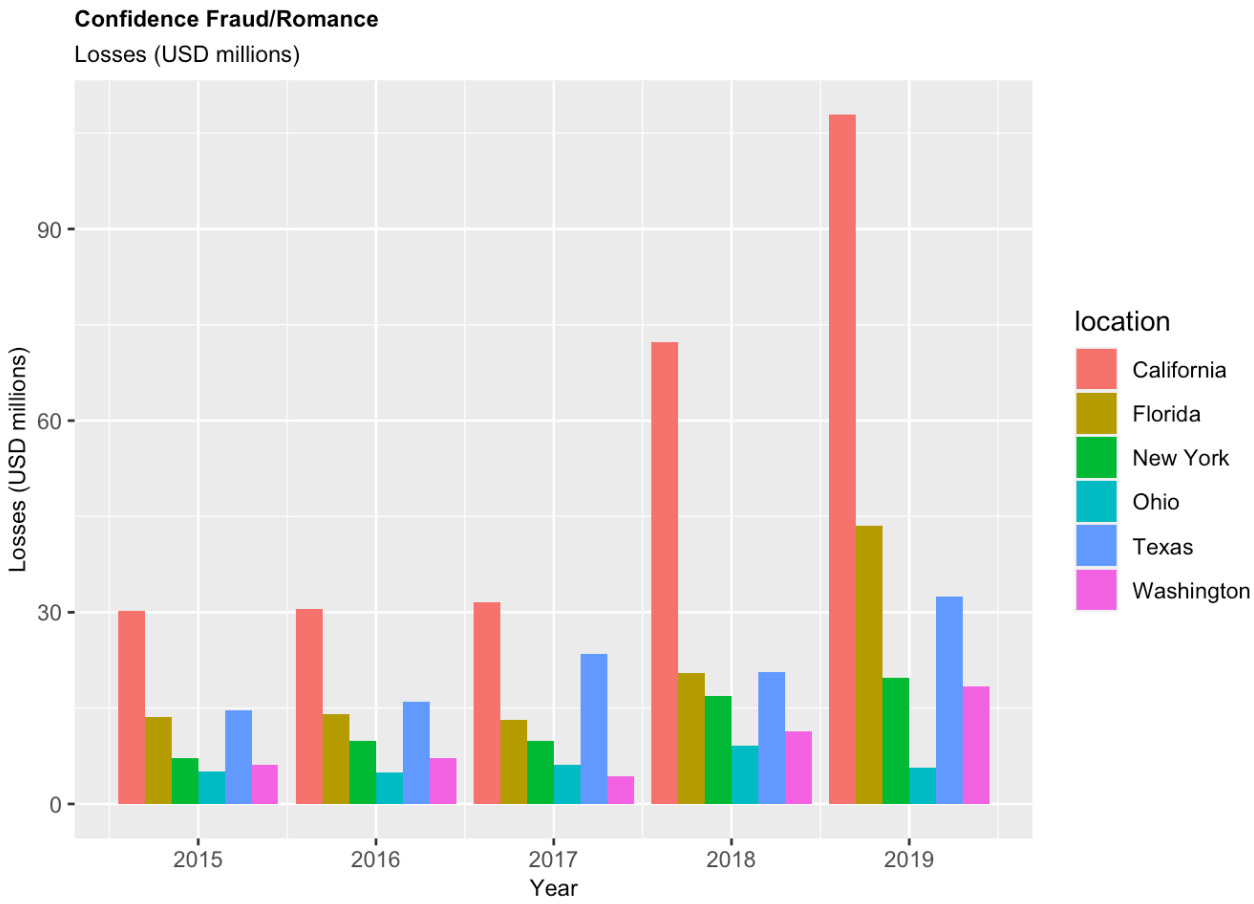
In sum, 2019 losses from BEC/EAC accounted for more than 45% of all online losses in California, New York, Ohio, and Washington. In Ohio, nearly all victim losses, 92%, were to BEC/EAC. In contrast, Florida's BEC/EAC portion was below 35%.

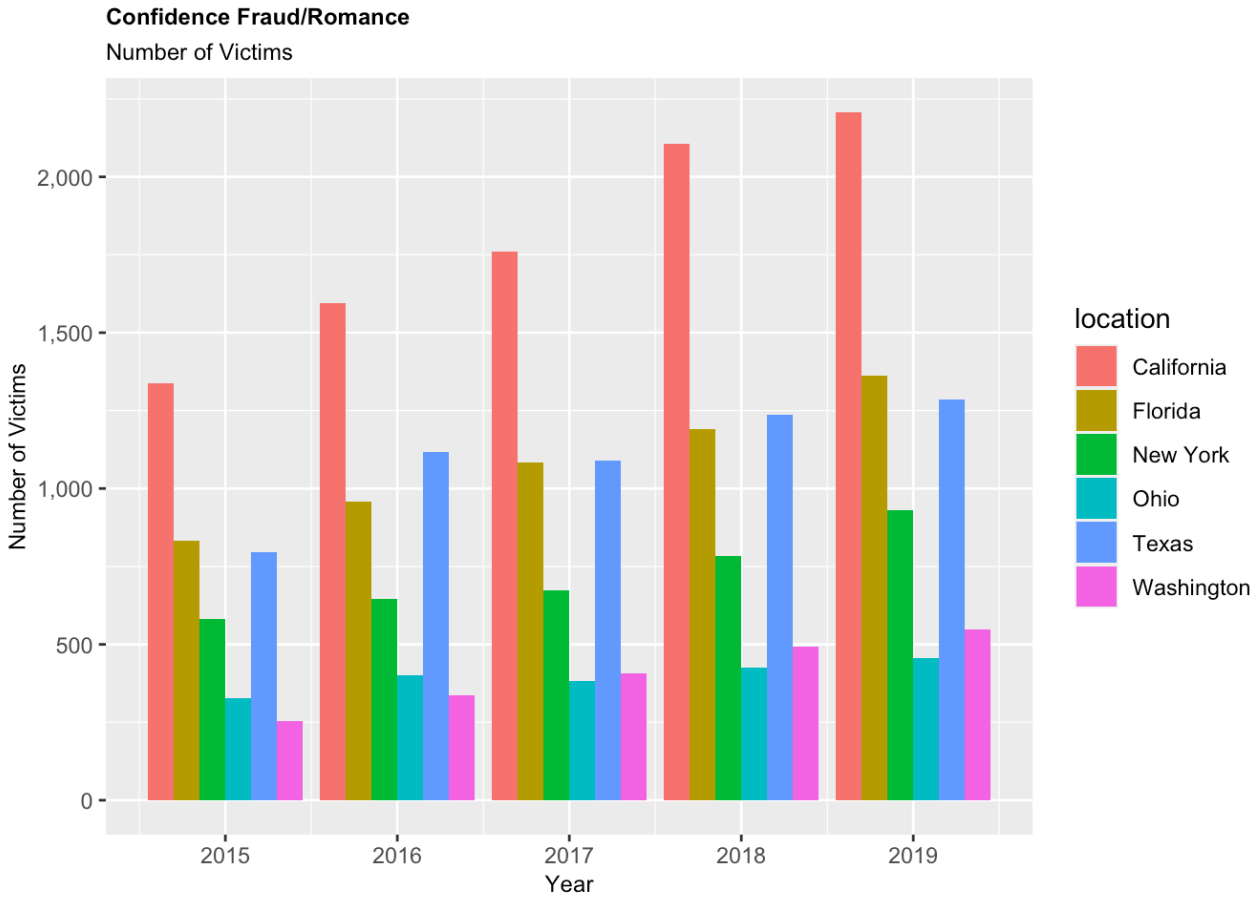
Confidence Fraud/Romance

Another growing internet scam is Confidence Fraud/Romance. This scheme occurs when an online fraudster pretends to be in a friendly, romantic, or family relation to win the trust of the victim to obtain money, finances, or other valuable possession. Variations of this crime include romance/dating fraud and grandparent fraud. Like BEC/EAC, Confidence Fraud/Romance has become more frequent as the victim losses and number of victims have been increasing over the past five years. In 2019, Confidence Fraud/Romance scams had the second highest victim losses in the top states after BEC/EAC.

From the 2019 population-adjusted victim losses, this measure also shows this crime is the second most common online crime after BEC/EAC. In 2019, Confidence Fraud/Romance victim losses in Washington were 26% of all online losses, followed by California with 19%, Florida and Texas with 15%, and New York with 10%. Ohio was the only state among the six top states where losses to Confidence Fraud/Romance fraud decreased in relation to its total losses in 2019.

During 2019, five of the six top states experienced increases in victim losses from this scam with Washington and Texas having the highest growth, 62% and 57%, respectively, followed by California with 49%. Florida and Texas with 21% and 17% growth, respectively. Ohio experienced a decline in victim losses of 37%.


Confidence Fraud/Romance
Losses (USD millions)
Losses (USD millions)
90
60
30
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


Confidence Fraud/Romance
Number of Victims
Number of Victims
2,000
1,500
1,000
500
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington

In absolute numbers, California had both highest victim losses and highest number of victims in 2019 increasing from $72.4 million in losses during 2018 to $107.9 million, and from 2,105 in 2018 to 2,206 victims. California's victim losses increased rapidly during 2019 while the growth in number of victims was slower. In contrast, New York's victim losses grew more slowly at 17% from $16.9 million in 2018 to $19.7 million in 2019.

Florida ranked second in the amount of victim losses in 2019 among the top states from this scam after California. Losses increased 112% from $20.5 million in 2018 to $43.5 million in 2019. In addition, the number of Florida victims increased 14% from 1,191 to 1,363.

In Texas and Washington, victim losses grew faster than in the other top states during 2019. In Texas, losses grew from $20.6 million in 2018 to $32.4 million in 2019, and in Washington from $11.4 million to $33.3 million. Further, the number of victims grew 4.0% in Texas and 11.2% in Washington during 2019.

In terms of loss rates, California had the highest rate among the top states in 2019. Its loss rate was $2.7 million per one million in population, up from $1.8 million in 2018. California has had a large rise in its victim loss rate each year since 2017.

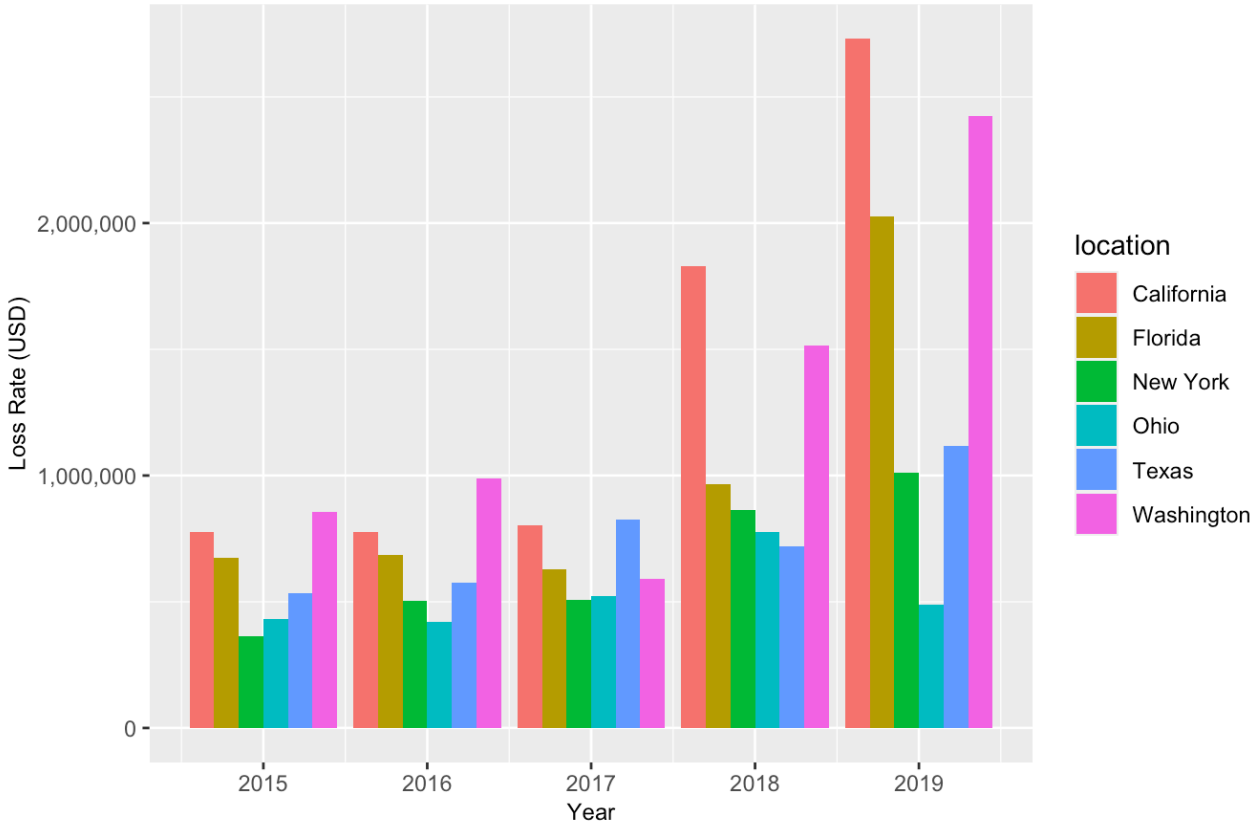
Washington follows California closely with a loss rate of $2.4 million per one million in population during 2019. In addition, Washington also had the highest victim rate among the top states, 72 victims per one million in population.

In 2019, Florida had the third highest loss rate of $2.0 million per one million in population, and the second highest victim rate of 63.5 victims per one million in population. New York and Texas had loss rates of $1.0 million and $1.1 million and victim rates of 48 and 44, respectively, in 2019.

Ohio had the lowest incidence of Confidence Fraud/Romance among the top states. In 2019, it had a loss rate of $490,000 per one million in population, and a victim rate of 39 per million.

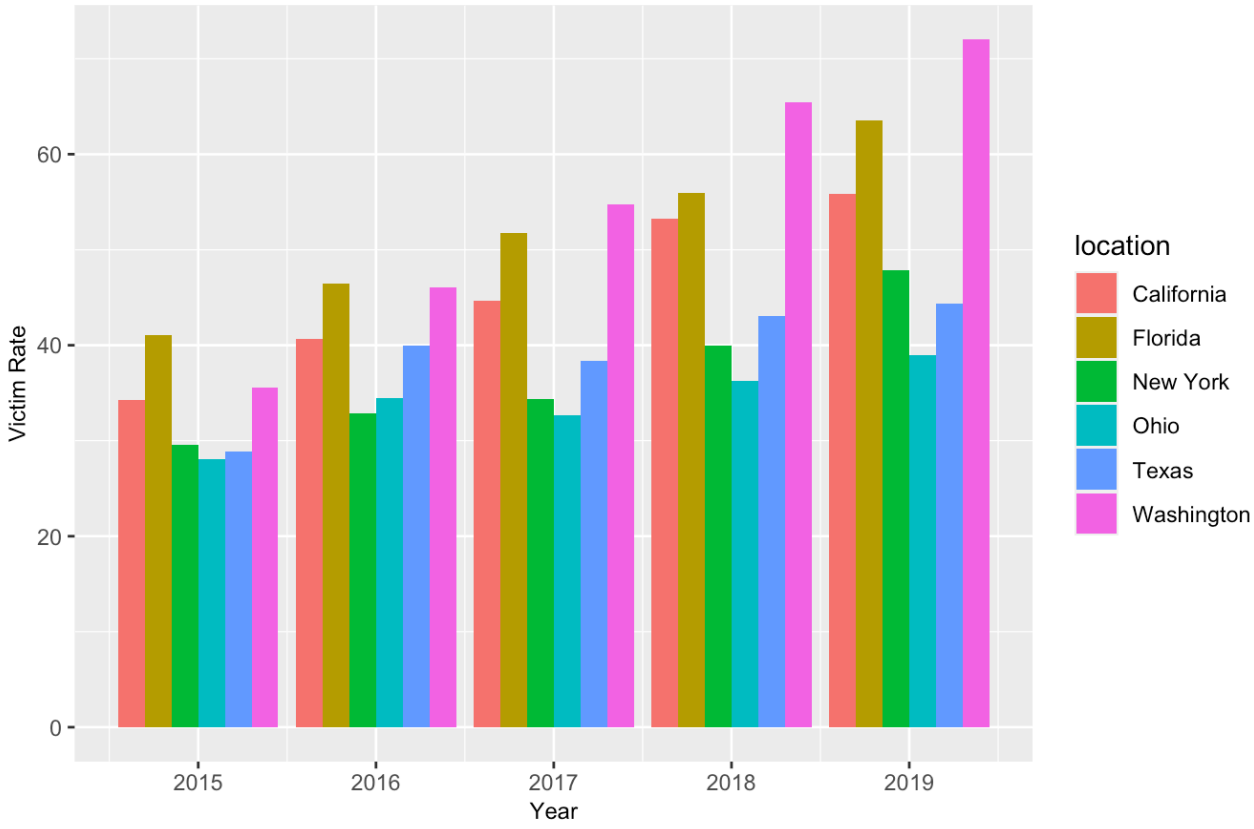
Confidence Fraud/Romance

Loss Rate (USD) per 1 Million Population



Confidence Fraud/Romance

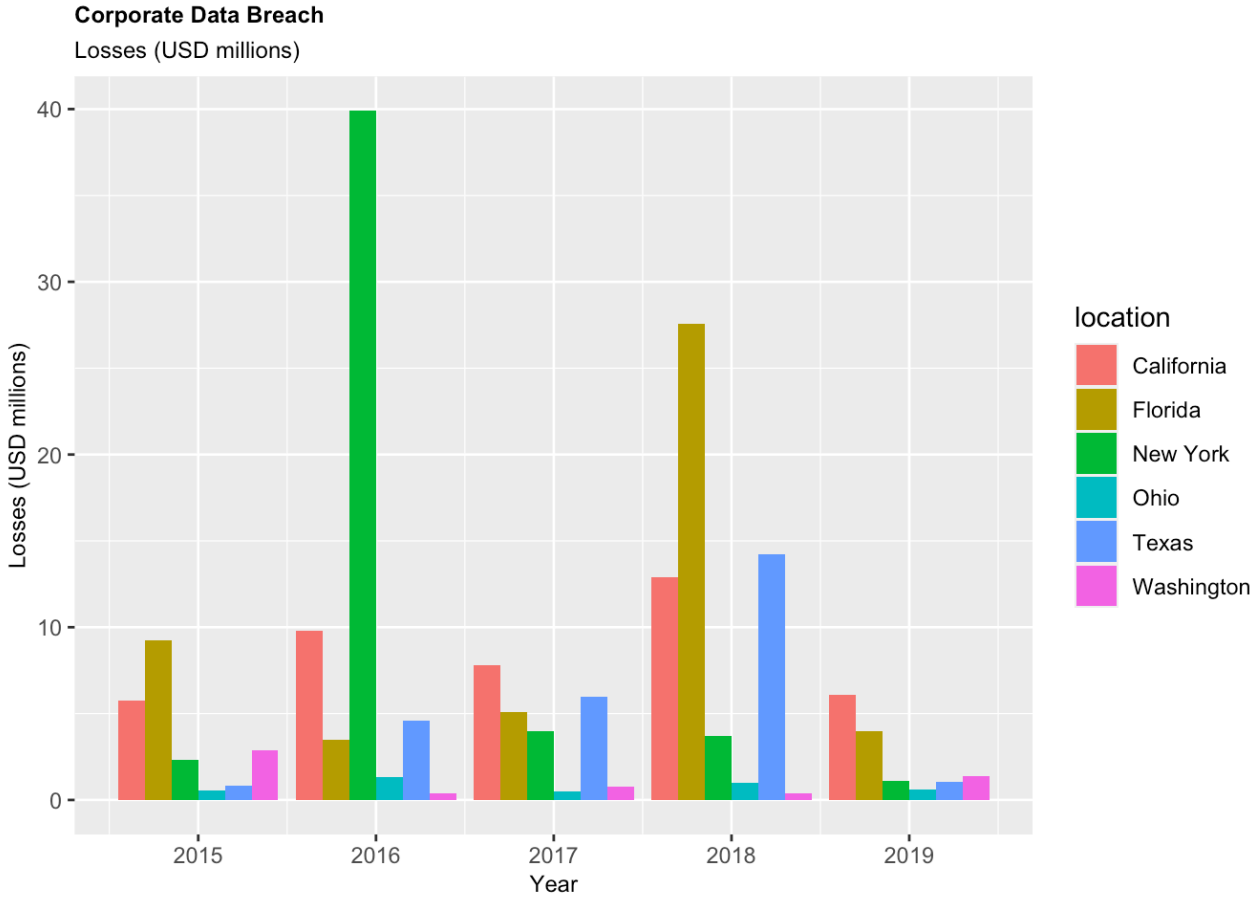
Victim Rate per 1 Million Population



In summary, Confidence Fraud/Romance schemes continued to grow in the US and especially in five of the six top states. California's victim losses continued to increase fastest followed by Washington and Florida.

Corporate data breach

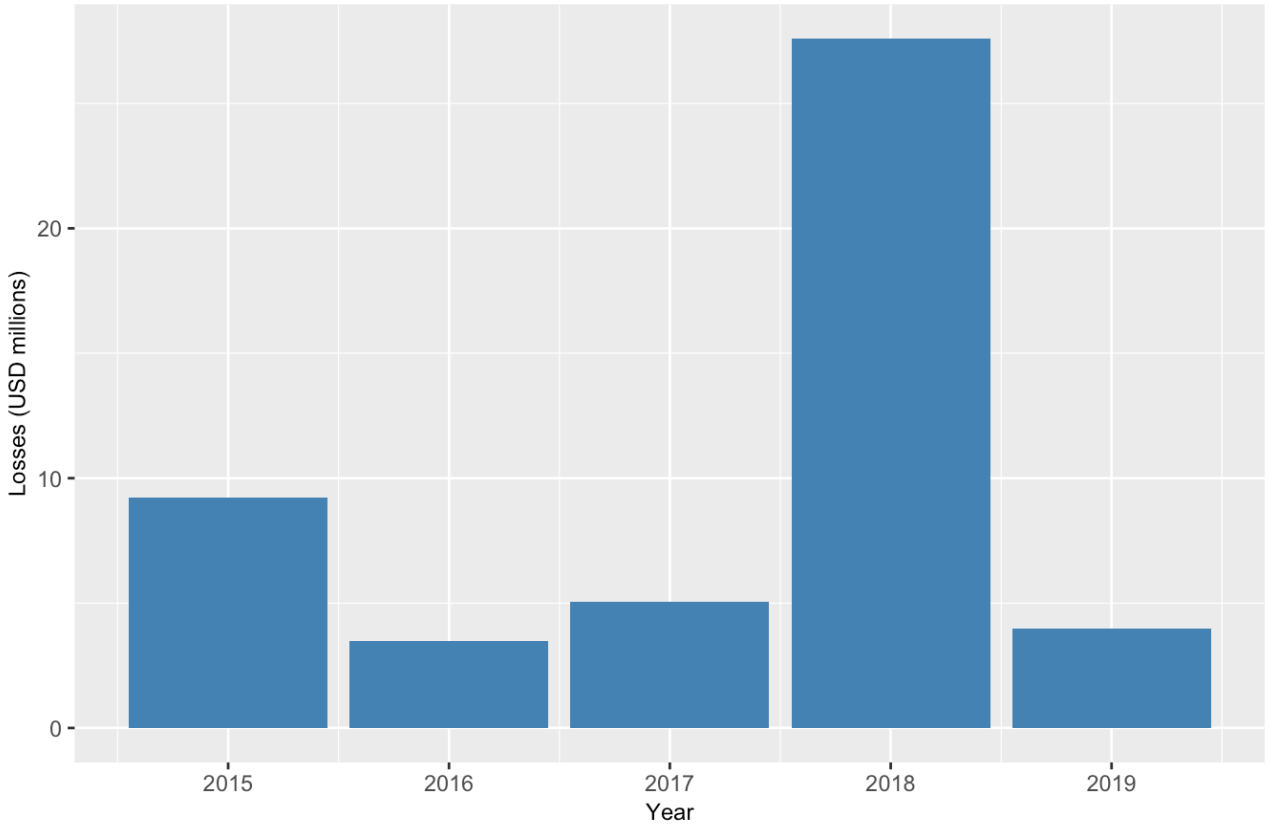
Corporate Data Breach was not a very prominent online crime in any of the six top states in 2019. However, corporations might be reluctant to report a data breach to FBI because such breaches might negatively affect their business. xs We included this crime in our 2018 report because victim losses were high, especially in Florida, where victim losses reached $27.6 million in 2018 up from $5.1 million in 2017. Florida's losses declined 86% to $4.0 million in 2019. Further, in Florida, victim losses from Corporate Data Breach to total online losses was 15.5% in 2018 and decreased to 1.4% in 2019.



Losses to Corporate Data Breach decreased significantly in 2019 in all top states except in Washington where victim losses increased 264%. Yet, Washington victim losses to this crime were relatively small in 2019 at $1.1 million, only 1.9% of its total online losses. In California, victim losses fell 53% to $6.1 million, the highest loss among all the top states in 2019. These losses represented only 1.1% of its total losses. In New York, Ohio, and Texas, losses decreased by 70%, 43%, and 93%, respectively, in 2019.

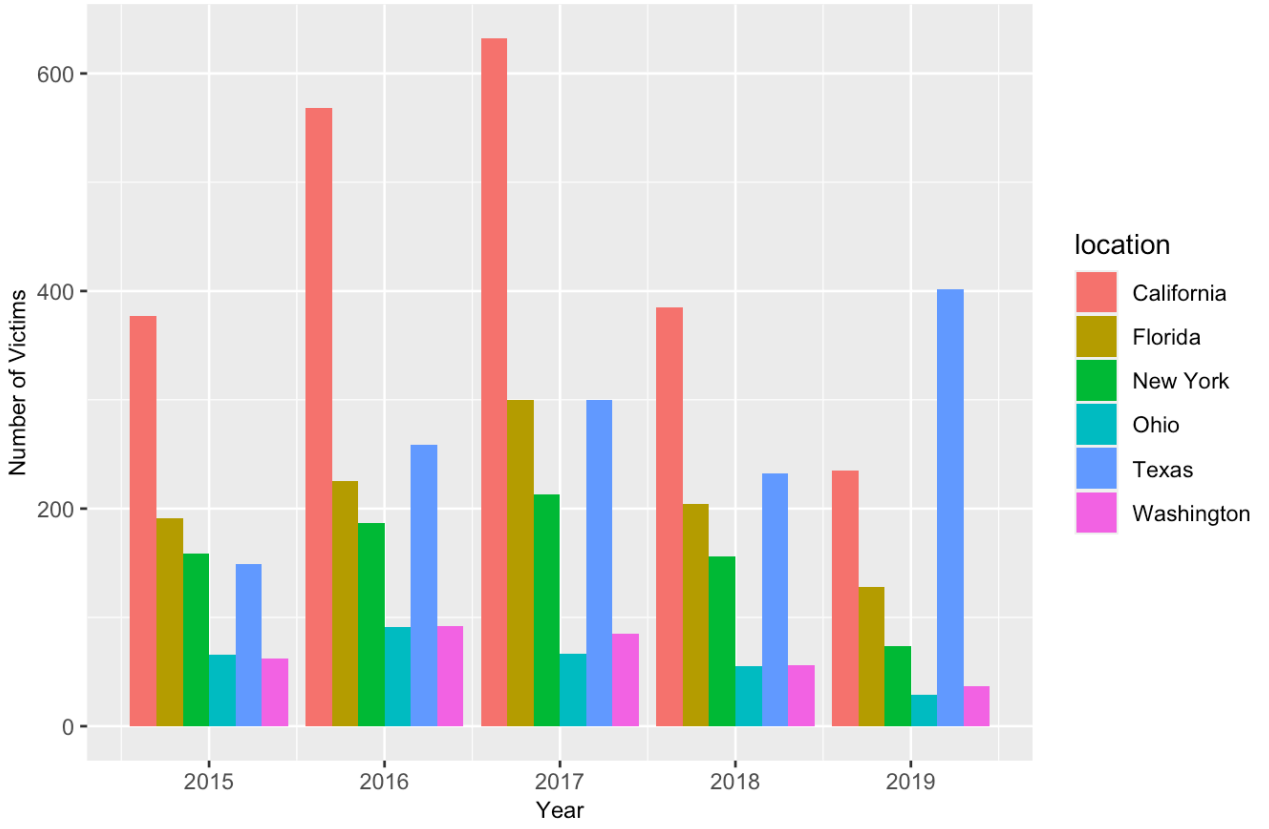
Florida -- Corporate Data Breach

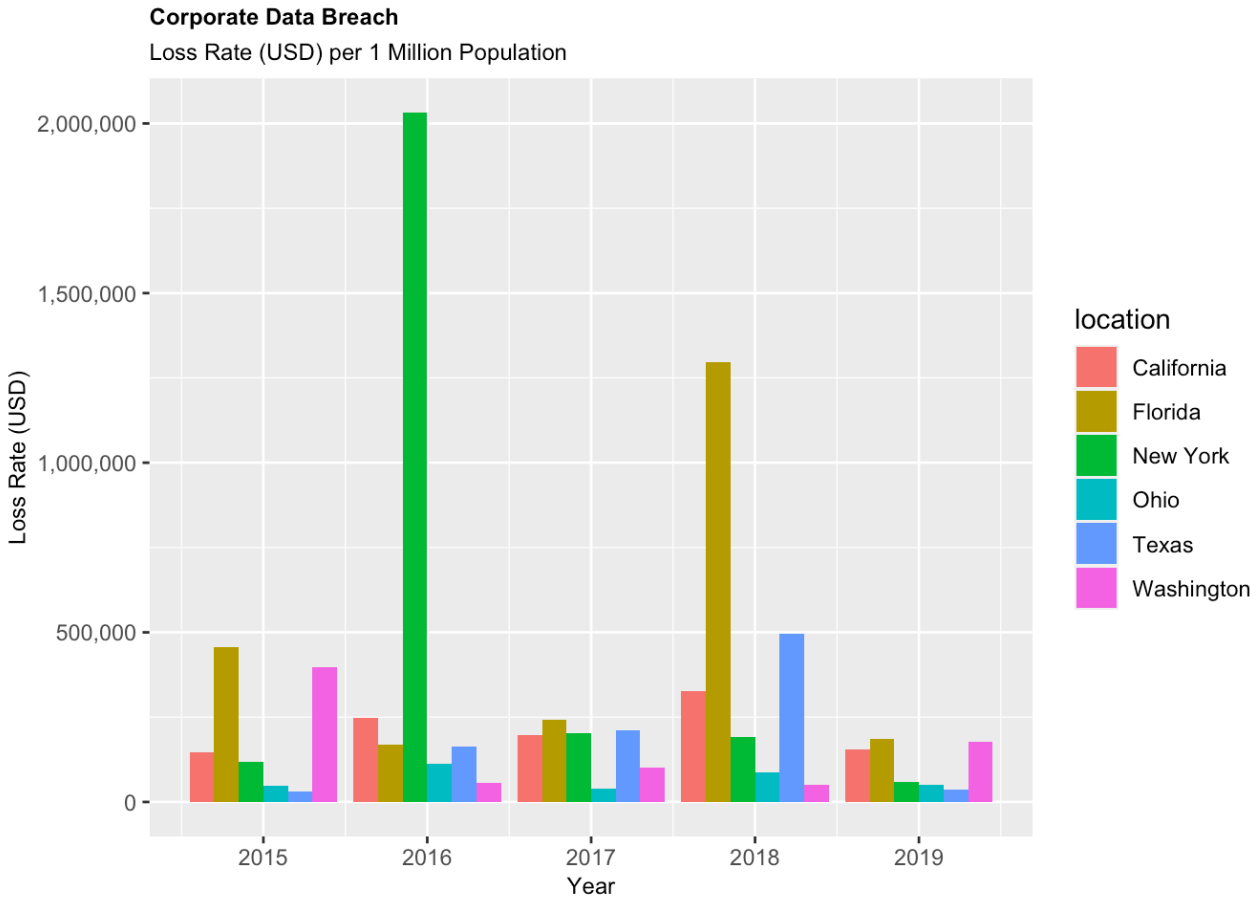
Losses (USD millions)



Corporate Data Breach

Number of Victims





In terms of victim loss rates, Florida and Washington were the states with the highest 2019 rates of $185,000 and $179,000 per one million in population, respectively. California's loss rate of $153,000 was close to Florida and Washington. New York, Ohio, and Texas had much lower loss rates.

Overall, 2019 victim losses from Corporate Data Breach were relatively similar to their losses in 2015. Between these years, however, California , Florida, New York, and Texas experienced one-year spikes in victim losses before declining.

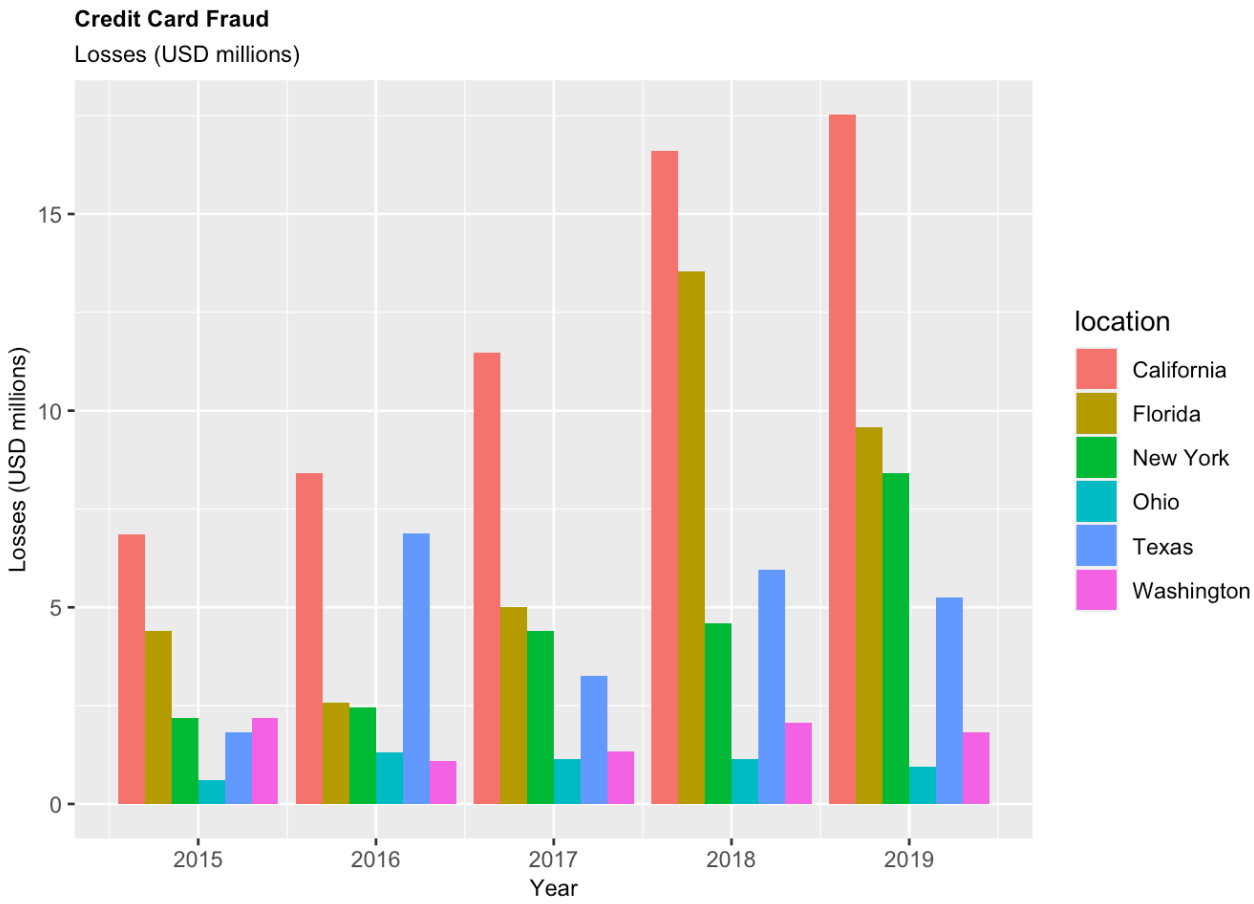
Credit card fraud

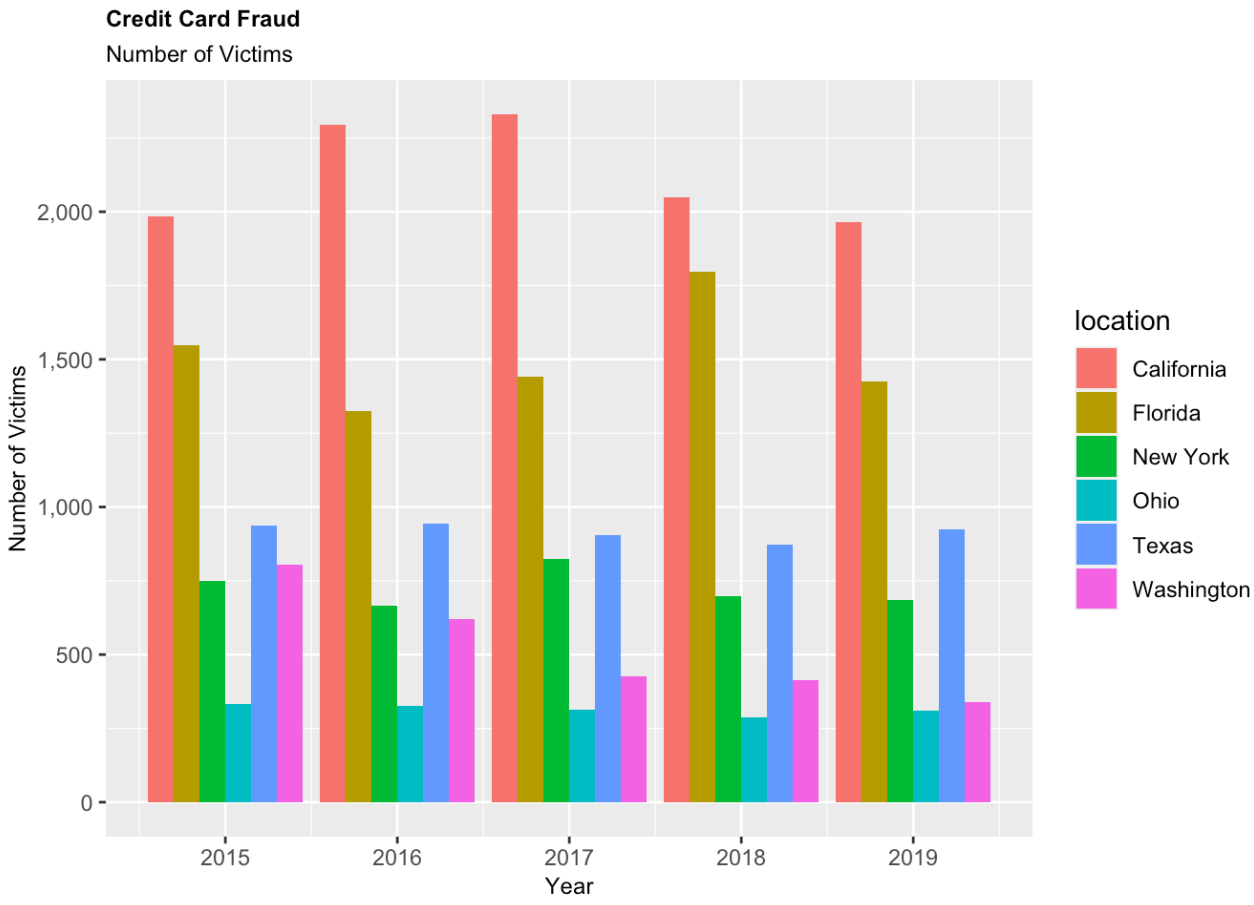
Credit Card fraud refers to online crimes committed using a credit card or similar form for payment as a source of funds to make a fraudulent transaction such as buying goods or services.

Even though online Credit Card fraud victim losses and the number of victims decreased during 2019, it continued to be an important crime in the six top states especially in New York and California.

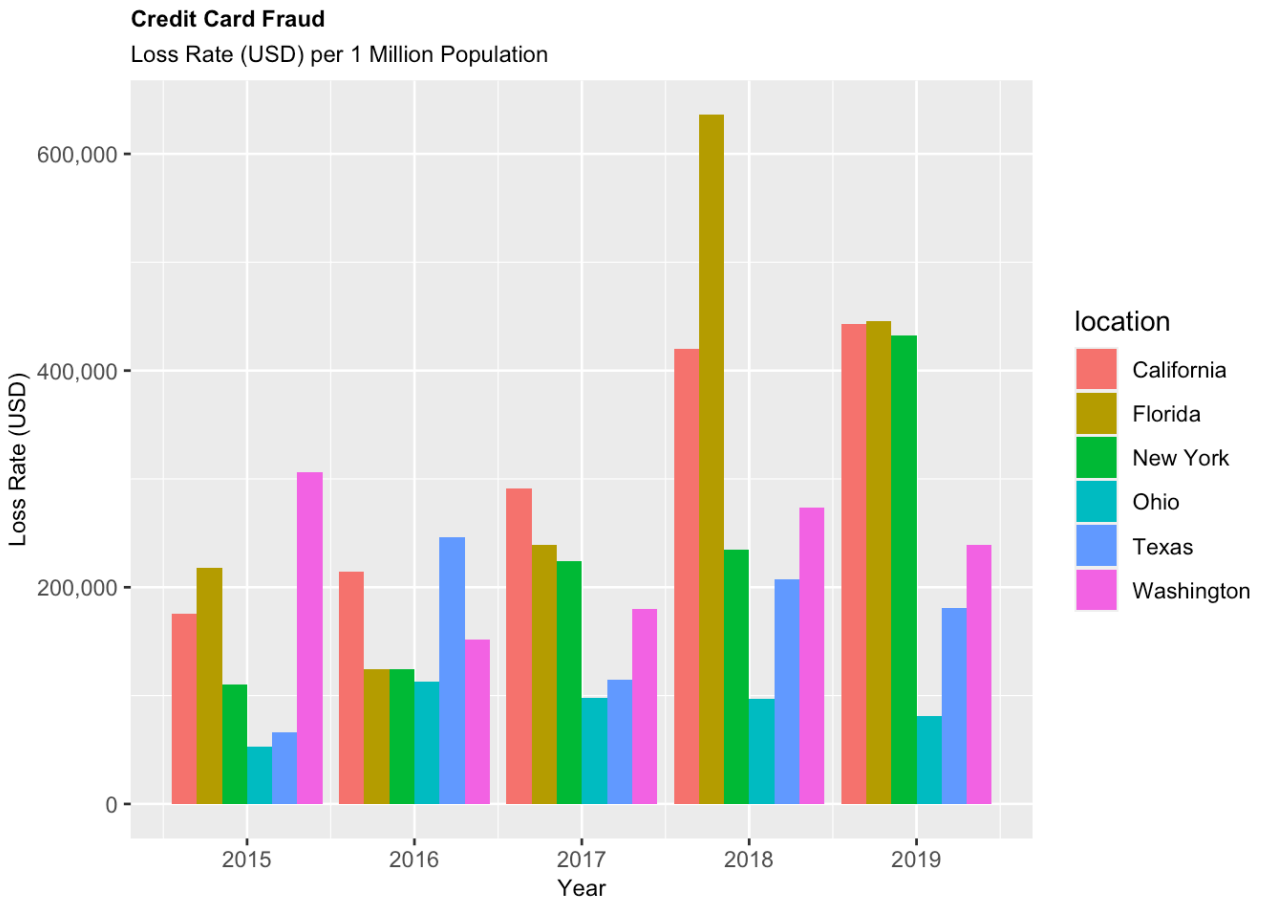
Victim losses in New York increased 83% from $4.6 million in 2018 to $8.4 million in 2019, and 5% in California from $16.6 million to $17.5 million. In contrast, victim losses in Florida declined by 29% in 2019 from $13.5 million in 2018 to $9.6 million in 2019, in Ohio from $1.1 million to $935,000, Texas from $5.9 million to $5.2 million, and Washington from $2.0 million to $1.8 million.

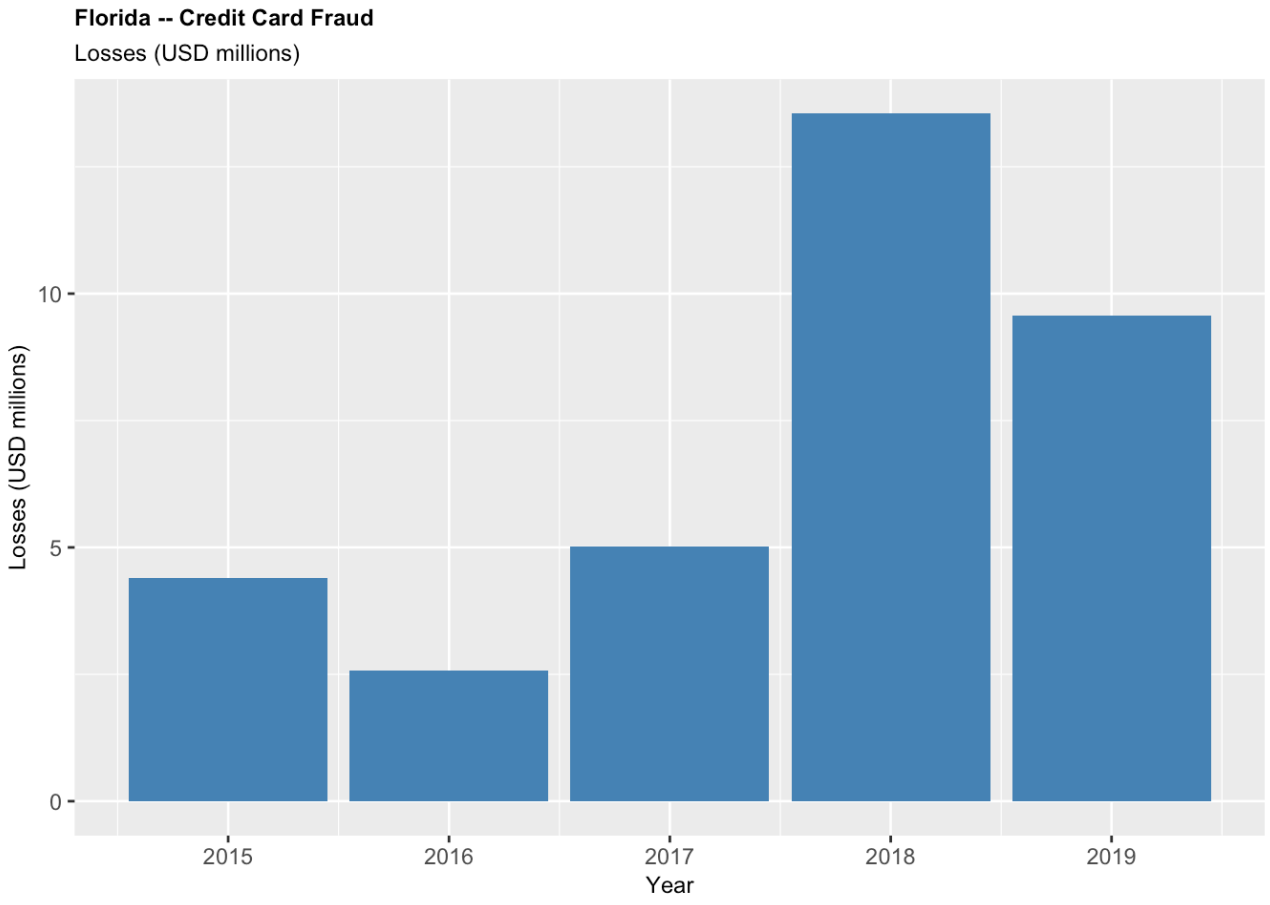
Florida's credit card victim losses to its total victim loss ratio decreased from 8% in 2018 to 3% in 2019.



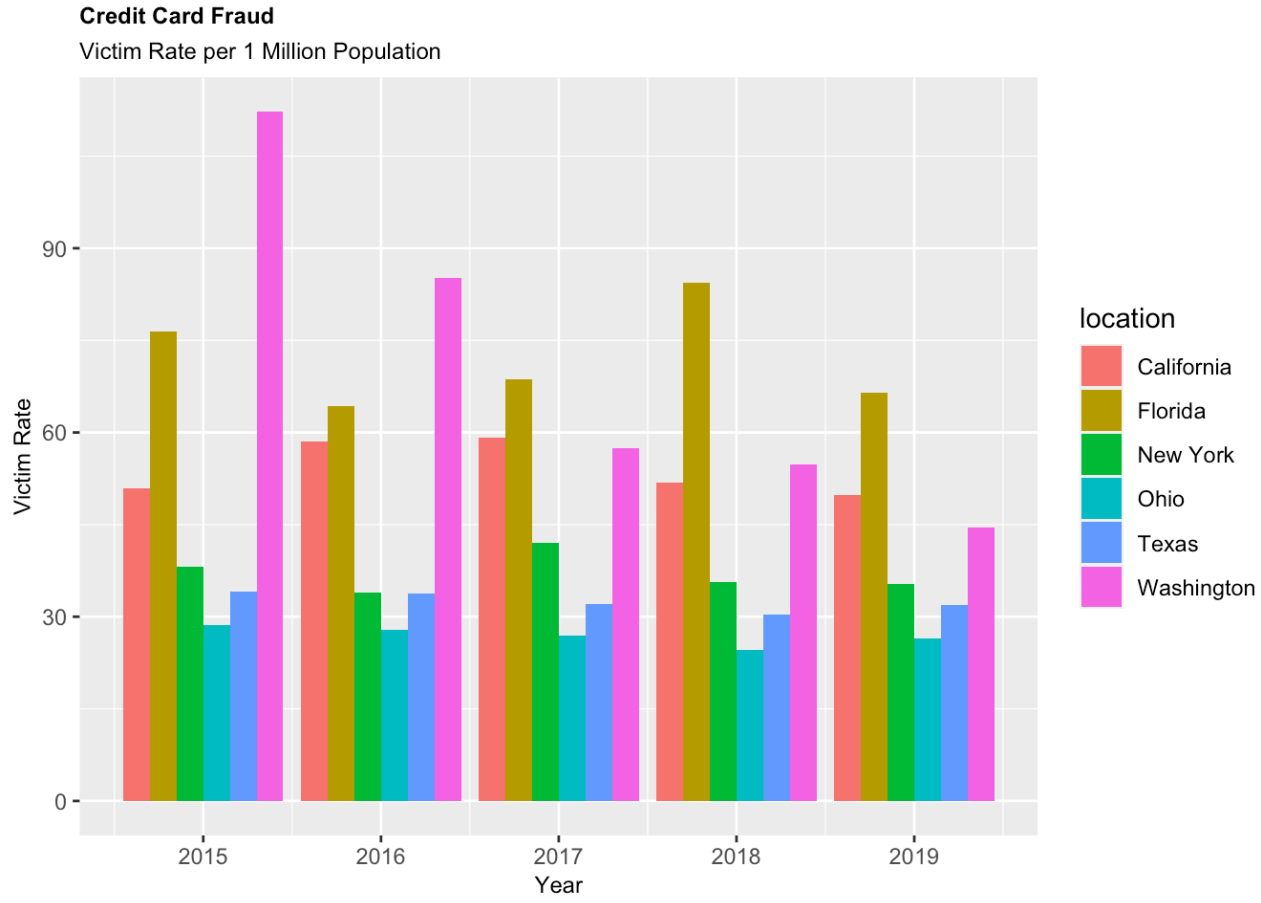


Moreover, the number of 2019 victims in Florida decreased 21%, Washington 18%, California 4%, and New York 2%. Ohio and Texas experienced increases of 8% and 6%, respectively.


Credit Card Fraud
Loss Rate (USD) per 1 Million Population
600,000
400,000
200,000
0
Loss Rate (USD)
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


Florida -- Credit Card Fraud
Losses (USD millions)
10
5
0
Losses (USD millions)
2015
2016
2017
2018
2019
Year

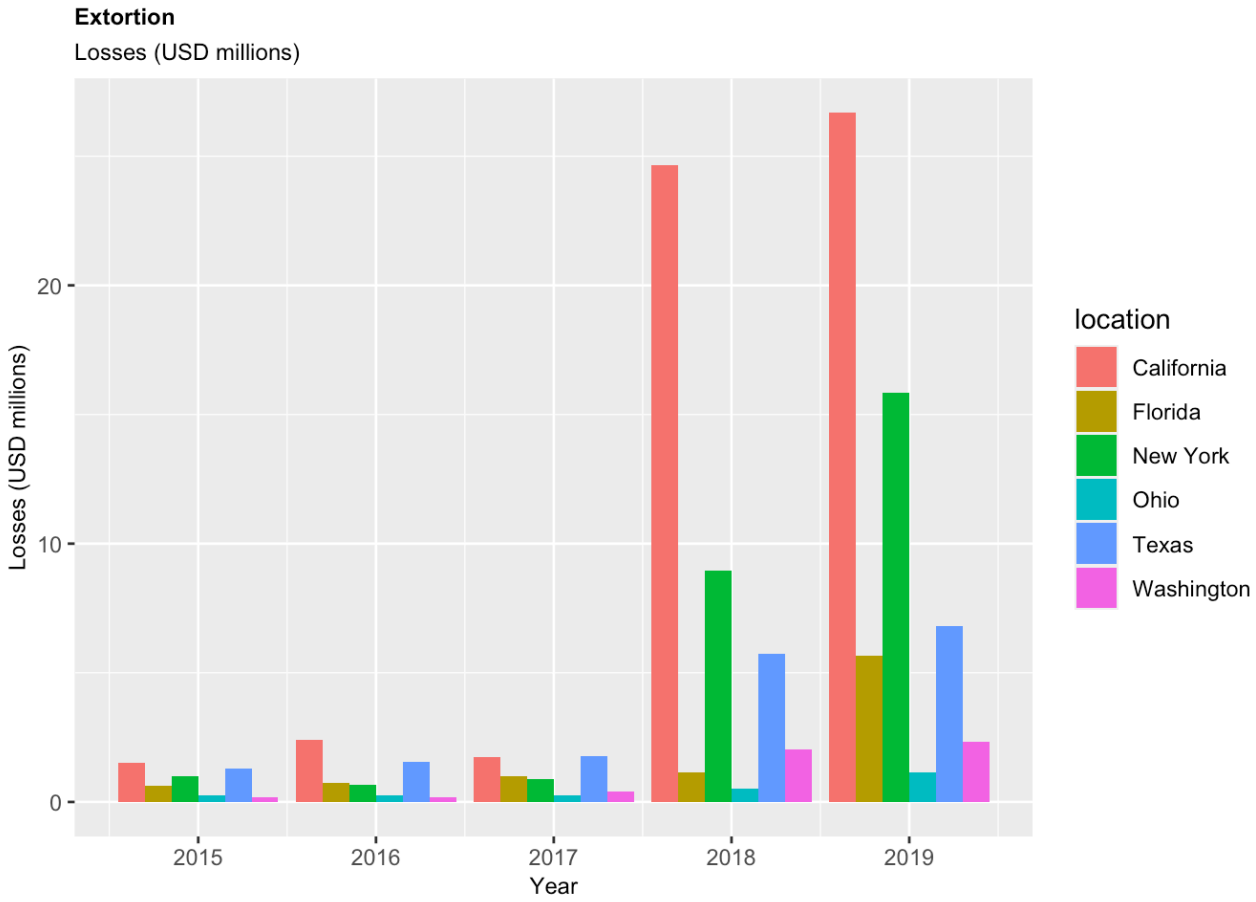
Florida's 2019 online loss rate fell from $636,000 in 2018 to $446,000 in 2019. New York's loss rate jumped to $432,000 in 2019 from $235,000 in 2018. Further, Florida's 2019 victim rate of 66 per one million in population continued to be above the other top states.



In general, online Credit Card fraud in 2019 was a serious crime with victim loss growth in California and New York. Victim losses declined somewhat in Florida and several other top states during 2019.

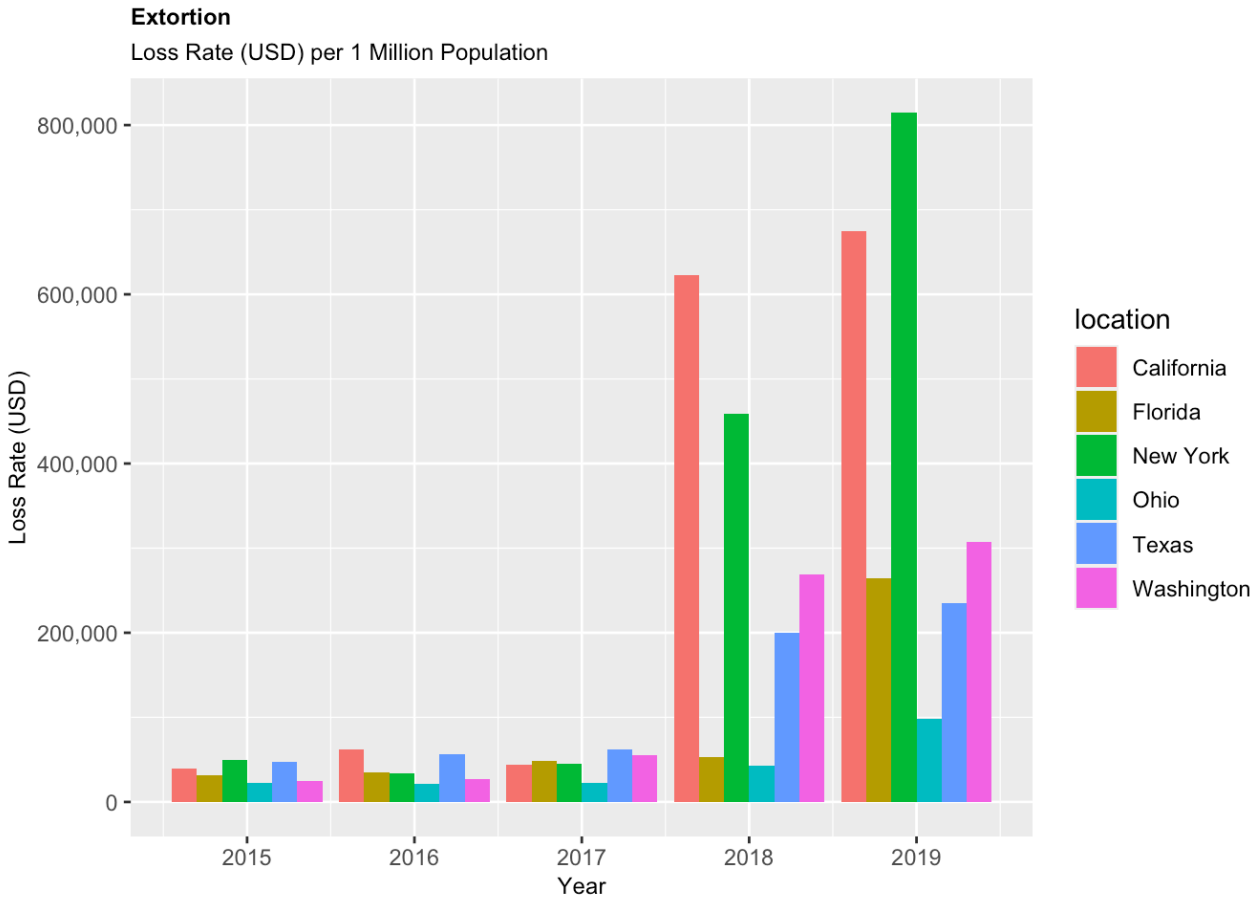
Extortion

Extortion is not a new online crime. Online Extortion takes place when a fraudster demands money or property through intimidation, force, or threat. The FBI has been tracking complaints on this online crime for more than a decade. Reported victim losses were low in earlier years but from 2017 through 2019, and especially from 2018 through 2019, victim losses from this crime increased sharply in the six top states.

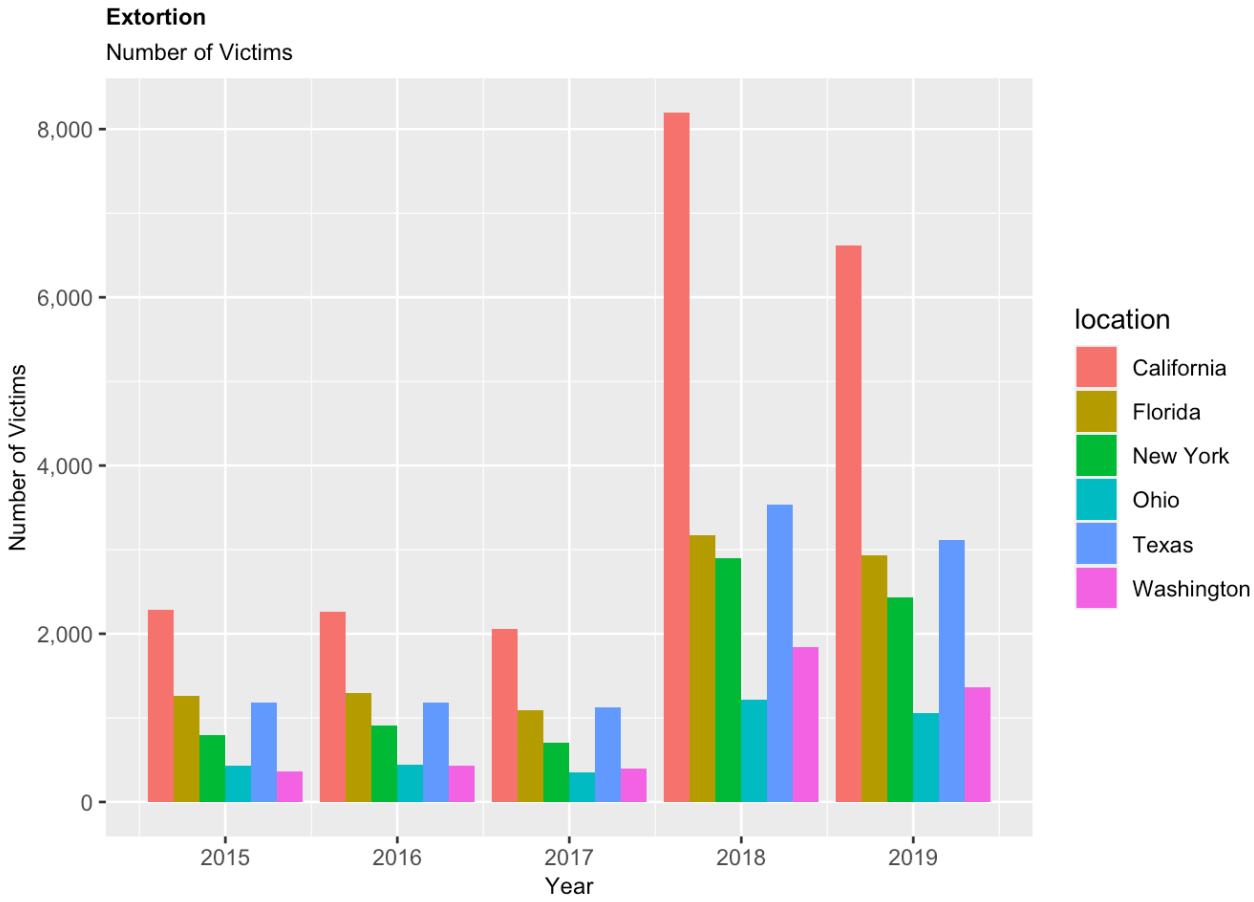


In Florida, Extortion victim losses jumped 400%, from $1.1 million in 2018 to $5.7 million in 2019. This growth rate was Florida's second highest after Identity Theft. Yet, Extortion losses in Florida was only 1.9% of its total online losses in 2019, while in New York it was 8% and in California 4.7%.

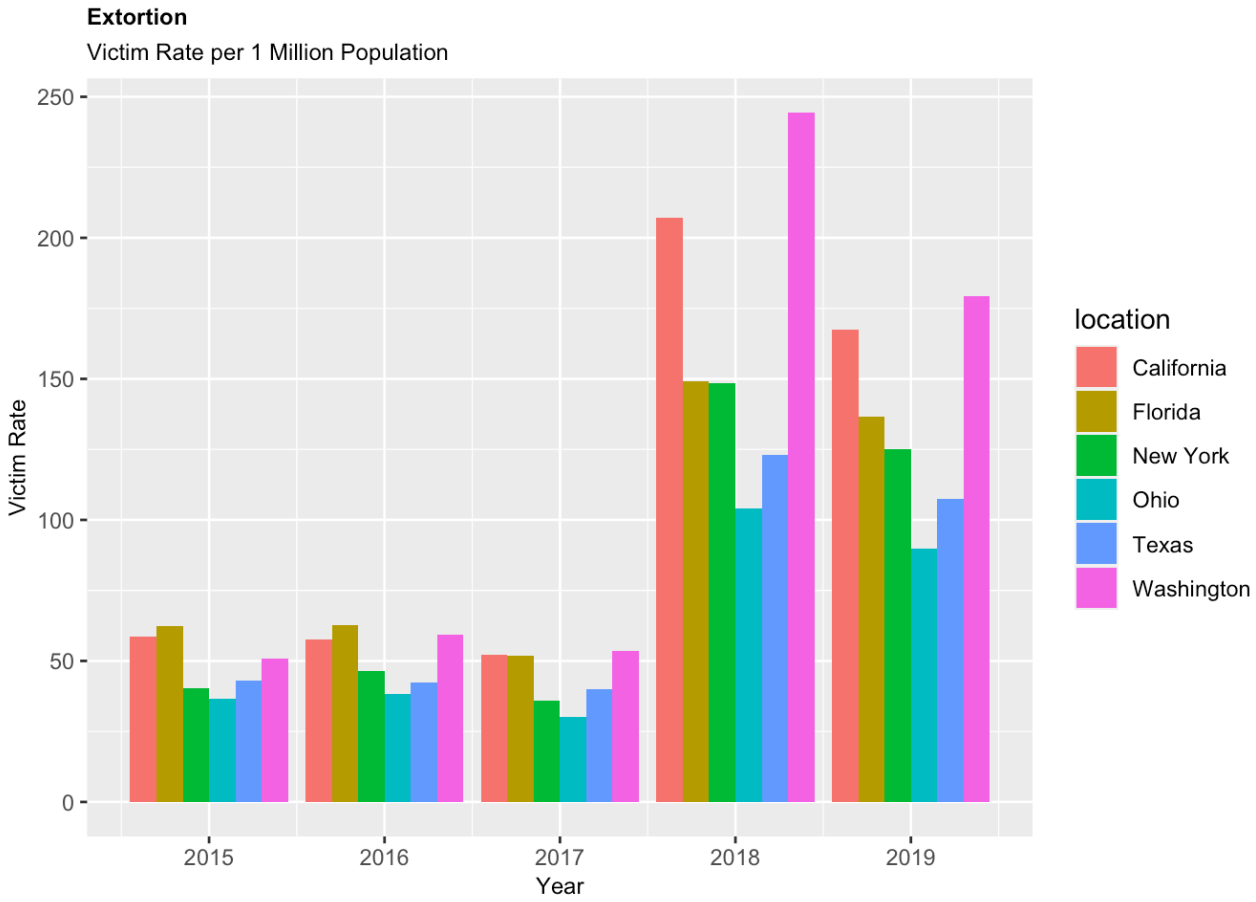
In California, New York, Texas, and Washington, Extortion victim losses spiked in 2018. California's victim losses increased 1,347% from $1.7 million in 2017 to $24.6 million in 2018 and modestly 8.5% from 2018 to 2019. New York had an increase in victim losses of 900% from $886,000 in 2017 to $9.0 million in 2018 and 75.6% in 2019. Victim losses in Texas increased 222% from 2017 to 2018, but only 18% in 2019. Washington had an increase of 400% from 2017 to 2018 but only 16% in 2019. Ohio had the lowest growth in victim losses from 2017 to 2018, at 68% but had significant growth of 120% in 2019.



In terms of 2019 victim losses adjusted for population, New York had the highest loss rate of $814,000 per one million in population, followed by California with $675,000. Florida, Texas, and Washington had loss rates of $264,000, $235,000, and $308,000, respectively. Ohio had the lowest loss rate of the six top states in 2019 with victim losses of $98,000 per one million in population. Nevertheless, Ohio's loss rate jumped 127% in 2019.



The number of victims also jumped in 2018 with the highest increases in Washington (360%), New York (312%), and California (300%). Florida also experienced growth in victim numbers in 2018 of 191% but a decline in 2019 of 7.6%. The other five top states also experienced a decline in the number of victims in 2019.



In terms of the number of victims adjusted to population, Washington had the highest victim rate with 179 per one million in population. California followed with 167, and Florida with 137.

Overall, online Extortion had not been a relatively large online crime prior to 2018. However, online Extortion losses and number of victims grew sharply in 2018 and remained high in 2019.

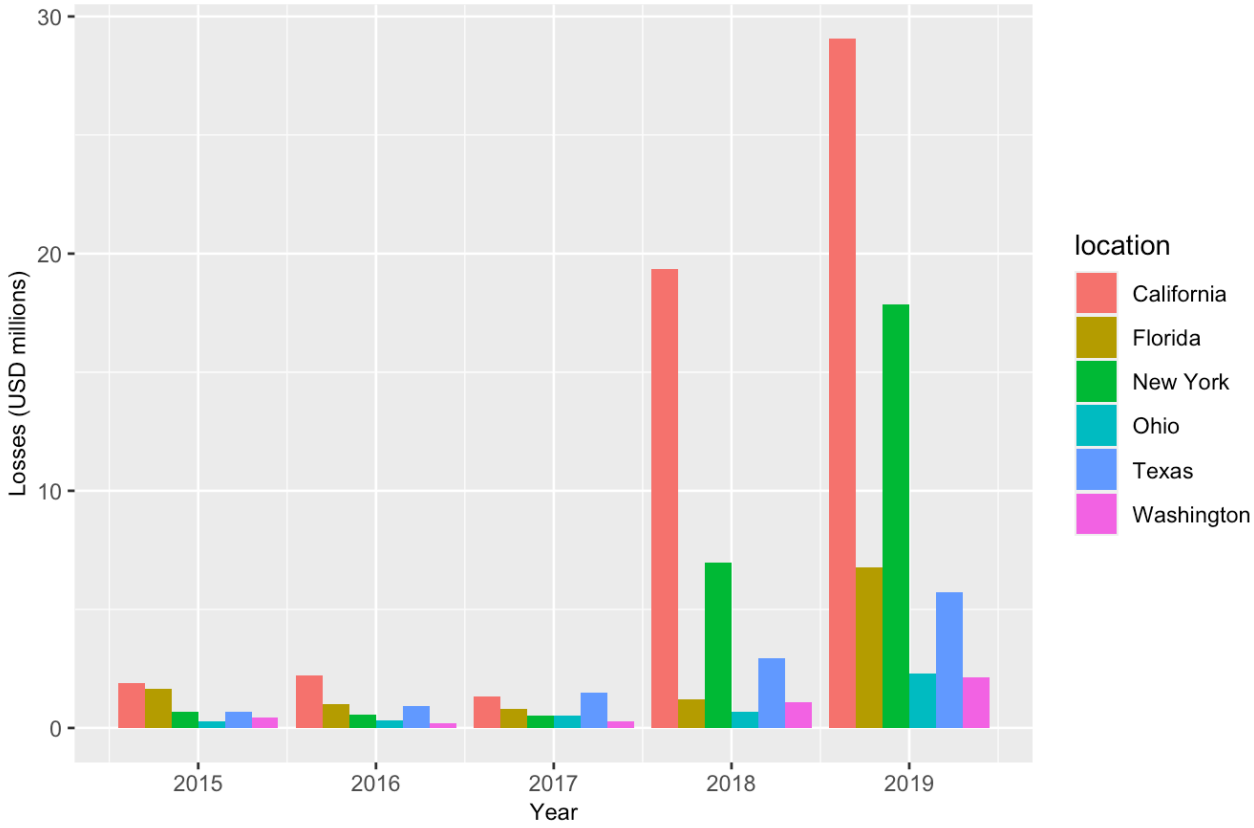
Government Impersonation

The Government Impersonation scheme takes place when an online fraudster pretends to work for a government agency to obtain money from a victim. For instance, in 2019, victims reported receiving calls from scammers saying they were from the IRS. The fraudster told a victim they owed money to the IRS and threaten them with arrest or prison if not returning the scammer's call.

Government Impersonation, like Extortion, has been around for many years but gained momentum in 2019, becoming a high growth online crime especially in California and New York.

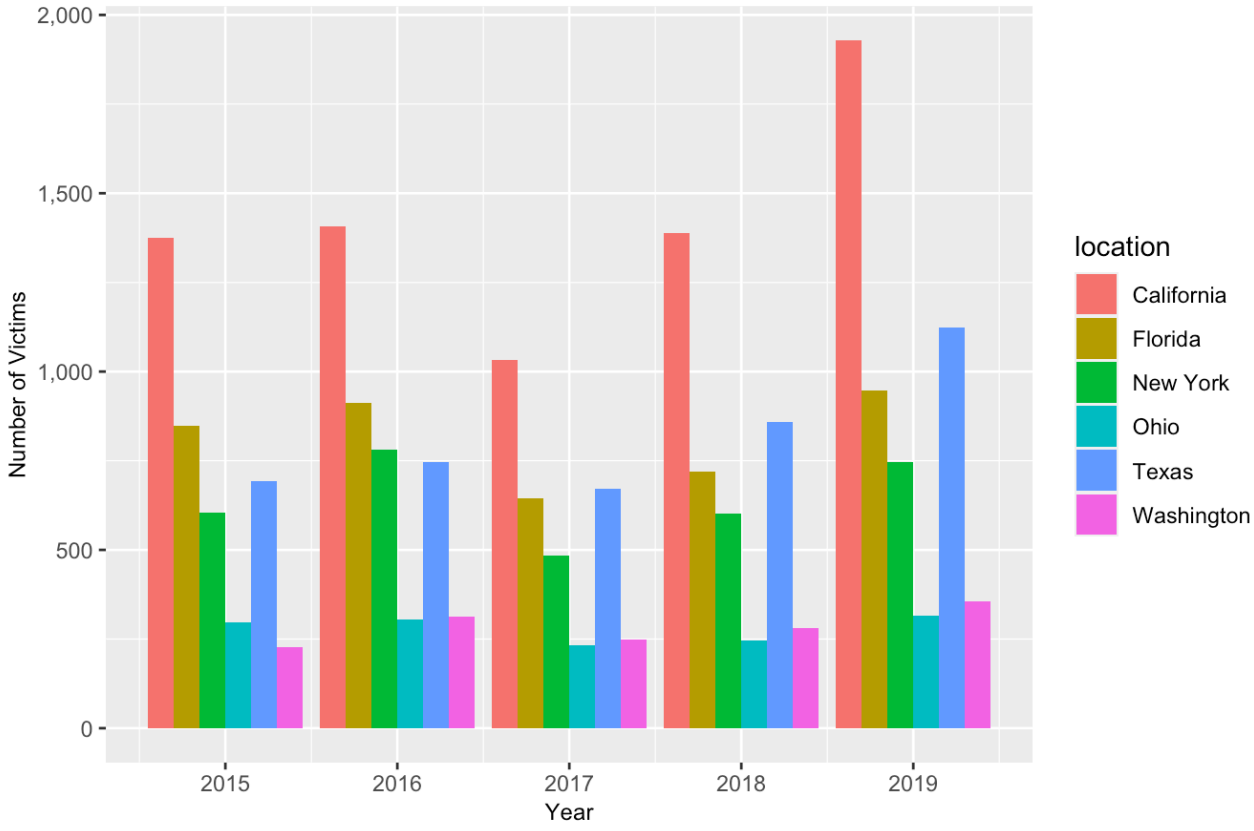
Government Impersonation

Losses (USD millions)



Government Impersonation

Number of Victims



Government Impersonation victim losses in California and New York spiked during 2018 while the number of victims increased more slowly. In California, victim losses increased sharply by 1,362%, from $1.3 million in 2017 to $19.0 million in 2018, and a smaller increase of 50% to $29 million in 2019.

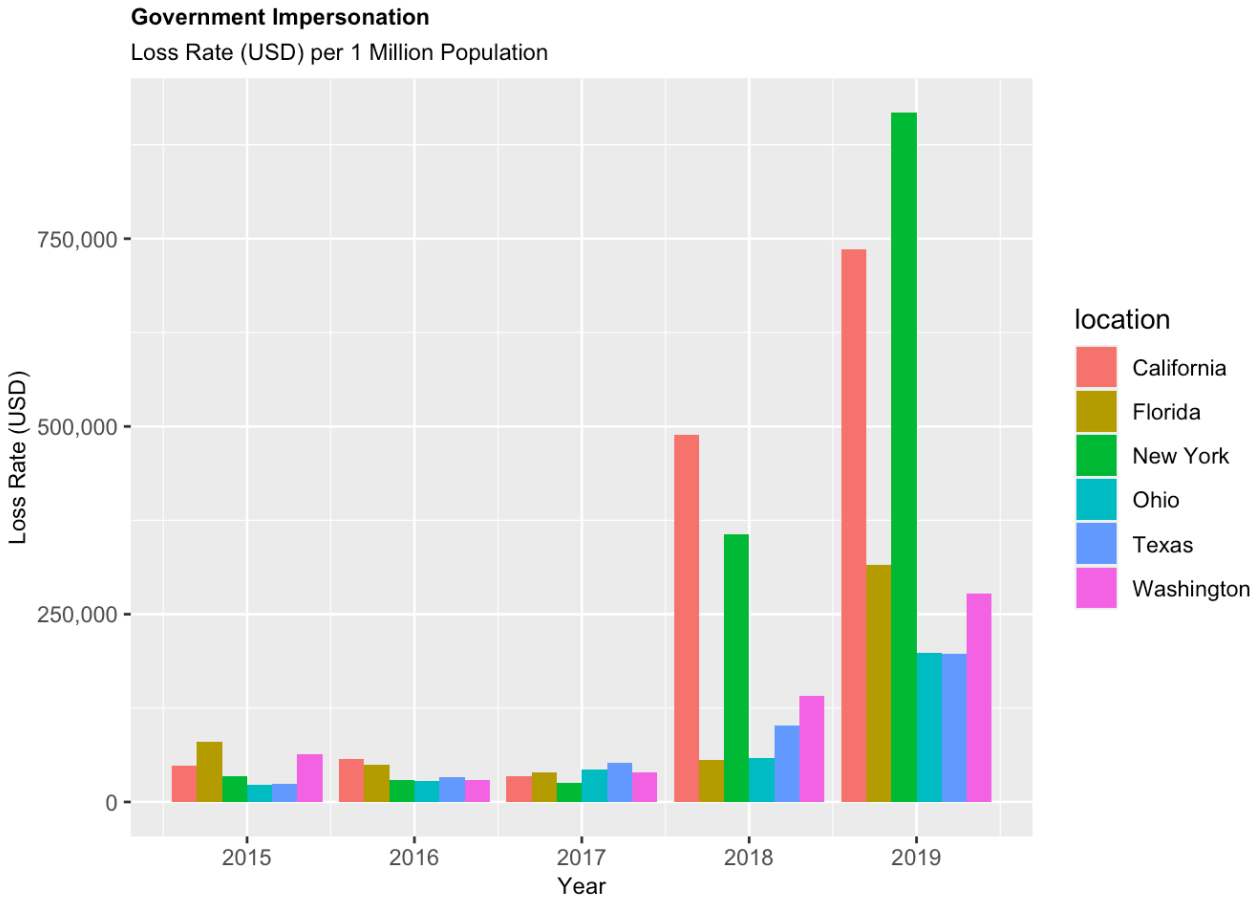
Similar to California, New York's victim losses increased sharply, 1,300% from $505,000 in 2017 to $7.0 million in 2018, and 156% to $17.9 million in 2019. Government Impersonation victim losses in New York had a 9% share of its total online victim losses in 2019 compared to California's 5% share.

Texas and Washington also experienced increases in Government Impersonation victim losses from 2017 to 2018. In Texas, victim losses grew 107% from $1.4 million in 2017 to $2.9 million in 2018, and a 96% increase to $5.7 million in 2019.

In Washington, victim losses increased 267% from $294,000 in 2017 to $1.1 million in 2018, and 98% to $2.1 million in 2019.

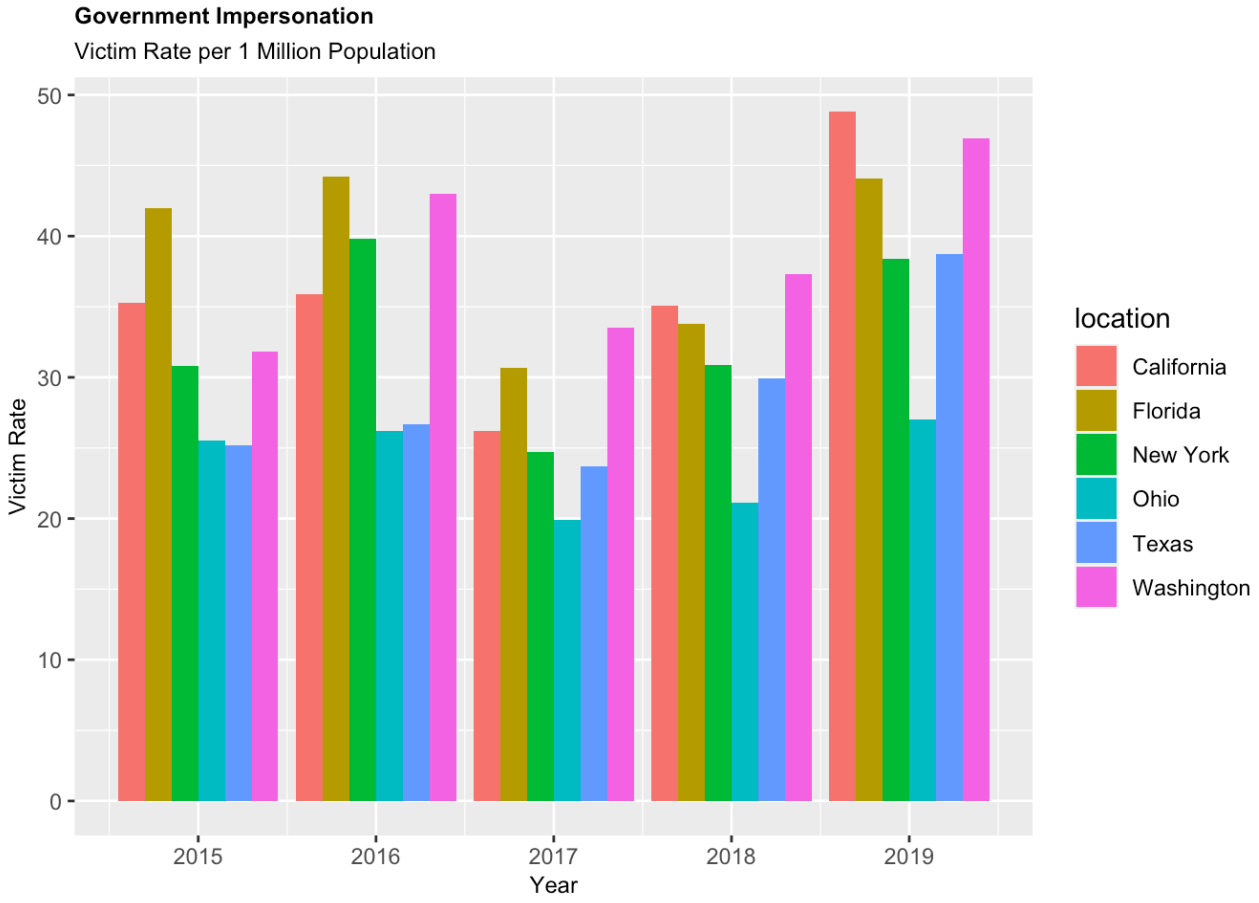
In Florida and Ohio, most of the increases in victim losses took place in 2019. Florida had victim losses in 2019 of $6.8 million, up from $1.2 million in 2018, a 465% increase. Ohio had an increase of 235% from $690,000 in 2018 to $2.3 million in 2019.

The number of victims grew at a much slower pace than victim losses among the six top states in 2019. California had the highest growth of 39% followed by Florida with 32%, Texas 31%, Ohio 28%, Washington 27%, and New York with 24% increase.



Government Impersonation loss rates in the six top states had some sharp growth in 2018 and 2019. California and New York had the highest rates among the top states in 2018 and 2019. In California, loss rates jumped from $34,000 per one million in population in 2017 to $489,000 in 2018, and to $735,000 in 2019. Similarly, New York loss rates increased from $26,000 per one million in population in 2017 to $356,000 in 2018, and to $917,000 in 2019.

Florida, with the third highest loss rate in 2019 after California and New York, loss rates increased from $56,000 per one million in population in 2018 to $316,000 in 2019. In Washington, loss rates increased from $142,000 per one million in population in 2018 to $278,000 in 2019.



Overall, victim rates increased during 2018 in the top states and increased further in 2019. In 2019, California, Florida, and Washington had the highest victim rates. California (40%), Florida (29%), Ohio (29%) and Texas (30%) had the highest victim rate growth from 2018 through 2019.

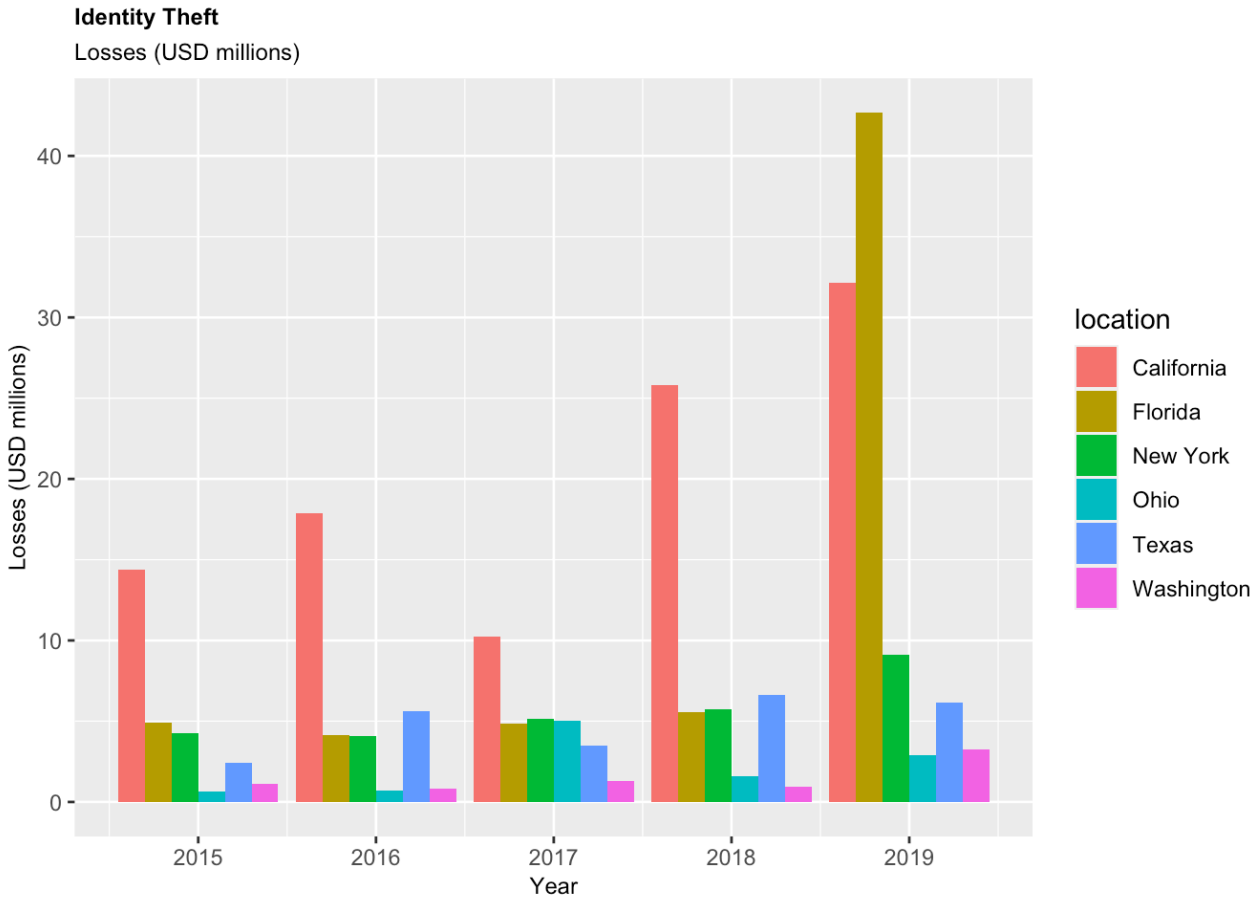
Identity Theft

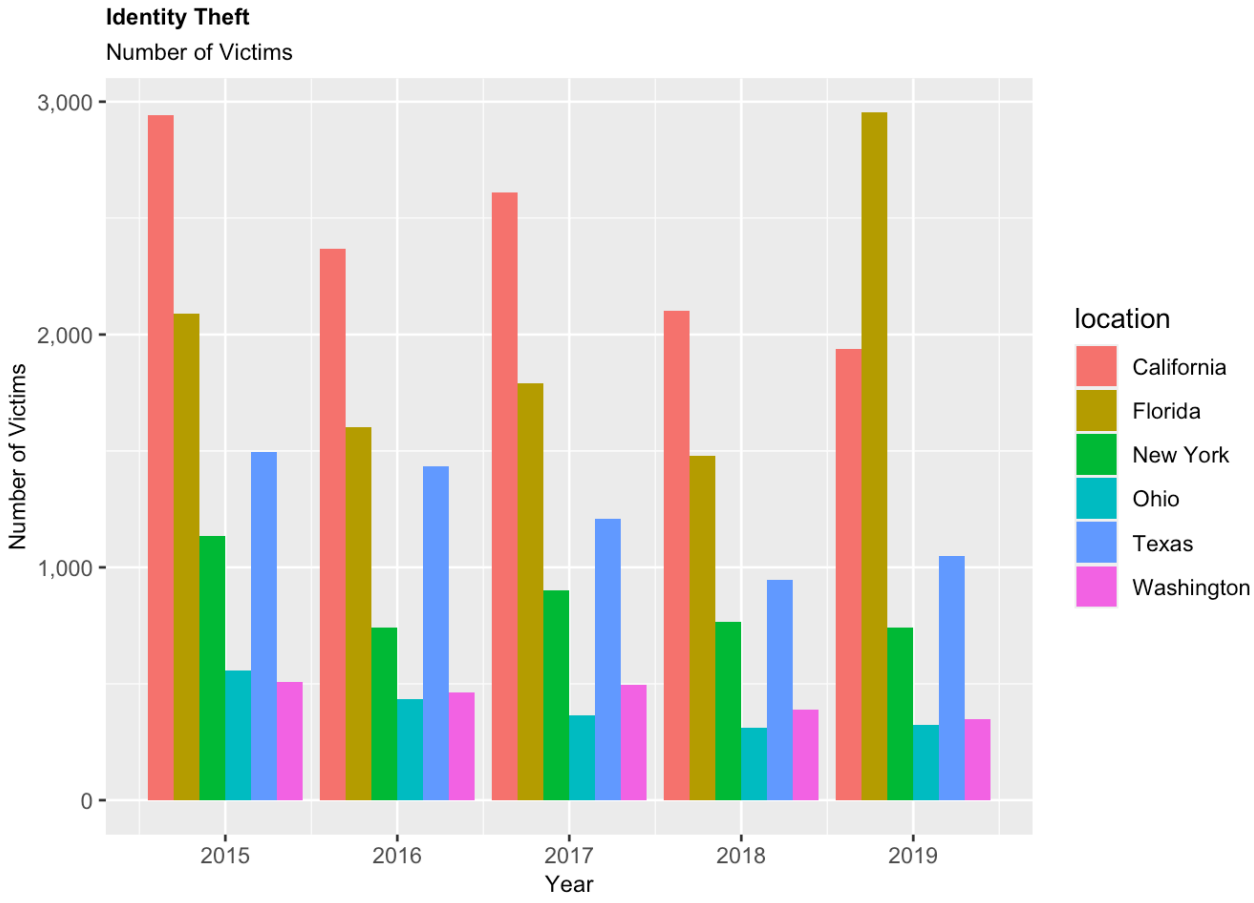
Identity Theft occurs when a scammer steals a victim's personal identifying information such as their Social Security Number or Medicare number without permission, to commit fraud or another crime on the victim or another person/organization. Electronic records have made identity theft relatively common.

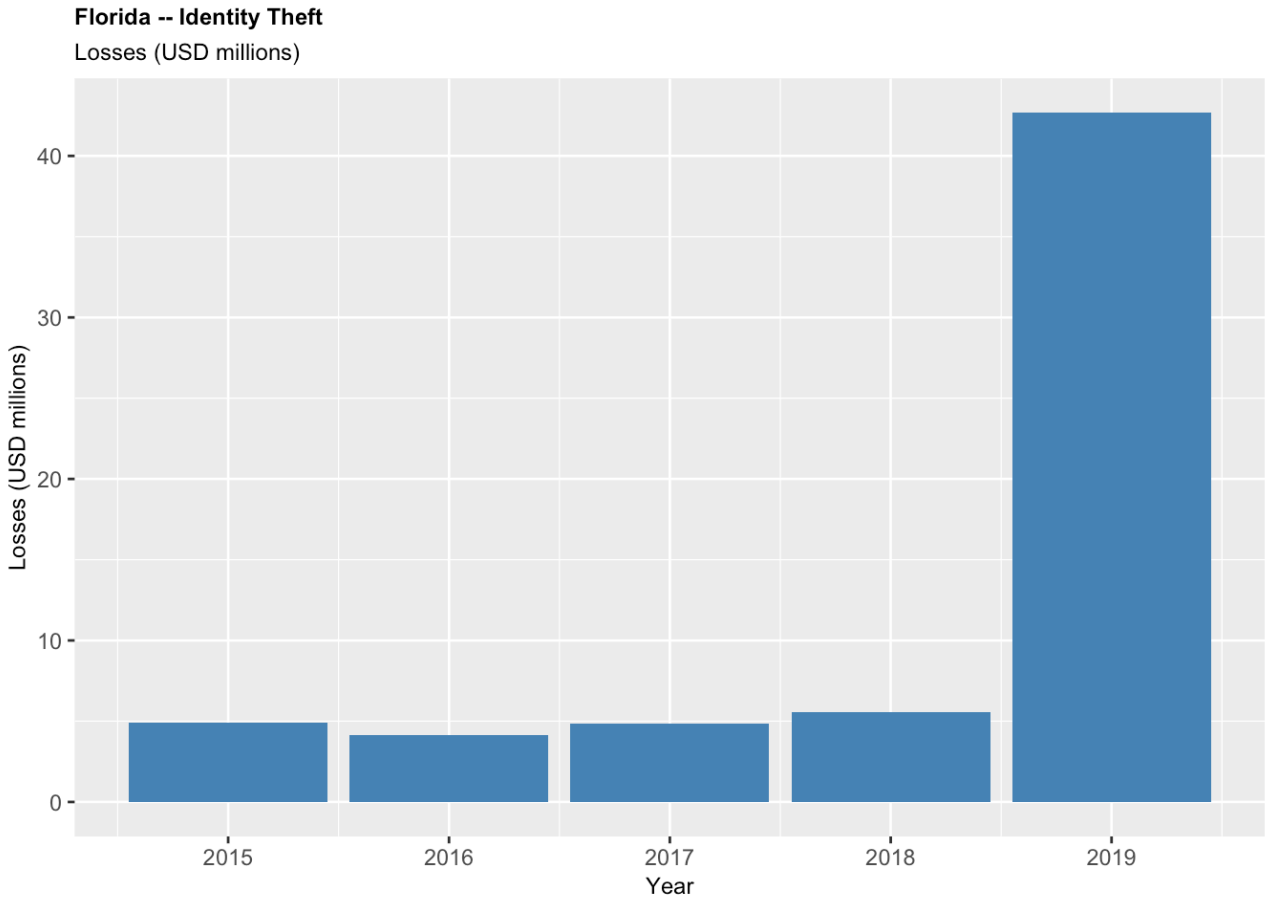
Among the six top states, California had the most victim losses due to online Identity Theft from 2015 through 2018. But in 2019, Florida became the top growth state with a 669% increase from $5.6 million in 2018 to $42.6 million. Identity Theft was a small portion of Florida's total online victim losses through 2018 ranging from 3% to 5% of all losses. But in 2019, 16% of its total losses came from online Identity Theft. In addition, the number of victims in Florida doubled in 2019.

Other top states also experienced increases in losses during 2019: Washington with a 248% increase, Ohio 83%, New York 59%, and California 25%. In 2019, California, with the second highest victim losses, grew from $26 million to $32 million in losses but the number of victims decreased by 8%. Washington's losses increased from $937,000 in 2018 to $3.3 million in 2019 but it had a 10% decline in number of victims.

In Ohio, victim losses increased from $1.6 million in 2018 to $2.9 million in 2019 with an increase of 4% in the number of victims. New York losses increased from $5.7 million in 2018 to $9.1 million in 2019 with a 3% decrease in number of victims. In contrast, Texas had a 7.4% decline in victim losses in 2019 compared to the previous year, from $6.6 million to $6.1 million, but the number of victims increased by 11%.


Identity Theft
Losses (USD millions)
Losses (USD millions)
40
30
20
10
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


Identity Theft
Number of Victims
Number of Victims
3,000
2,000
1,000
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington

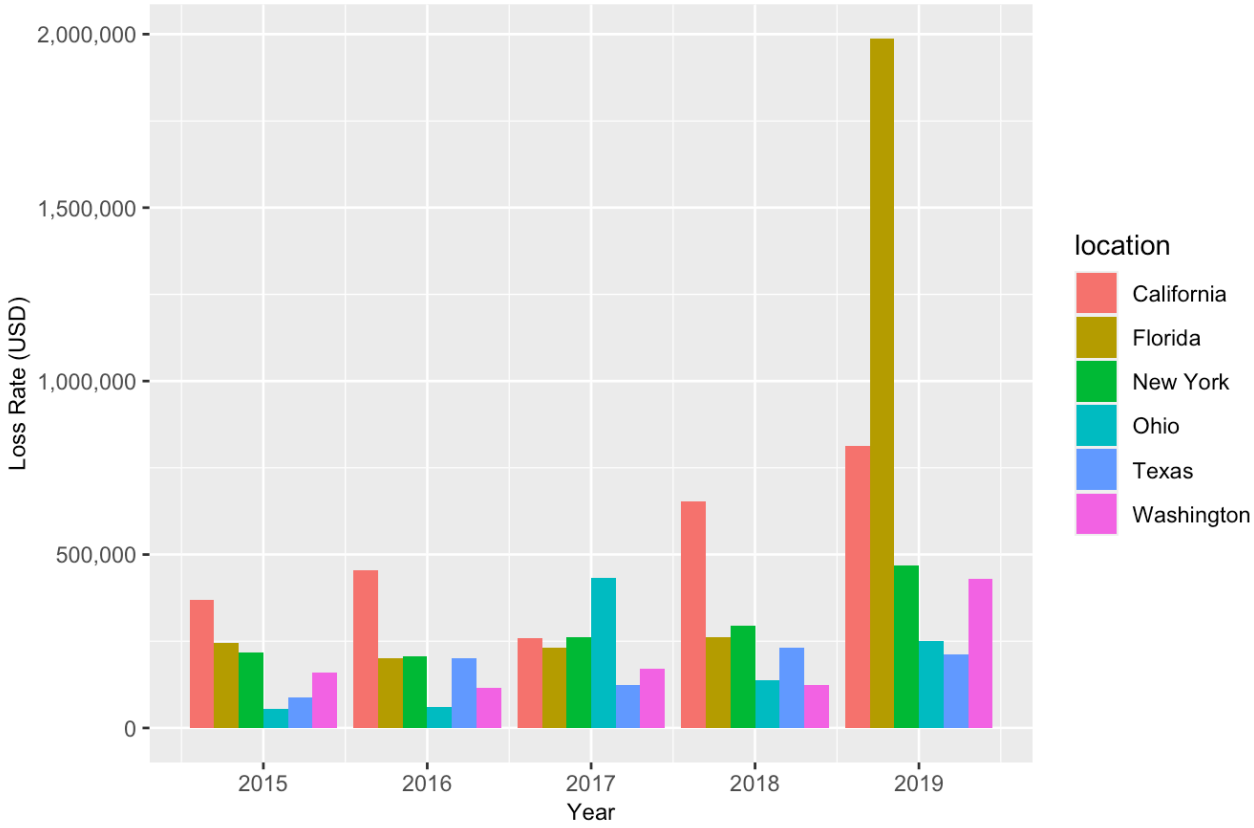


In terms of victim losses adjusted for population, Florida had the highest 2019 loss rate that was much higher than the other top states. Moreover, Florida's 2019 loss rate of $2.0 million per one million in population, for instance, was much greater than second place California with its rate of $813,000. New York had the third highest loss rate of $470,000 per one million in population followed by Washington of $429,000, and Ohio and Texas, with similar loss rates of $250,000 and $212,000, respectively.

In addition, Florida also had the highest victim rate of 138 victims per one million in population in 2019, followed by California with 49, and Washington with 46.

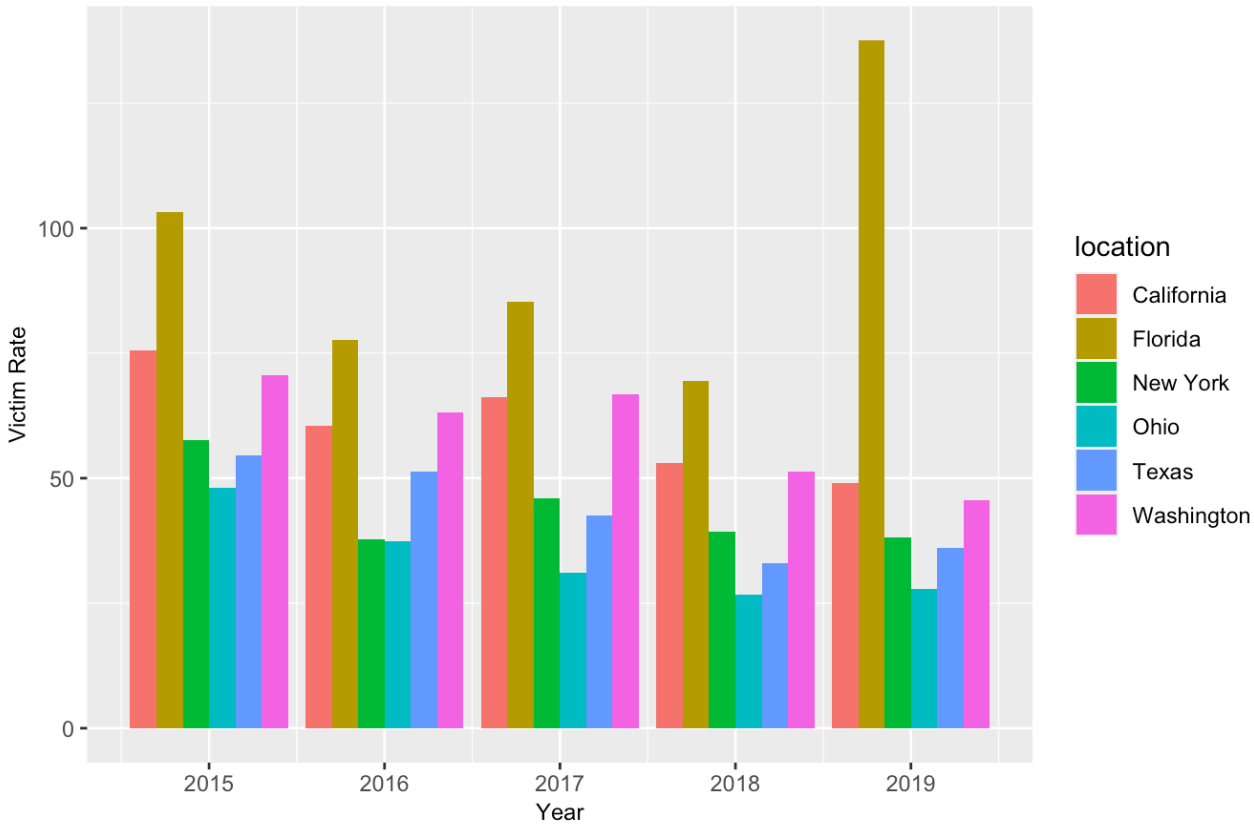
Identity Theft

Loss Rate (USD) per 1 Million Population



Identity Theft

Victim Rate per 1 Million Population

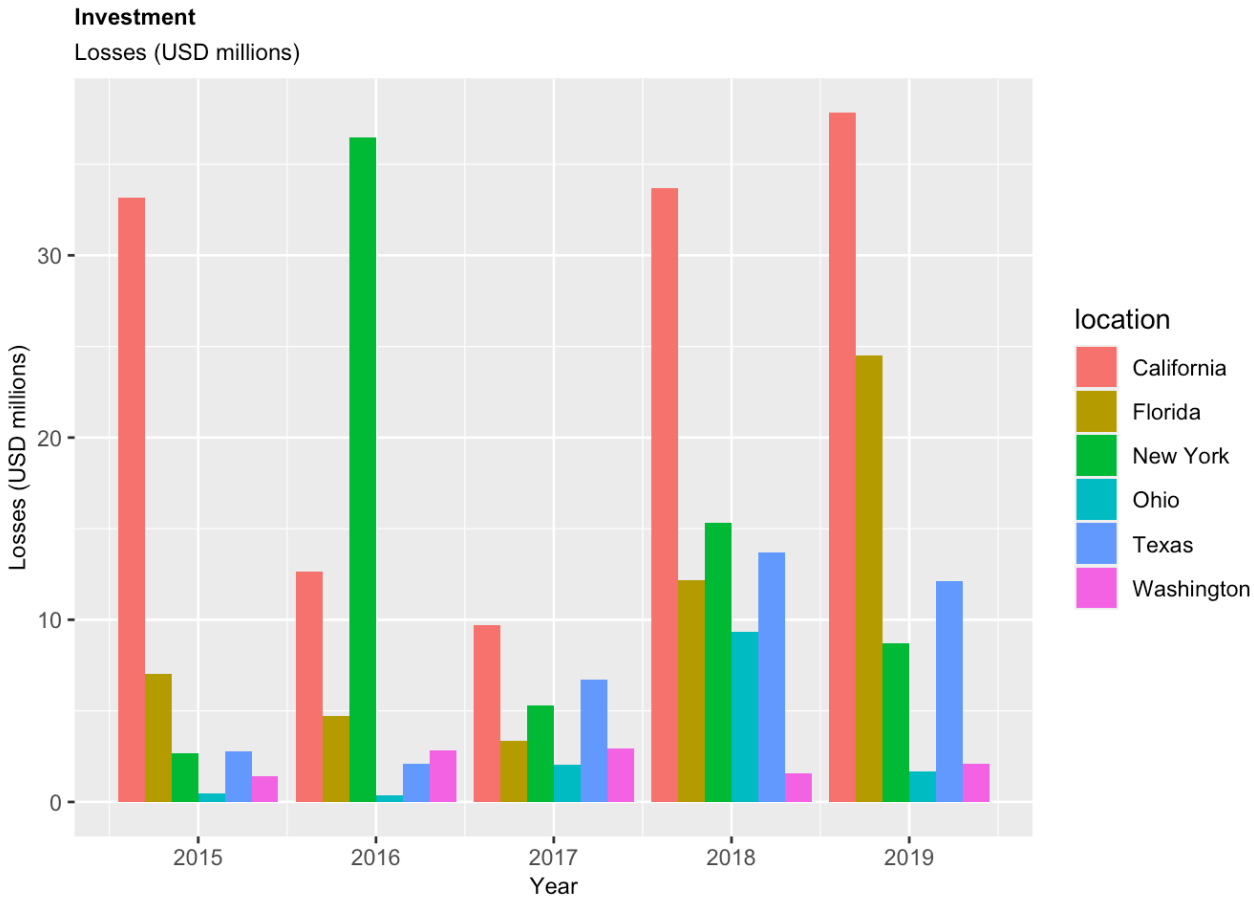


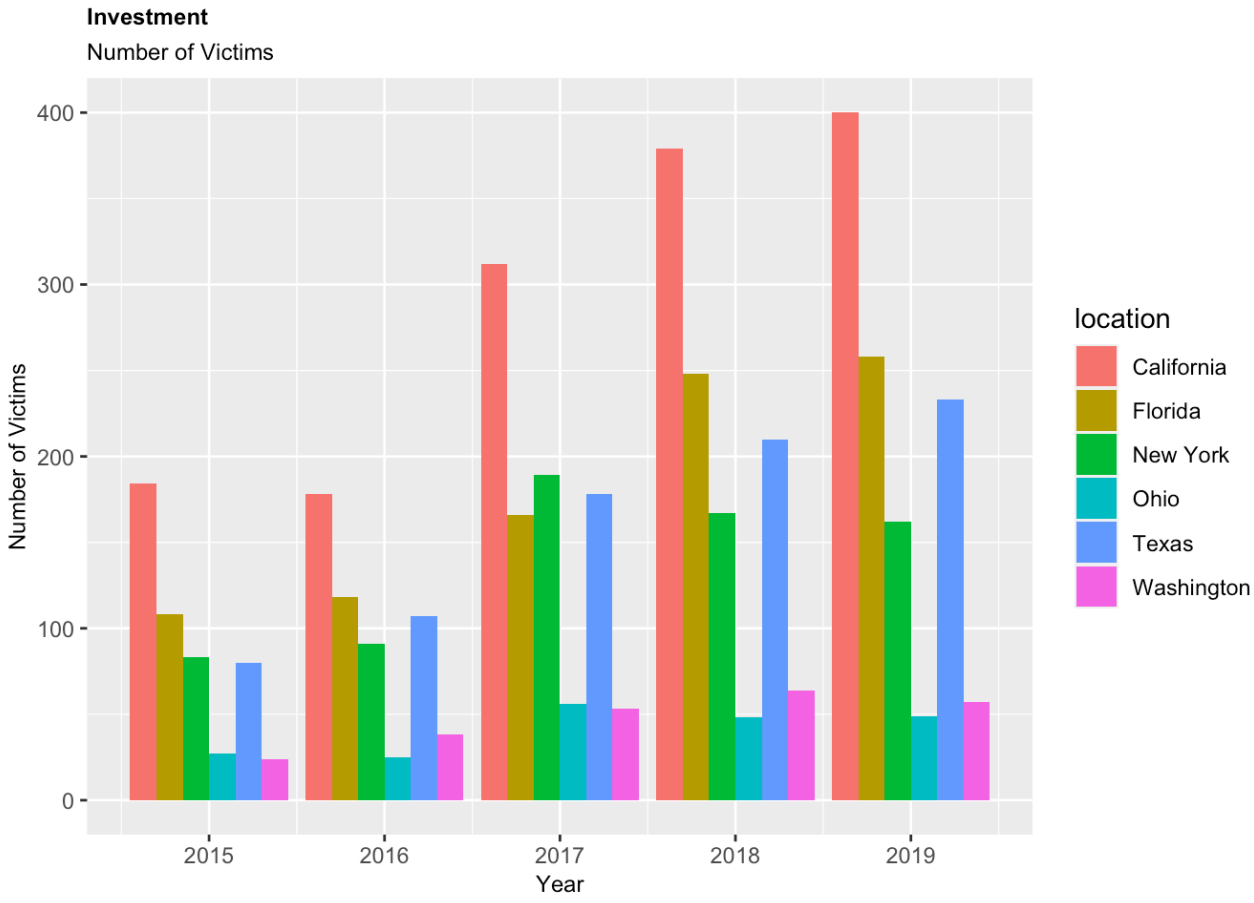
Overall, Identity Theft during 2019 increased in five of the six top states with a large spike in Florida. Victim numbers increased in Florida, Ohio, and Texas, but declined in California, Washington, and New York.

Investment fraud

Investment fraud is a white-collar crime where fraudsters lure investors, many times seniors, offering high returns if they make an investment. Online Investment fraud does not have a large numbers of victims but the average loss per victim can be very high. For instance, the amount of 2019 victim losses in Florida was $24.5 million on 258 victims.

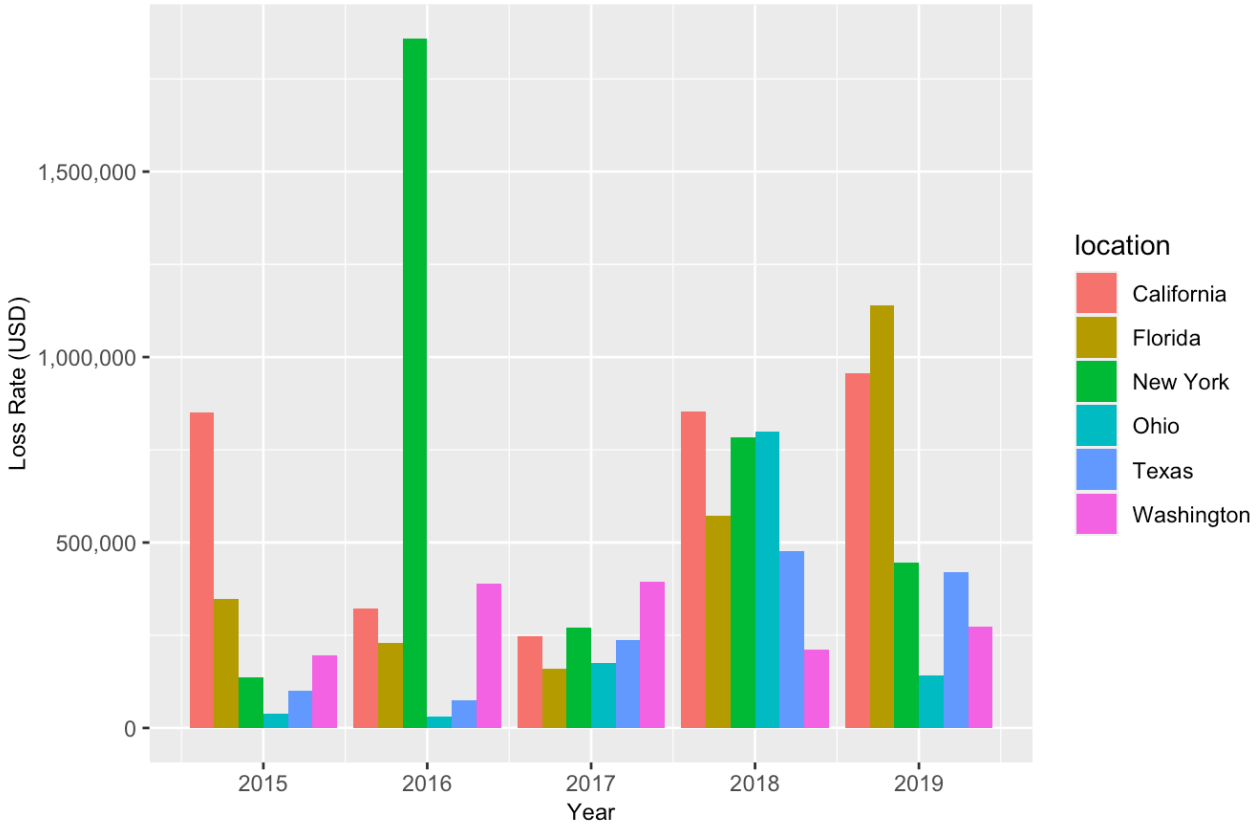
Although Florida's 2019 victim losses of $24.5 million are lower than California's $37.8 million (the highest among the top states), loss rates in Florida are the highest among the six top states. While California's 2019 loss rate was $957,000 per one million in population, Florida's rate was $1.1 million, making Florida where victims are most likely to lose more money to online investment fraud than in any other top state. In addition, victim losses in 2019 increased in Florida, California, and Washington, while decreasing in New York, Ohio, and Texas. Florida had the largest increase in victim losses among the top states with losses doubling from $12.2 million in 2018 to $24.5 million while the number of victims increased only 4% from 248 to 258. In California, losses increased 22% from $33.7 million in 2018 to $37.8 million in 2019 as the number of victims increased 6% from 379 to 400. In Washington, losses increased 31% from $1.6 million in 2018 to $2.1 million in 2019 but victims declined 11% from 64 to 57.


Investment
Losses (USD millions)
Losses (USD millions)
30
20
10
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


Investment
Number of Victims
Number of Victims
400
300
200
100
0
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington

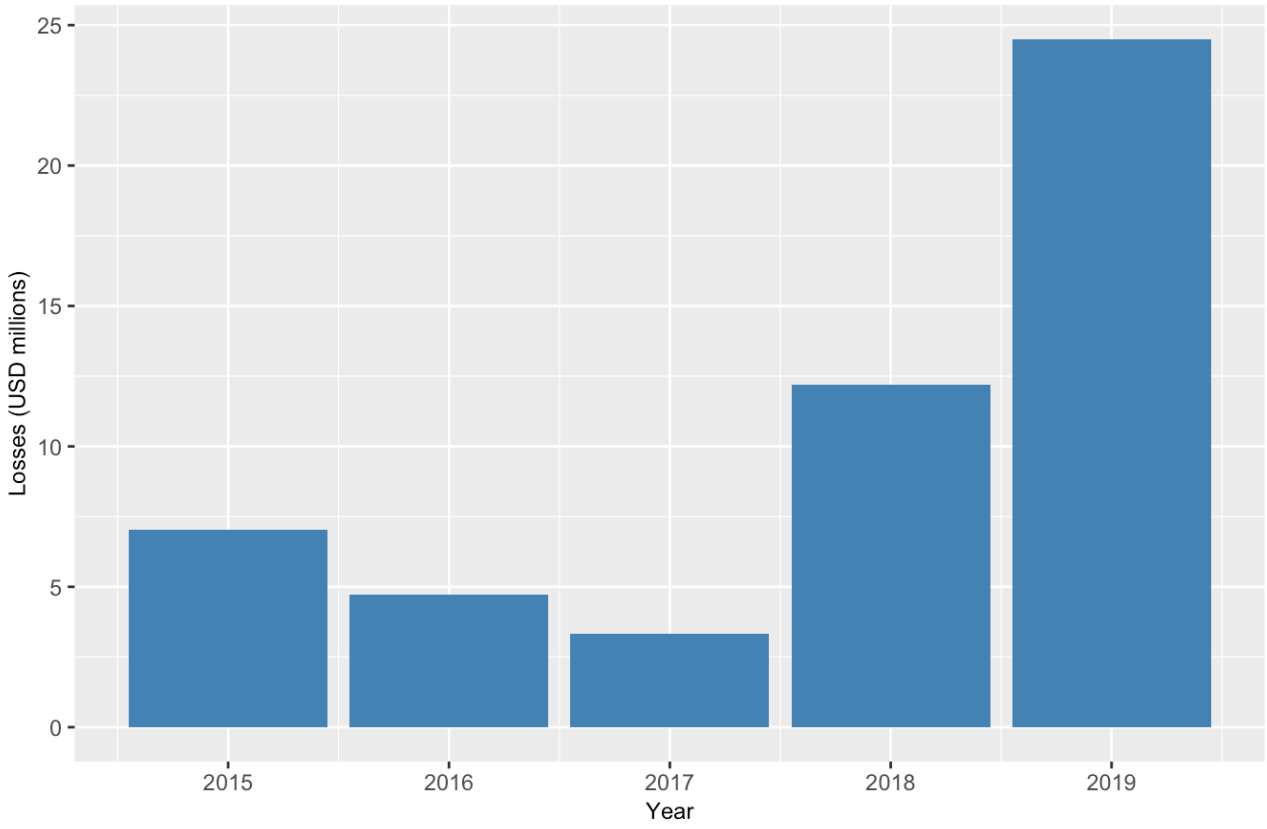
Investment

Loss Rate (USD) per 1 Million Population



Florida -- Investment

Losses (USD millions)



In contrast to the states with increases in victim losses during 2019, Ohio's losses declined sharply by 82%, from $9.3 million in 2018 to $1.7 million in 2019 with about the same the number of victims. New York had a 43% decline in losses from $15.3 million in 2018 to $8.7 million in 2019, and a 3% decline in number of victims. Texas also experienced a decline of 11% in losses from $13.7 million to $12.1 million but had an increase of 11% in the number of victims.

Overall, Investment fraud is an online crime with a disproportionate average loss per victim. In 2019, Investment fraud victim losses increased even more from the previous year. It continued to be a top crime in Florida. Among the six top states in 2019, three states had increases in victim losses and three had declines. On the number of victims, fluctuations in the top states were relatively small.

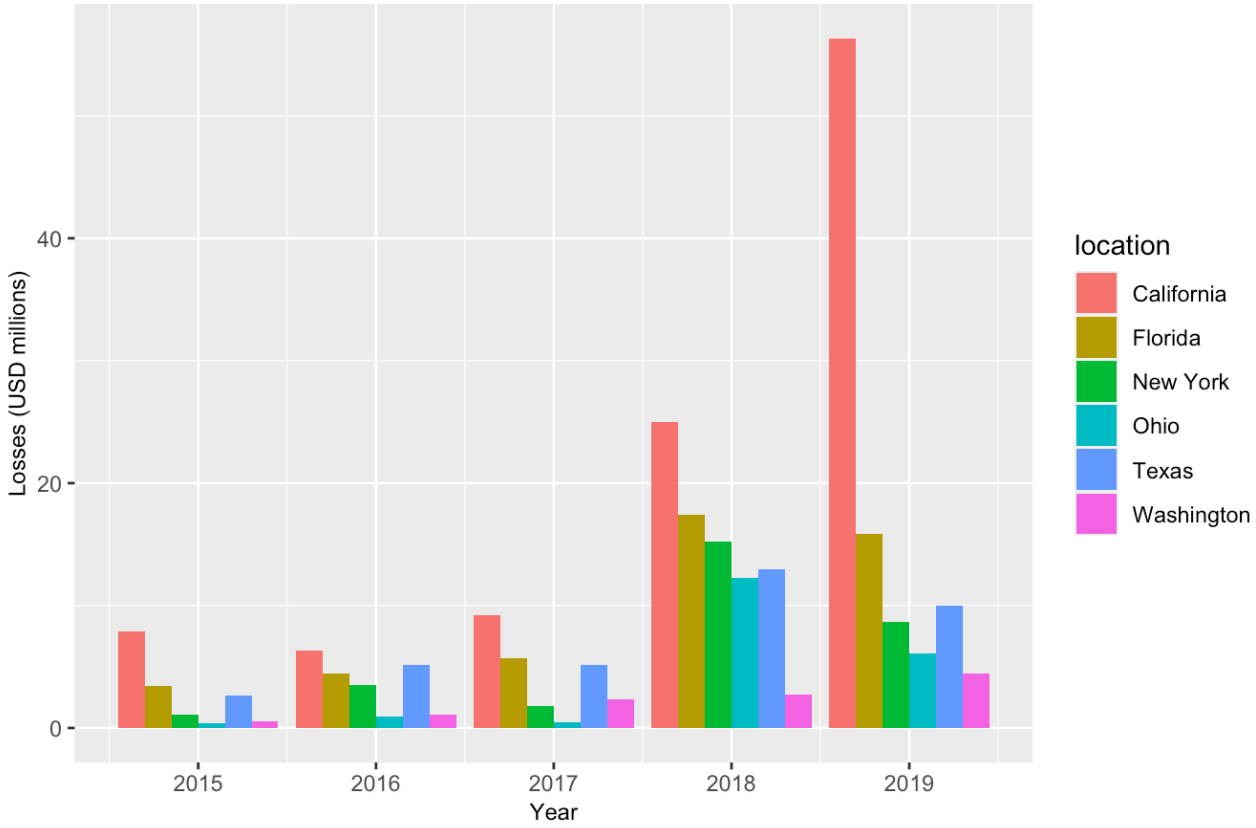
Real estate/ Rental

Real Estate/Rental fraud includes online real estate, rental, and timeshare scams. This scheme continued to be a popular online crime in 2019, especially in California where victim losses jumped to $56.3 million from $25.0 million in 2018, a 126% growth rate. Washington also had a significant increase in 2019, 62%, growing from $2.8 million in 2018 to $4.5 million in victim losses. Washington not only had the second highest percentage growth, but it also had the highest percentage increase in the number of victims among the top states.

Although victim losses in 2019 were relatively high in Florida, New York, Ohio, and Texas, they declined in these states from the prior year. Florida continued to have the second highest victim losses in the top states, after California, even as losses declined by 9%, from $17.5 million in 2018 to $15.9 million in 2019. In New York, a state with 1,282% growth in victim losses during 2018 its losses fell 43% in 2019 from $15.2 million in 2018 to $8.7 million.

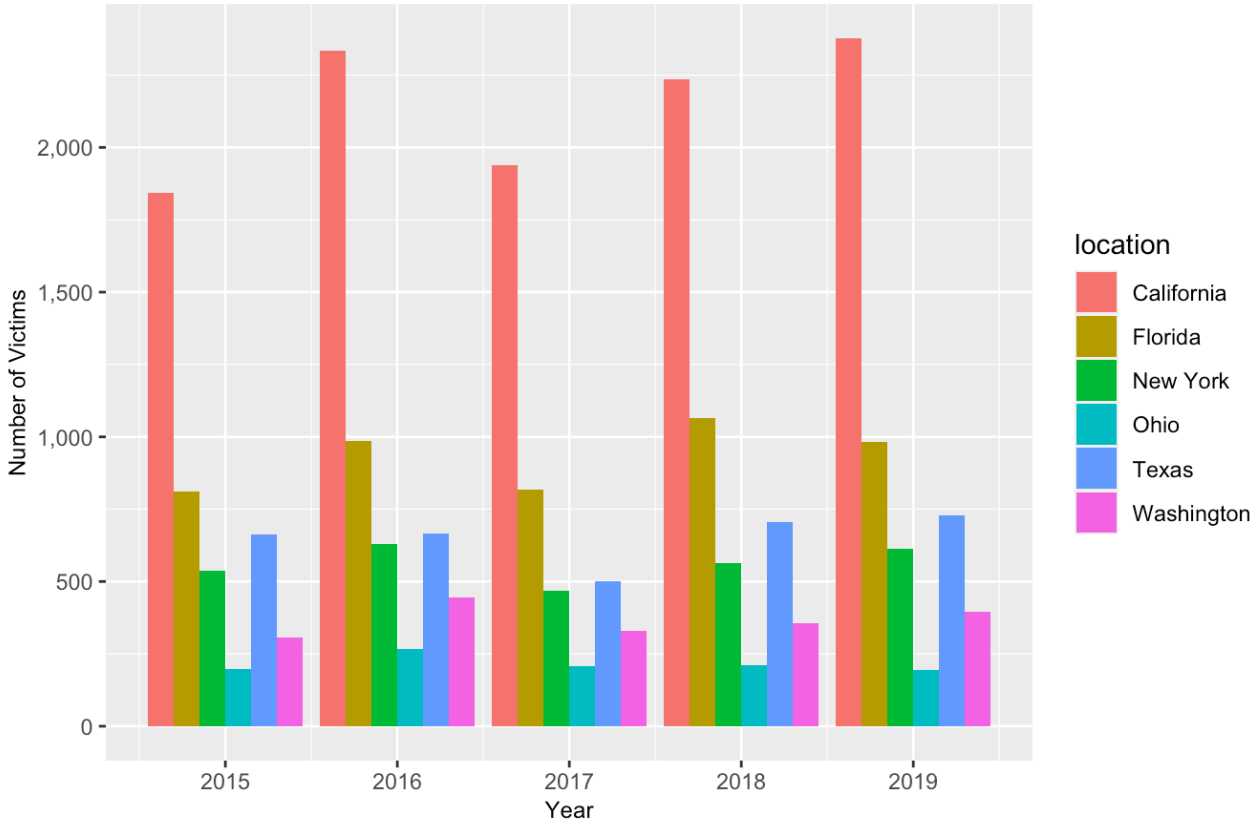
Real Estate/Rental

Losses (USD millions)



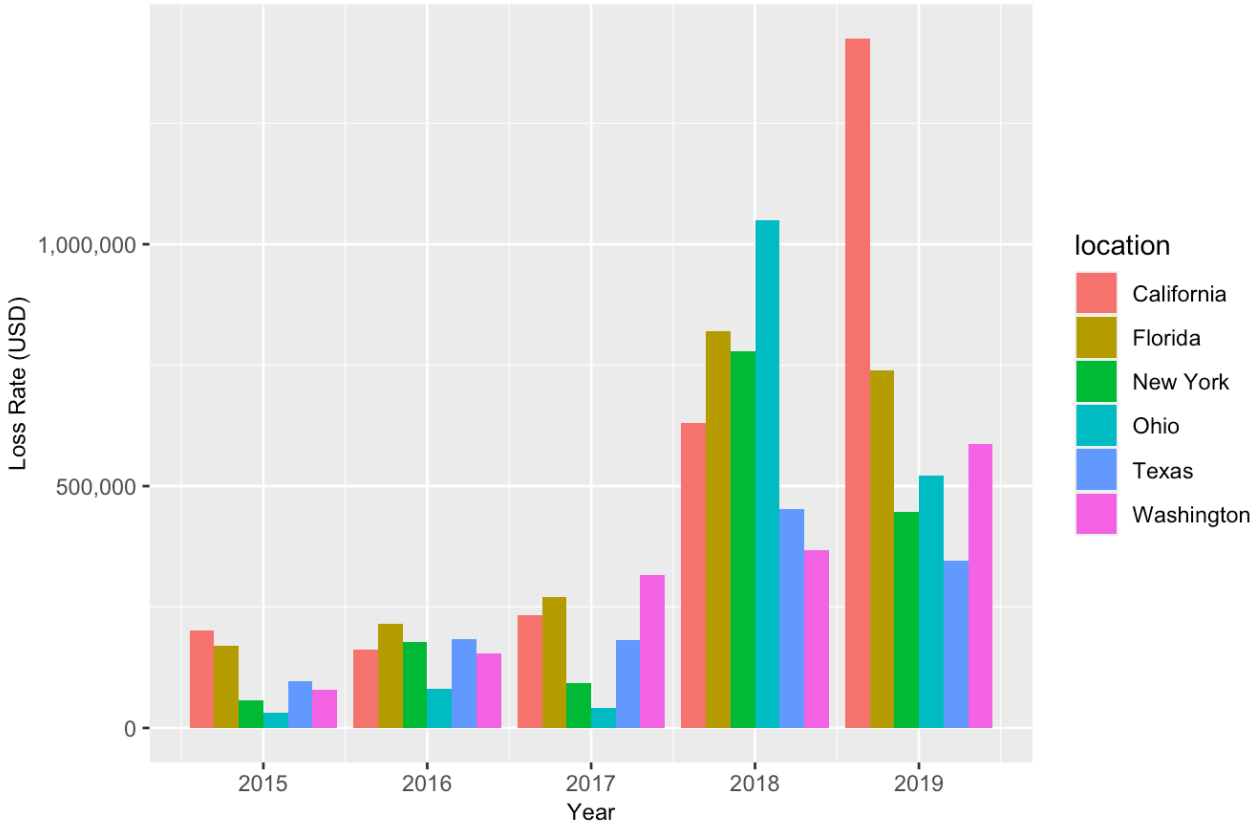
Real Estate/Rental

Number of Victims



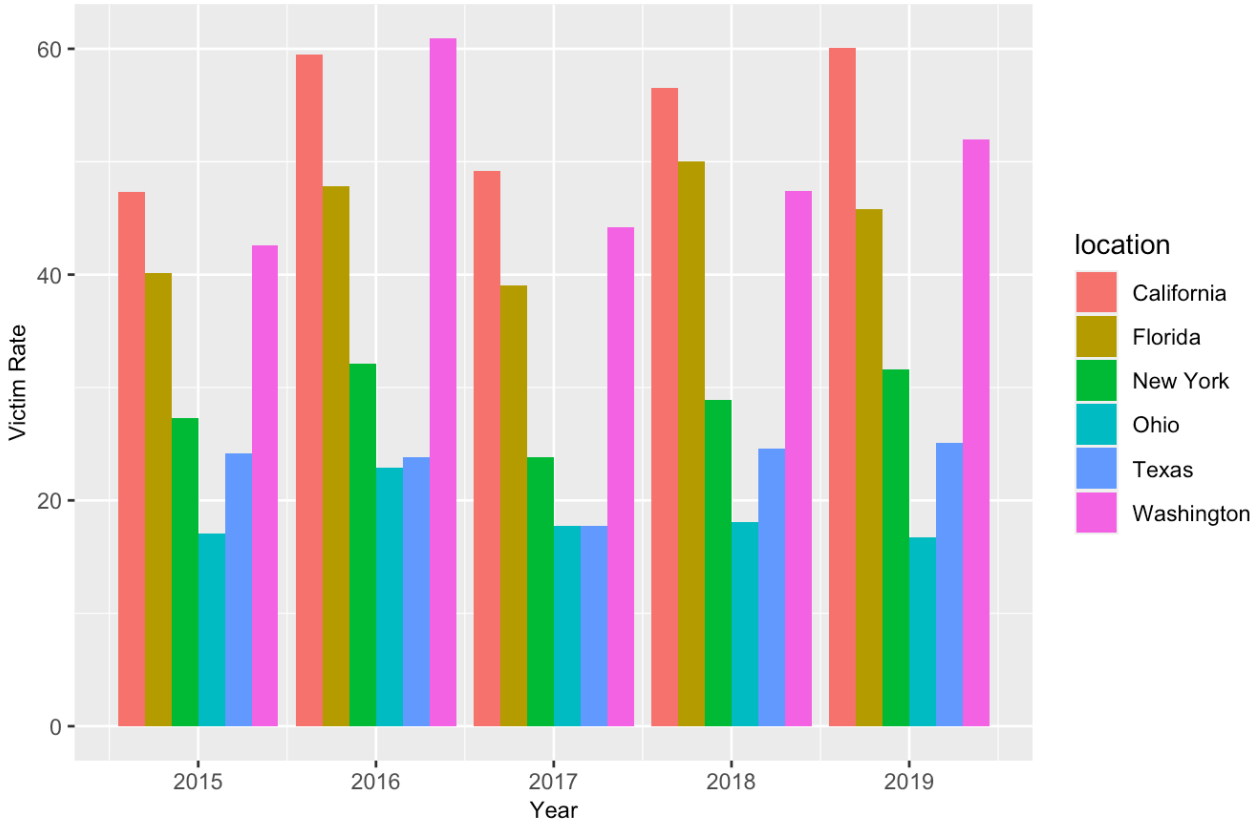
Real Estate/Rental

Loss Rate (USD) per 1 Million Population



Real Estate/Rental

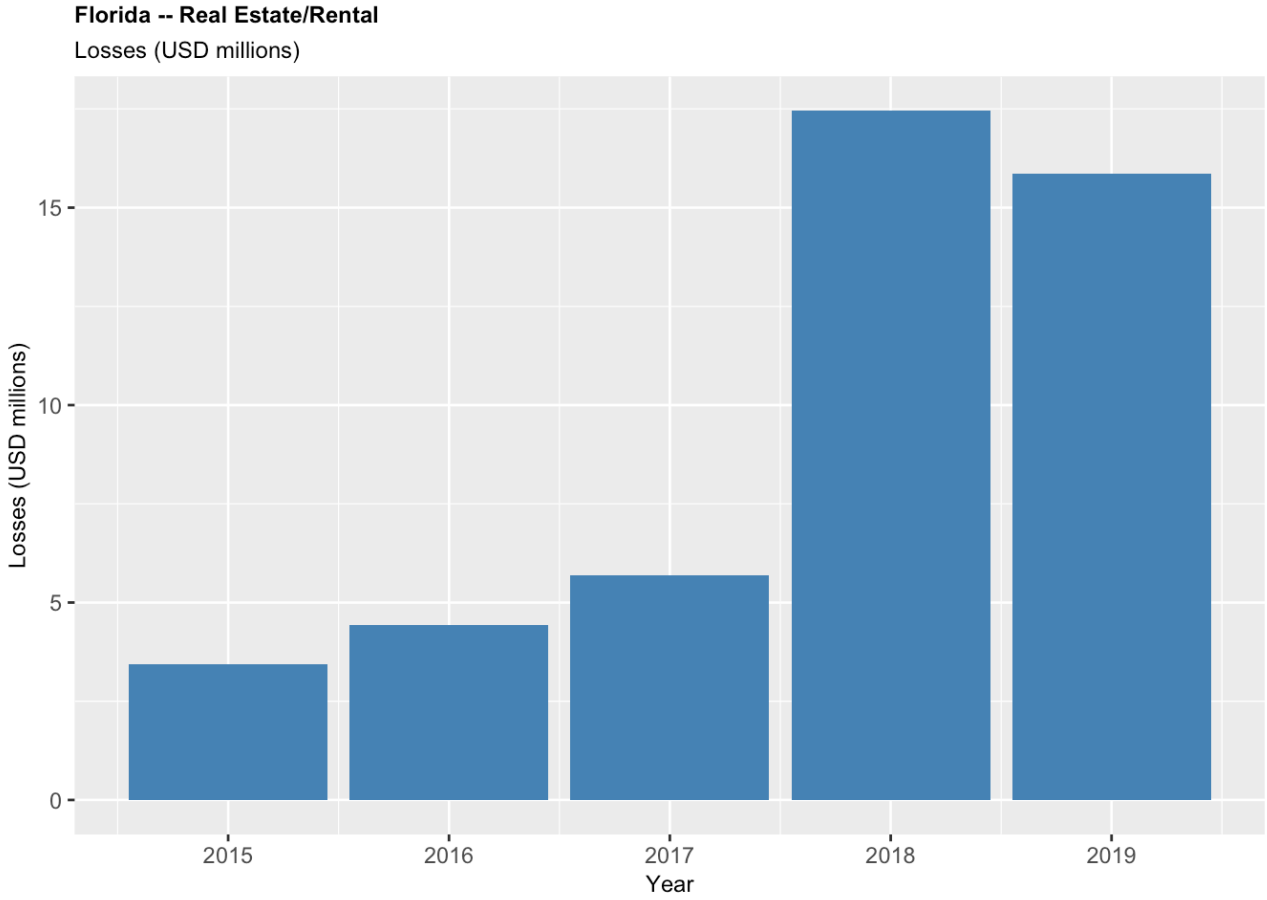
Victim Rate per 1 Million Population



In 2019, the number of victims changed relatively little overall from the previous year in the top states. Washington had the highest growth of 11% during 2019, followed by New York of 9%, California 6%, and Texas 3%. In contrast, Florida and Ohio had declines of 8%.

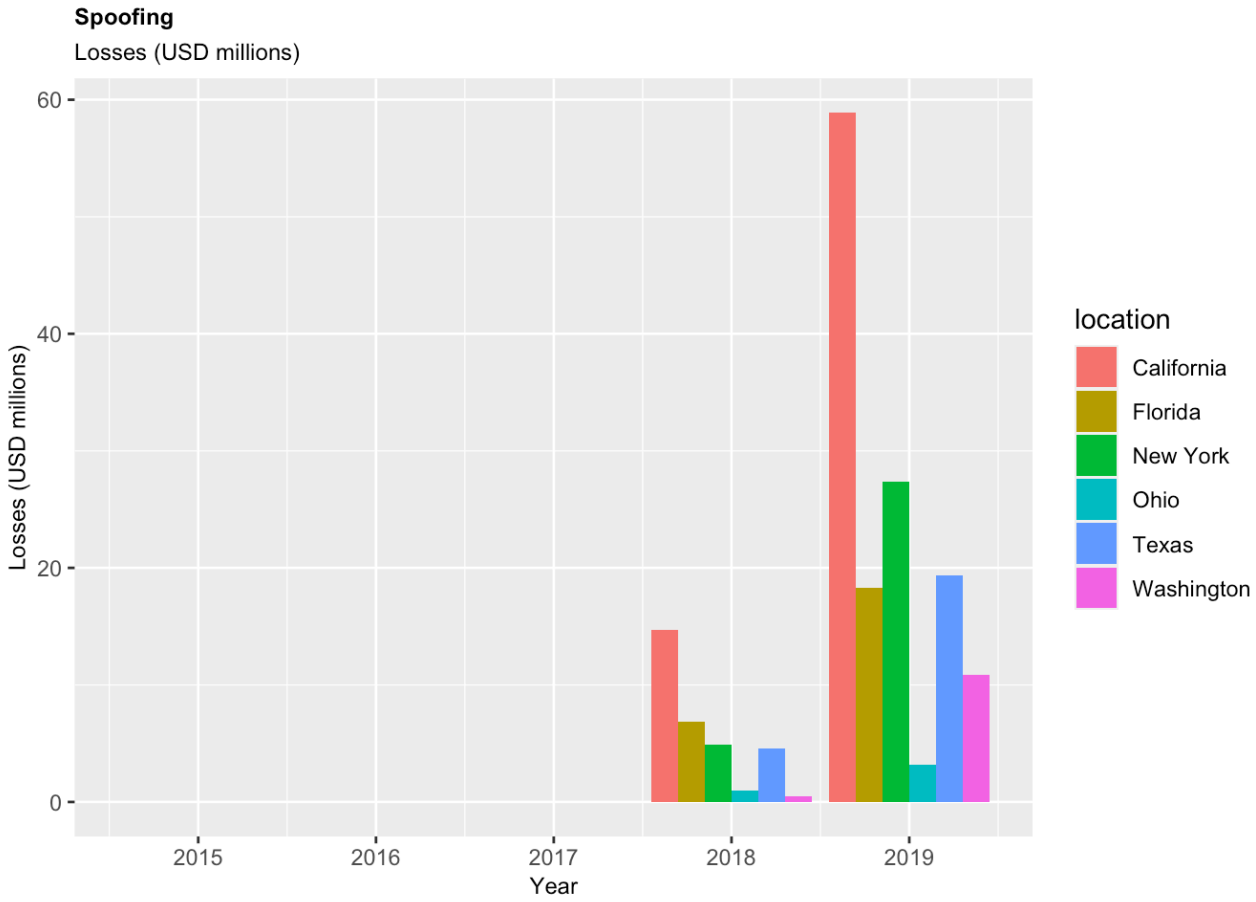
Victim rates showed that people in California were more likely to fall for this crime, followed by Washington and Florida. In addition, California had the highest victim loss rate of $1,425,000 per one million in population, followed by Florida with $739,000, and Washington with $586,000.

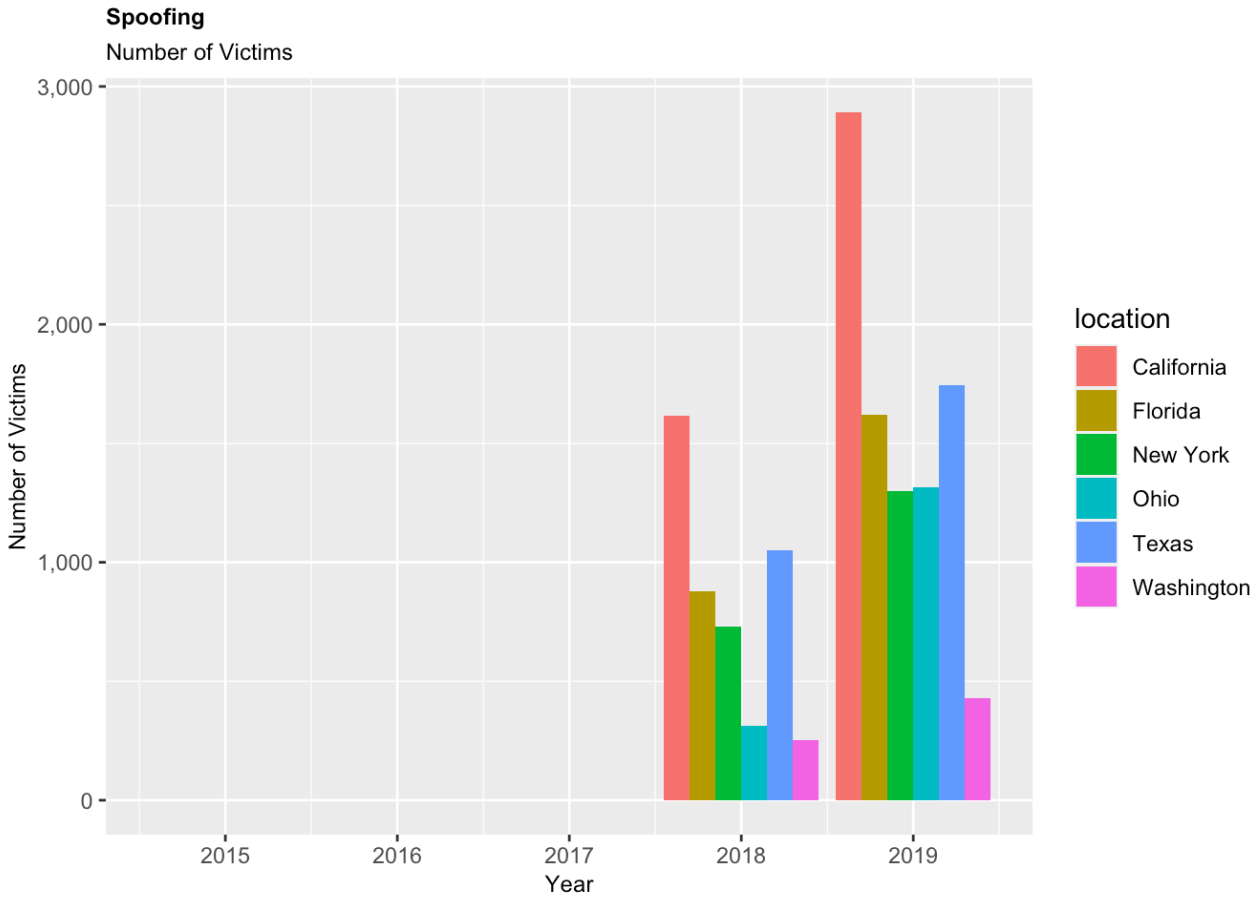
Overall, victim losses from Real Estate/Rental online crime was largest in California by a large margin as losses spiked in 2019, followed by Florida.



Spoofing

Spoofing is an online crime used as a tool to commit other kinds of online crimes. Generally, spoofing is done by falsifying email contact information making an email message appear to have been sent by a trustworthy source in order to fraudulently obtain sensitive information from a victim. FBI started classifying Spoofing as a separate category in 2018. No previous data are found in earlier FBI reports. Spoofing was the crime with the largest percentage increase in victim losses in the top states during 2019.


Spoofing
Losses (USD millions)
60
40
20
0
Losses (USD millions)
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington


Spoofing
Number of Victims
3,000
2,000
1,000
0
Number of Victims
2015
2016
2017
2018
2019
Year
location
California
Florida
New York
Ohio
Texas
Washington

Spoofing became a top crime in Washington in 2019 with the highest 2018 to 2019 increase in victim losses of 2,158% among the top states. Victim losses in Washington increased from $481,000 (0.8% of its total losses) in 2018 to $10.9 million (15.2% of total losses) in 2019.

Similarly, New York experienced a jump in its ratio of Spoofing losses to its total losses in 2019 where losses grew from $4.9 million (a ratio of 2.4%) in 2018 to $27.3 million (13.8%) in 2019. In absolute numbers, New York's victim losses increased 462% from 2018 to 2019.

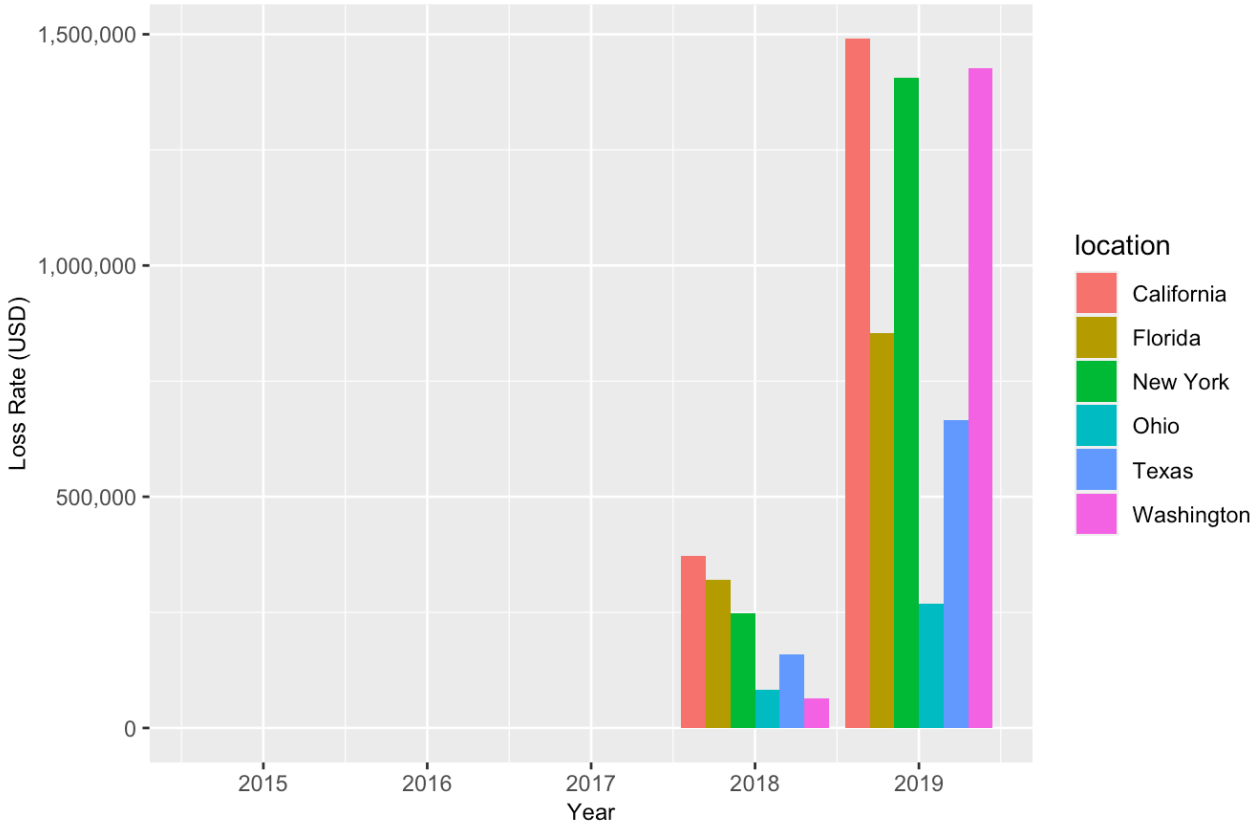
The state with the third highest victim growth rate is California, where victim losses increased 300% from $14.7 million in 2018 to $58.9 million in 2019. Spoofing losses were 3.3% of its total losses in 2018 and jumped to 10.3% in 2019.

Although victim losses to Spoofing in Florida were not as high as in California, Washington, and New York in 2019, its losses increased 169% from $6.8 million in 2018 to $18.3 million. In addition, Florida's Spoofing losses were 6.8% of all its online victim losses in 2019.

On the number of Spoofing victims in 2019 across the top states, California, Texas, and Florida had the most victims. New York and Ohio had victim numbers similar to each other, and Washington had the lowest number of victims of the six top states. In terms of growth in the number of victims from 2018 to 2019, Ohio had the highest growth of 323%, up from 311 victims in 2018 to 1,316 in 2019, and Florida, the second highest, with an 85% increase from 877 to 1,619.

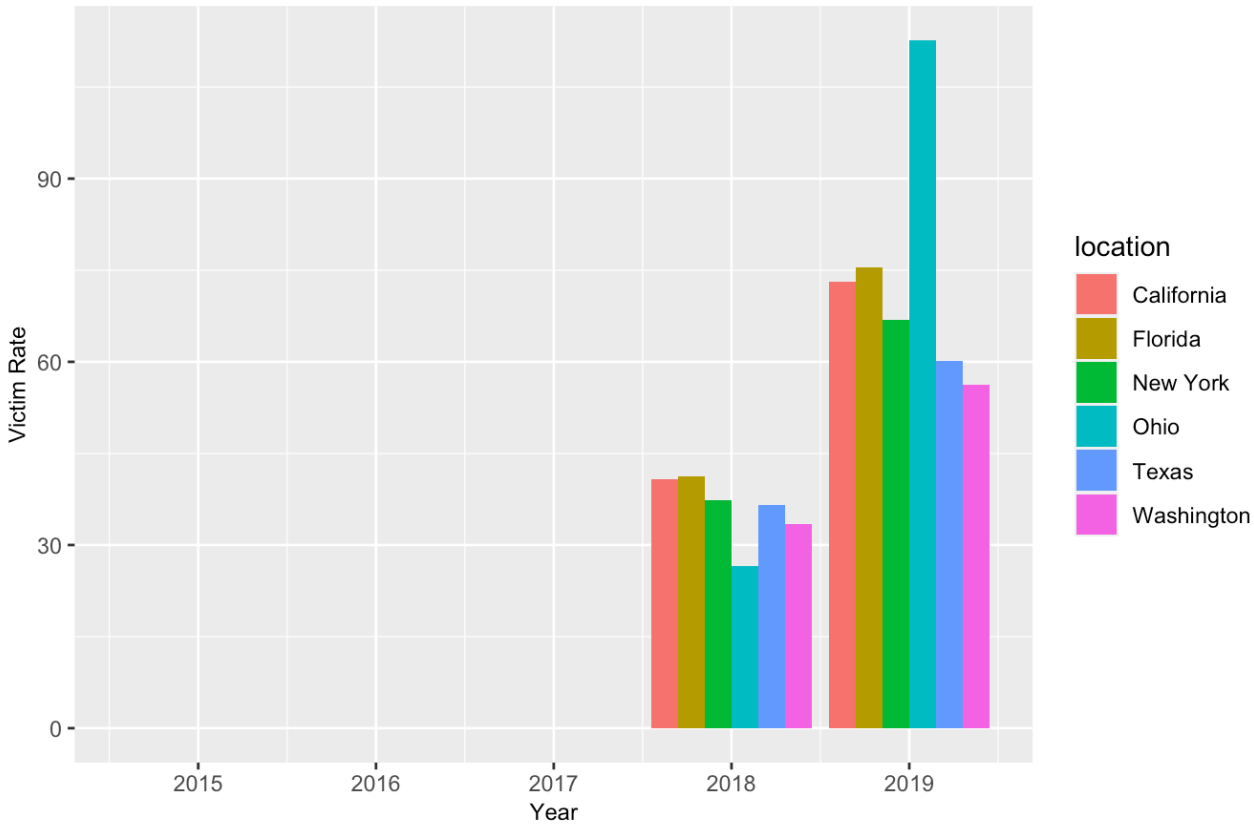
Spoofing

Loss Rate (USD) per 1 Million Population



Spoofing

Victim Rate per 1 Million Population



In terms of victim losses adjusted for population, California, Washington, and New York had the highest victim loss rates among the six top states in 2019. California had a loss rate of $1,490,000 per one million in population that was its third highest online crime after BEC and Confidence/Romance. It had the highest loss rate among the six top states in 2019. Washington had the highest growth in the loss rate of all the six top states during 2019 with $1,426,000 per one million in population, up from $64,000 in 2018. In New York, the 2019 loss rate jumped from $249,000 per one million in population in 2018 to $1,405,000 in 2019 making New York the state with the third highest loss rate. Texas, Ohio, and Florida also had increases in their 2019 loss rates, with Florida having lowest growth of 166% from $320,000 per one million in population in 2018 to $854,000 in 2019.

Victim rates were similar in all the top states during 2018. Although all these states had increases in 2019 victim rates, Ohio's rate spiked and the state became the leader with the highest victim rate of 113 per one million in population. The other five top states continued to have 2019 victim rates similar to each other. Overall, people in Ohio seemed to be more likely to fall for an online Spoofing crime than people in the other top states.

Overall, victim losses from Spoofing increased significantly in 2019 especially in Washington, New York, and California with losses surpassing $1.4 million per one million in population. In terms of the number of victims, in 2019 people were much more likely to fall for Spoofing crime in Ohio than in any other top state.

Conclusion

This report is based on FBI internet crime statistics from 2015 through 2019. FBI collects data from victims reporting alleged internet crimes. FBI's Internet Crime Complaint Center (IC3) receives victim complaints and classifies them by number of victims and loss amounts according to location and crime types. Almost certainly, the actual internet crime victim losses and number of victims are larger than what is reported to FBI.

Although this report analyzes data from 2015 to 2019, we emphasize 2018 to 2019 trends. We discuss crimes in six top states: This year we identified six top states: California, Florida, New York, Ohio, Texas, and Washington. These states had the largest 2019 online fraud victim losses or number of victims. Ohio and Washington were added in our 2019 report as they experienced higher losses or number of victims while North Carolina and Virginia dropped out.

In 2019, California still has the largest online fraud victim losses and number of victims followed by Florida. Ohio, Texas, New York, and Washington follow. Victim losses adjusted for population show that Ohio had the highest per capita victim losses that was much higher than the other five top states. Washington still had the highest number of victims per capita in 2019.

Business Email Compromise/Email Account Compromise (BEC/EAC) continued to be the top internet crime in 2019. Following BEC/EAC was Confidence Fraud/Romance and Spoofing.

Among the top states, BEC/EAC accounted for about 30% to 90% of all victim losses in 2019 and has grown rapidly from 2015 through 2019. Confidence Fraud/Romance was the second largest online crime during 2019 in California, Florida, New York, Texas, and Washington. In Ohio, it was third highest after BEC/EAC and Real Estate/Rental frauds.

Other online crimes identified to have the highest victim losses after BEC/EAC and Confidence Fraud/Romance were Real Estate/Rental in California and Ohio, Identity Theft in Florida, Government Impersonation in New York, and Spoofing in Texas and Washington. In addition, Extortion and Investment fraud were also online crimes with high victim losses in the six top states during 2019.

In 2019, online Credit Card fraud experienced a decline in victim losses in four of the six top states but had a large increase in New York. Corporate Data Breach, identified as a top crime in our 2018 report, declined in 2019 between 40% and 90% in the top states with the exception of Washington where victim losses increased in 2019.

Information in this report should be useful to the public, law enforcement agencies, other government agencies, and policy makers. Increasing public awareness may be the most effective way of mitigating online crime since it most likely originates outside the United States, beyond the reach of U.S. law enforcement. Foreign sources of internet crimes on U.S. residents and businesses make it challenging for whether internet crime levels can be reduced as the public becomes more connected and dependent on the internet.

Appendix

Descriptions of Internet Crime Types

The glossary terms herein are taken from FBI's 2019 Internet Crime Report.

Advanced Fee: In advanced fee schemes, the perpetrator informs a victim that the victim has qualified for a large financial loan or has won a large financial award, but must first pay the perpetrator taxes or fees in order to access the loan or award. The victim pays the advance fee, but never receives the promised money.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that 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 lawsuits are any disputes formally submitted to a court that is not criminal.

Confidence Fraud/Romance: A perpetrator deceives a victim into believing the perpetrator and the victim have a trust relationship, whether family, friendly or romantic. As a result of that belief, the victim is persuaded to send money, personal and financial information, or items of value to the perpetrator or to launder money on behalf of the perpetrator. Some variations of this scheme are romance/dating scams or the grandparent scam.

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 fraud committed using a credit card or any similar payment mechanism 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 service with multiple requests, slowing down or interrupting service.

Employment: Individuals believe they are legitimately employed, and lose 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, usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, or stolen health information, or may involve medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums or social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The theft and illegal use of others' ideas, inventions, and creative expressions, to include everything from trade secrets and proprietary products to parts, movies, music, and software.

Identity Theft/Account Takeover: Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud. Account Takeover is when a perpetrator obtains account information to perpetrate fraud on existing accounts.

Investment: A 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. Variations of this scam include retirement schemes, Ponzi schemes and pyramid schemes.

Lottery/Sweepstakes/Inheritance: Individuals are contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative and are asked to pay a tax or fee in order to receive their award.

Malware/Scareware/Virus: Software or code intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds.

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.

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak or spill of personal data that is released from a secure location to an untrusted environment. It may also refer to 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: 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 purchased through fraudulent means and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Fraud involving real estate, 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. Spoofing is 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: Attempts to gain access to a victim's electronic device by falsely claiming to offer tech support, usually for a well-known company. Scammer asks for remote access to the victim's device to cleanup viruses or malware or to facilitate a refund for prior support services.

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.

---

1. Federal Bureau of Investigation FBI, Internet Crime Complaint Center IC3. (Nd). *2019 Internet Crime Report*, 20. Retrieved February 2020, from https://pdf.ic3.gov/2019_IC3Report.pdf (https://pdf.ic3.gov/2019_IC3Report.pdf)↩
2. Ibid, 20.↩
3. Ibid.↩
4. Ibid. Filing a Complaint with the IC3. Retrieved June 19, 2020 from https://www.ic3.gov/default.aspx (https://www.ic3.gov/default.aspx)↩
5. Ibid.↩

© (https://a.cms.omniupdate.com/11/?skin=fau&account=FAUCOB&site=business&action=de&path=/images/business/centers/center-for-forensic-accounting/files/fbi_analysis_2019.html)