North Carolina Security Breach Report 2017

Attorney General Josh Stein
North Carolina Department of Justice

January 2018

Executive Summary

This report provides a summary and discussion of the 1,022 data breaches reported to the North Carolina Department of Justice (NCDOJ) between January 1, 2017 and December 31, 2017. Under North Carolina law, businesses and state and local governments are required to report all security breaches to the Attorney General's Office. Since this requirement became law in 2005, organizations have reported 4,945 security breaches affecting more than 14.2 million North Carolinians.

Highlighted findings:

- Hacking breaches accounted for 50% of all data breaches in North Carolina in 2017.
- Since 2006, reports of hacking have increased by more than 3,500%.
- Phishing scams made up 24% of all breaches in 2017, up from 1.76% in 2015.
- Accidental release and display breaches have steadily declined since 2013; they accounted for only 13% of total breaches in 2017.
- Last year, more than 5.3 million North Carolinians are estimated to have been affected by data breaches.

Background

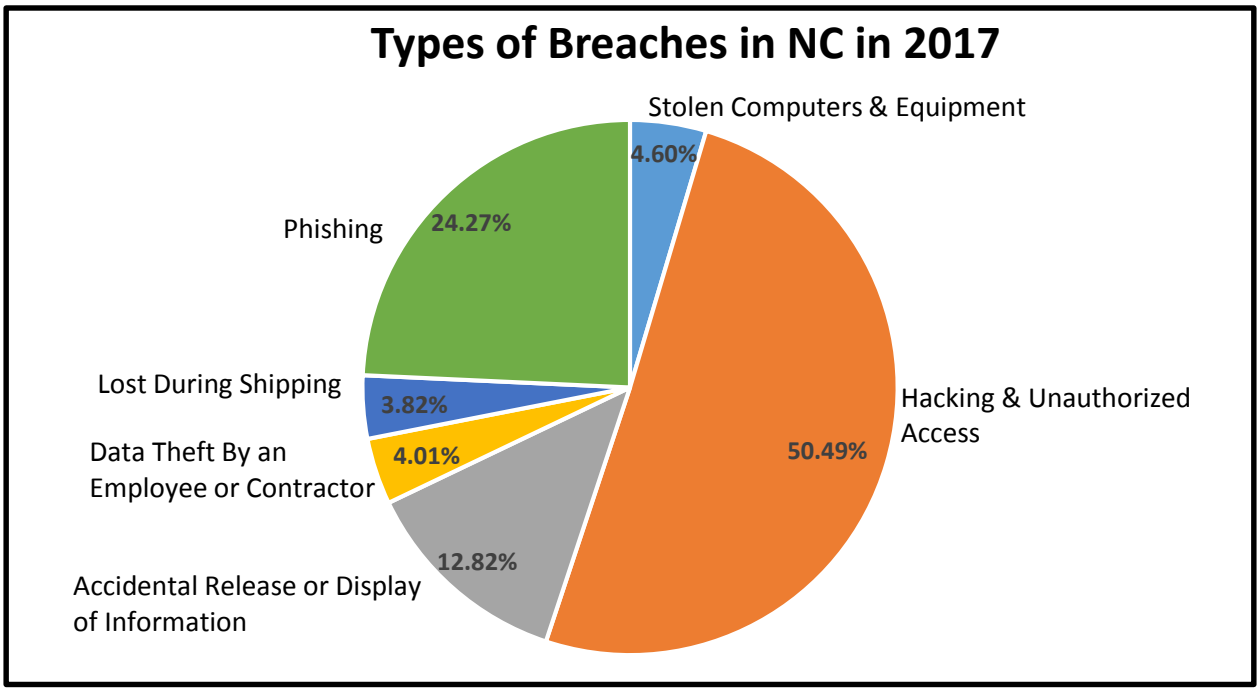
Whether directly or indirectly, North Carolinians increasing rely on computer networks for storing and sharing personal information. While greater access to technology has clear benefits, it also means more people are at risk of becoming a victim of cybercrime. This year, the national credit bureau Equifax experienced the most significant security breach in American history. Hackers accessed the private information of an estimated 5 million North Carolinians. This information included full names, dates of birth, Social Security numbers and driver license numbers.

Data security is critical to protecting North Carolinians from identify theft and financial fraud. Companies that store personal information about consumers must take responsibility for securing that data. Breaches are not only an invasion of consumer's privacy, but they can also risk the security and economic wellbeing of affected individuals.

Attorney General Stein has taken action on behalf of the many North Carolina consumers affected by data breaches this year. He is taking a lead role in an investigation into Equifax conducted with a bipartisan group of 48 attorneys general from across the nation. In addition, he has contacted Equifax to demand more information about how this breach occurred and what the company is doing to protect affected consumers. He has also written to the other two national credit bureaus – Experian and TransUnion – seeking information about their processes and how they plan to protect individual consumers' private information going forward.

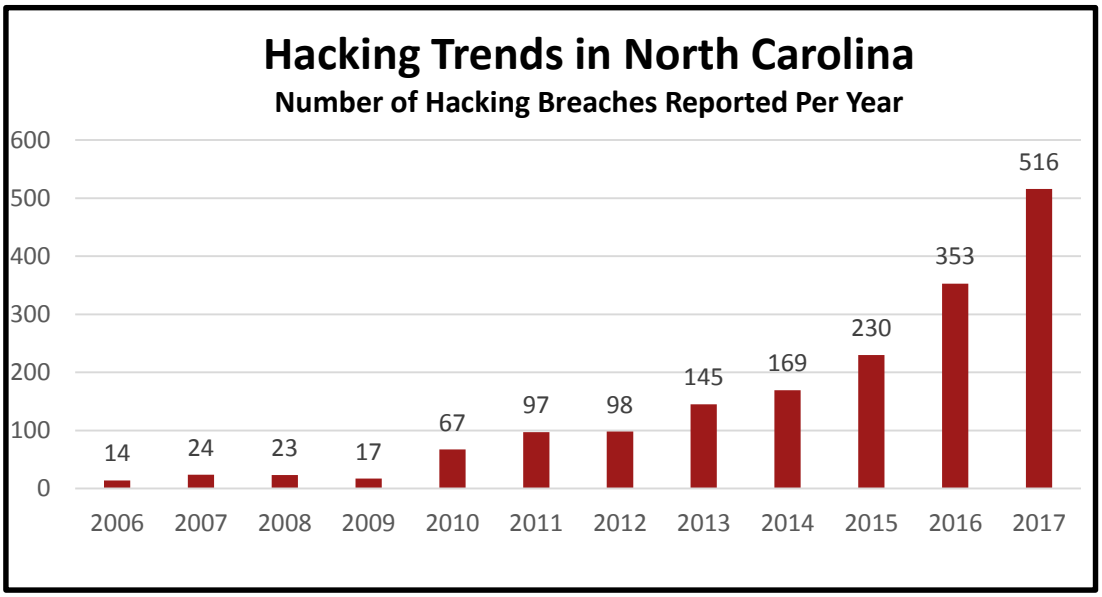
The Equifax breach is an example of just one of many types of security breaches. Data can be exposed from online breaches in computer systems or from physical breaches of lost or stolen equipment. Stolen information may range from medical records to retail credit card numbers. Breaches can impact any industry or individual.

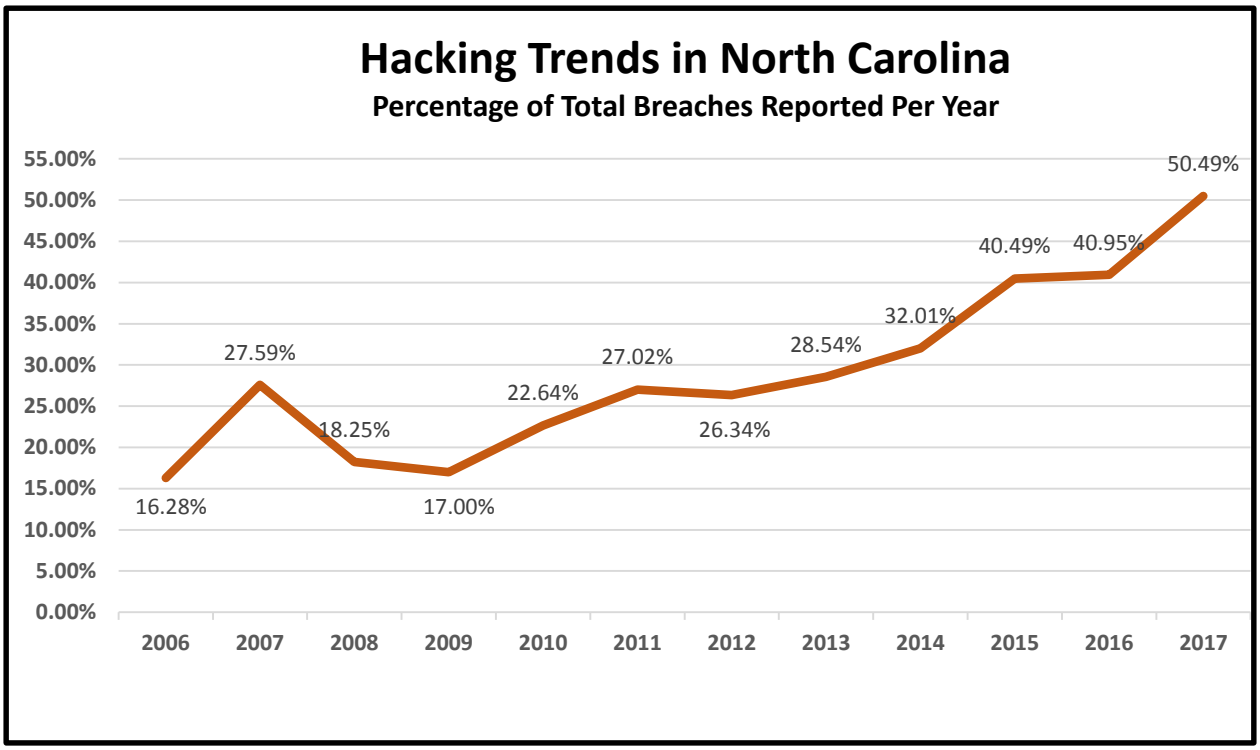
Data Breaches in North Carolina



Hacking and Unauthorized Access

By finding and exploiting weaknesses in a computer system, hackers can gain unauthorized access to information stored electronically. Many companies store private information about consumers on internal databases. Hackers target companies – especially those with financial information, such as Equifax – to access these large stores of data. They steal information that can be used to commit identify theft and financial fraud. NCDOJ received 516 reports of hacking during 2017. The number of hacking breaches in 2017 represents a 3,586% increase from the reports of hacking in 2006. Hacking breaches now make up approximately half of all breaches reported in North Carolina.





Protect Yourself From Hackers

Never share personal financial information by email or text message, even with someone you know and trust. Email and texts can be vulnerable to hackers.

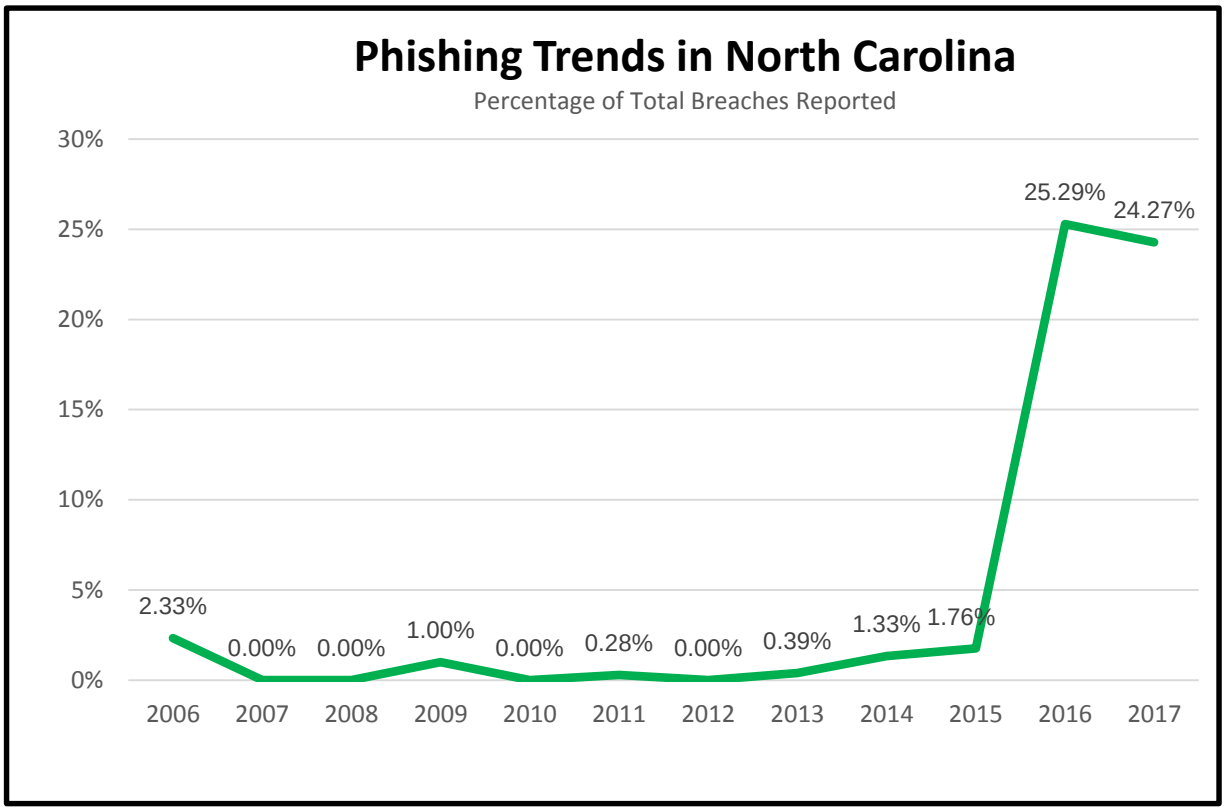
If you need to share information with a legitimate company, use a secure website. Look for a lock icon on the website and a URL that starts with "https." Use antivirus and firewall software on your computer.

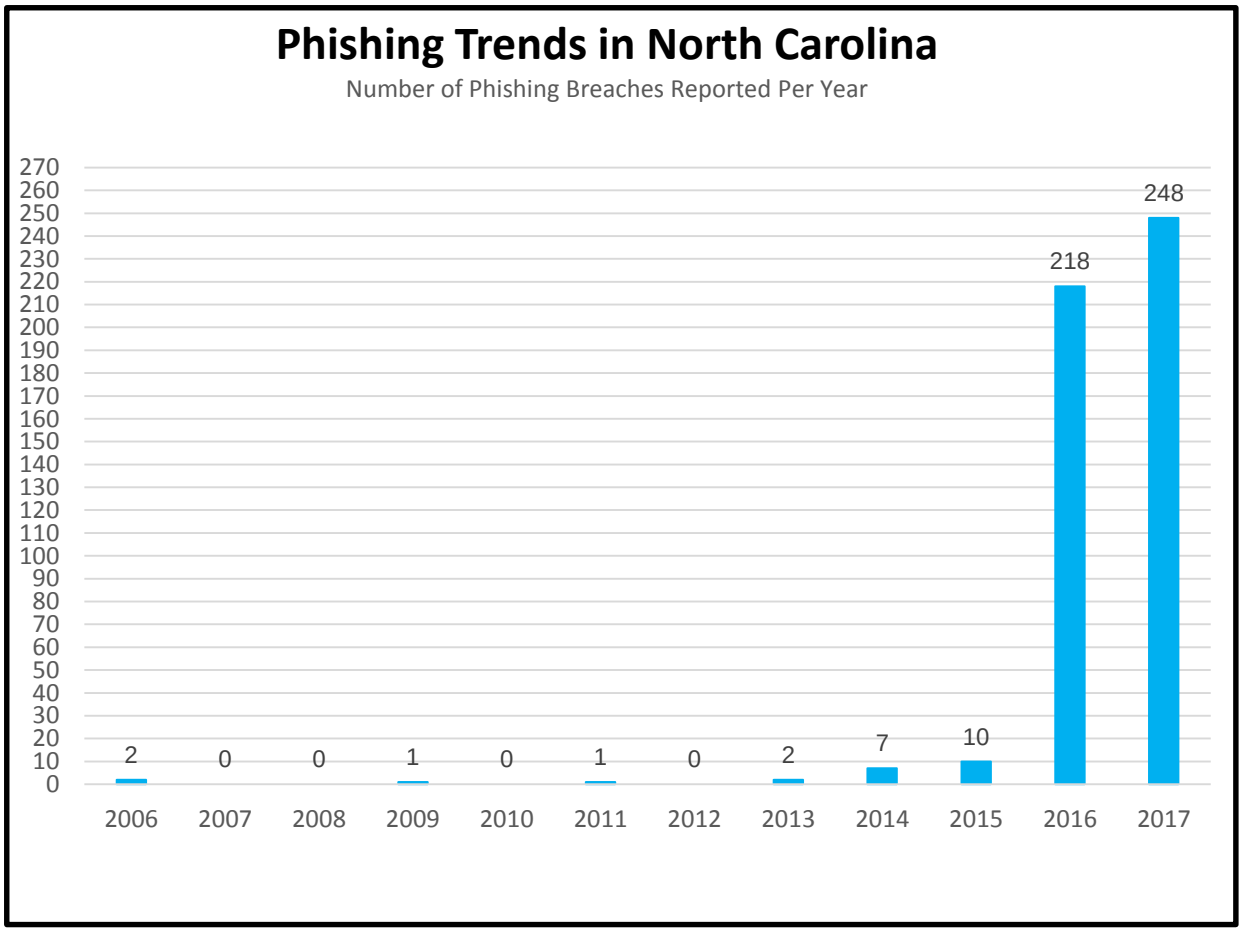
If you suspect hacking or email tampering, report it to your local law enforcement department.

Phishing

Scammers try to steal login credentials or personal information by sending phony emails or text messages that appear to come from legitimate organizations. These messages may ask for sensitive information such as social security numbers or bank account numbers. The message may ask for login credentials to computer systems or email accounts where personal information is often stored.

Last year NCDOJ received 248 reports of successful phishing scam campaigns. Between 2015 and 2017, reports of phishing increased by 2,380%.


Phishing Trends in North Carolina
Percentage of Total Breaches Reported
30%
25%
20%
15%
10%
5%
0%
2.33%
0.00%
0.00%
1.00%
0.00%
0.28%
0.00%
0.39%
1.33%
1.76%
25.29%
24.27%
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017


Phishing Trends in North Carolina
Number of Phishing Breaches Reported Per Year
270
260
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
2
0
0
1
0
1
0
2
7
10
218
248
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

Protect Yourself From Phishing

Beware of emails or text messages that ask for personal information such as Social Security number or bank account number. Scammers may use recognizable logos or link to a website designed to imitate a real website. Don't reply to the message or click on any links. Legitimate companies will not ask for personal information this way. In general, never open any attachments or download files sent by email from people you don't know.

If you see phishing, report it. Tell the real business or organization that is being mimicked about the scam so they can warn their customers. Forward the entire email to the Federal Trade Commission at spam@uce.gov.

If you do respond to a phishing email, contact your bank and your credit card company immediately. If you think you may be a victim of identity theft, contact NCDOJ for help at ncdoj.gov or 1-877-5-NO-SCAM.

Accidental Release or Display

Employee errors can be the cause of security breaches by accidental release. This type of breach can take a variety of forms: a staff member emails a spreadsheet to the wrong contact; a company fails to put information behind a firewall; a medical professional hands patient information to the wrong person. It can also occur when a document is mailed to the wrong address or when a mailing shows sensitive information in the address window of the envelope.

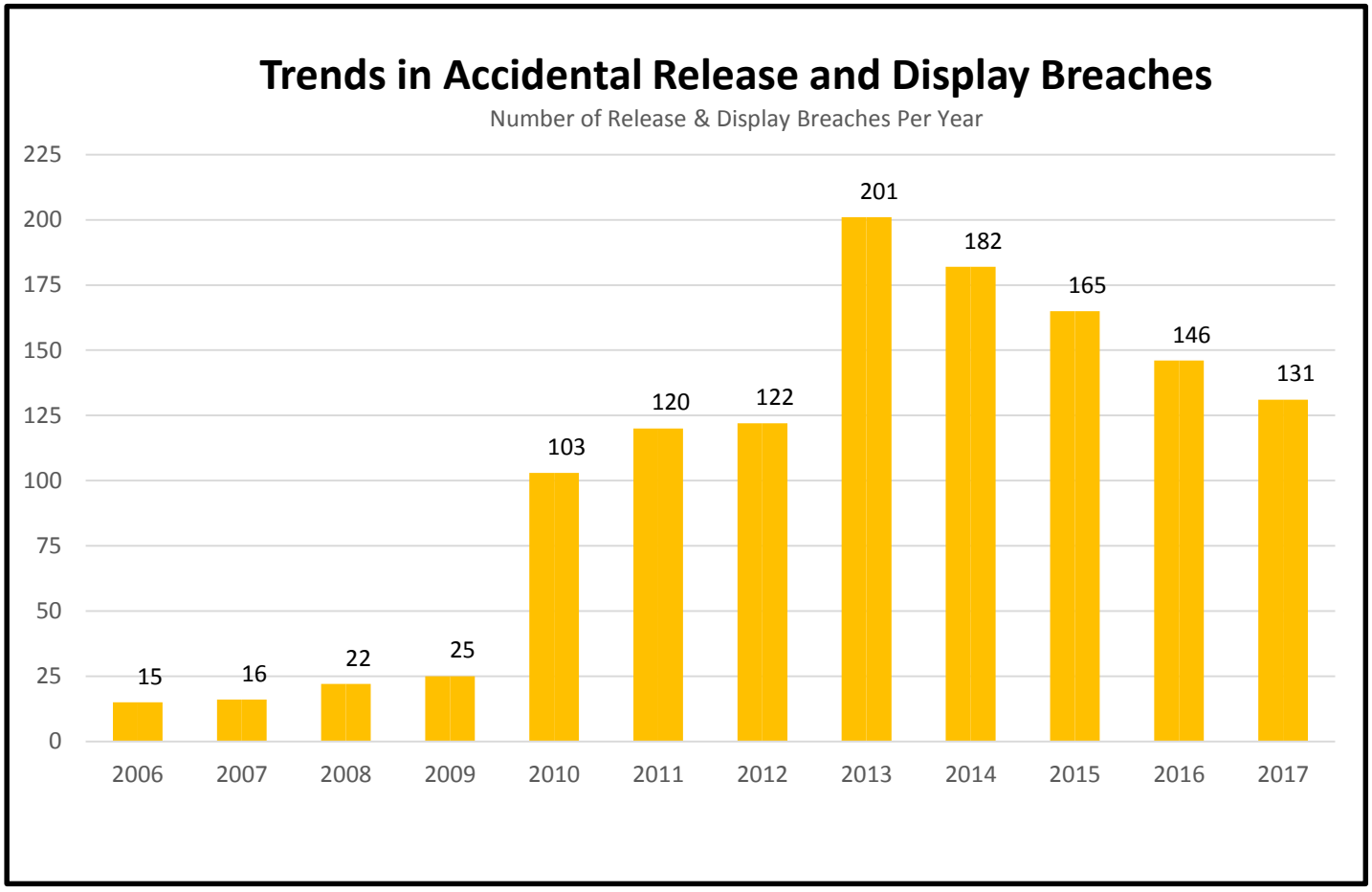
There were 131 accidental release and display breaches reported to the North Carolina Department of Justice last year accounting for approximately 13% of total data breaches for the year.

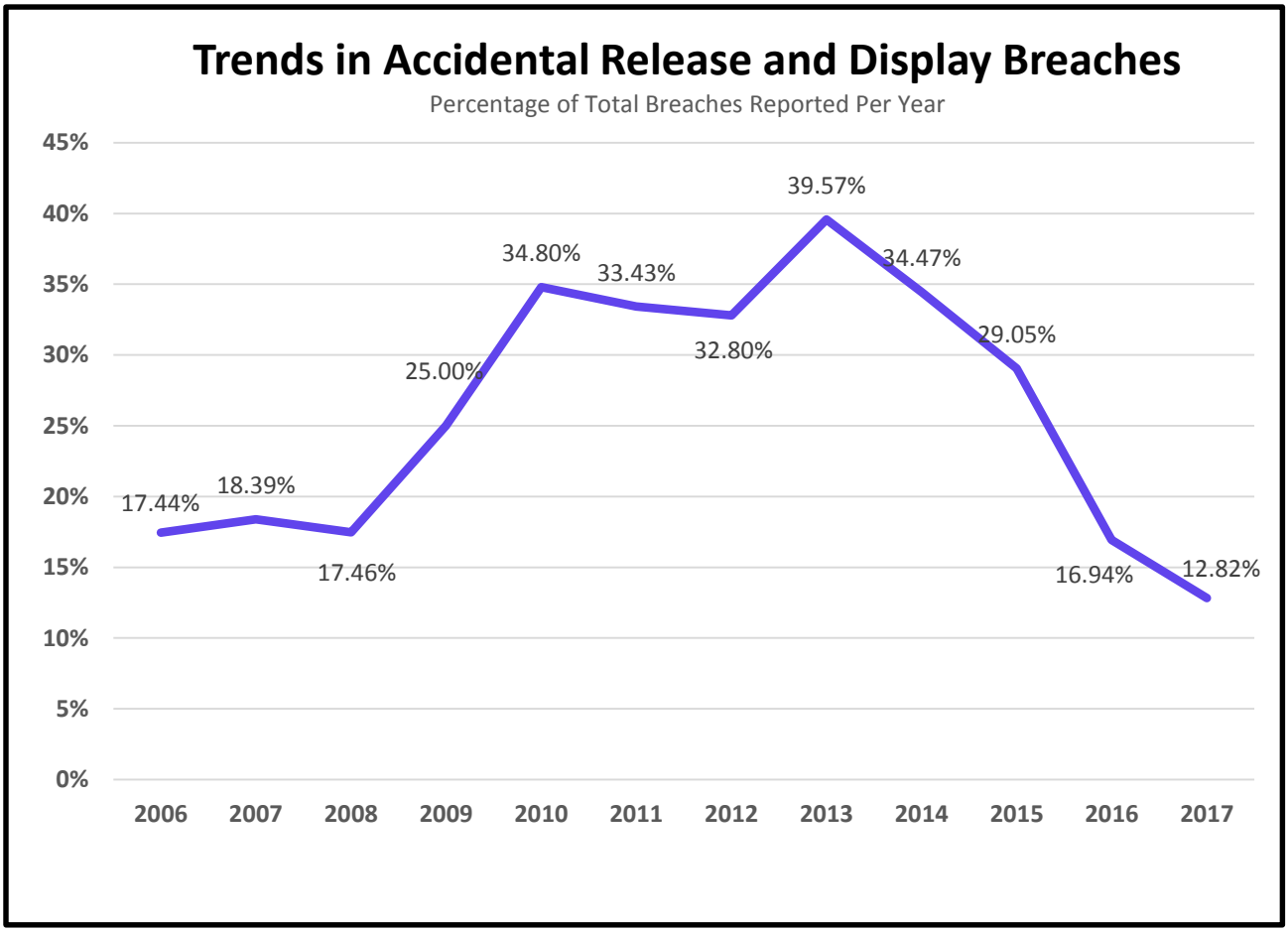
Protect Yourself If Your Information Has Been Compromised

Check your credit reports periodically. If you see a credit card or charge account you don't recognize, it could be a sign of identity theft or financial fraud.

If you have been impacted by a data breach, freeze your credit with all credit reporting services. Online credit freezes are free for all North Carolinians.

Visit www.ncdoj.gov/creditfreeze to learn more.

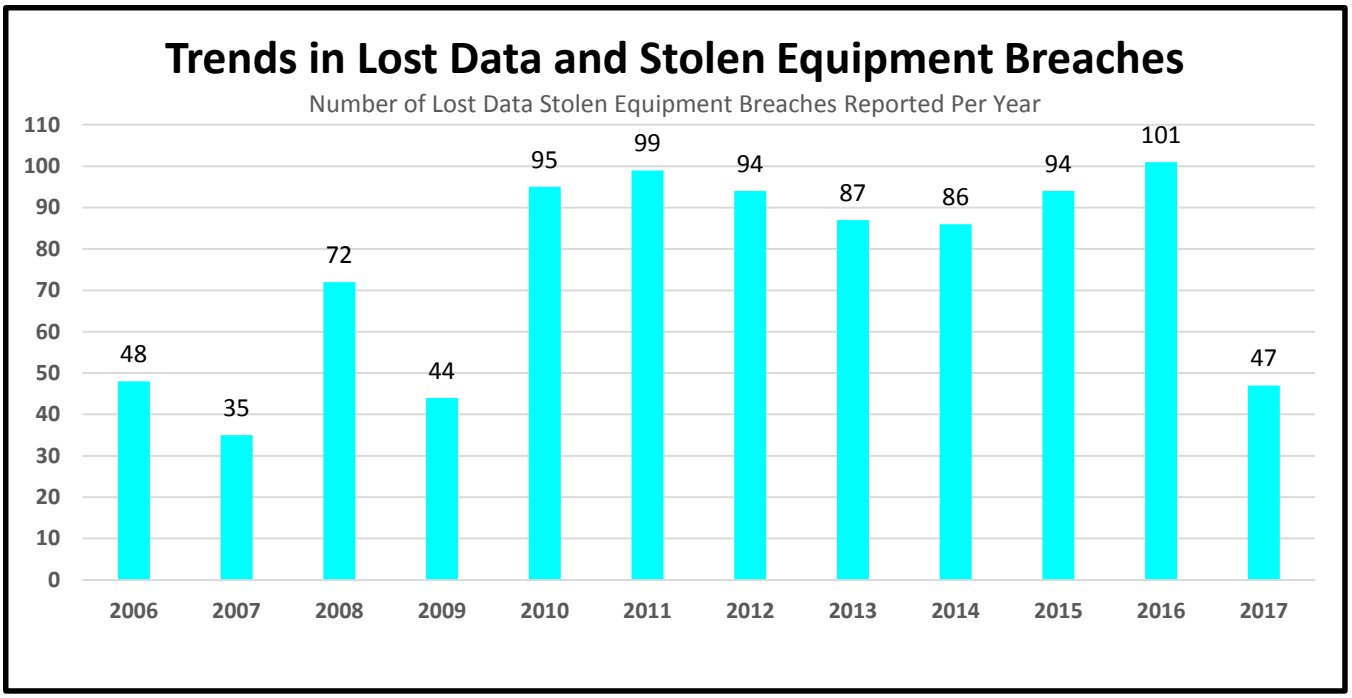

Trends in Accidental Release and Display Breaches
Number of Release & Display Breaches Per Year
225
200
175
150
125
100
75
50
25
0
15
16
22
25
103
120
122
201
182
165
146
131
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

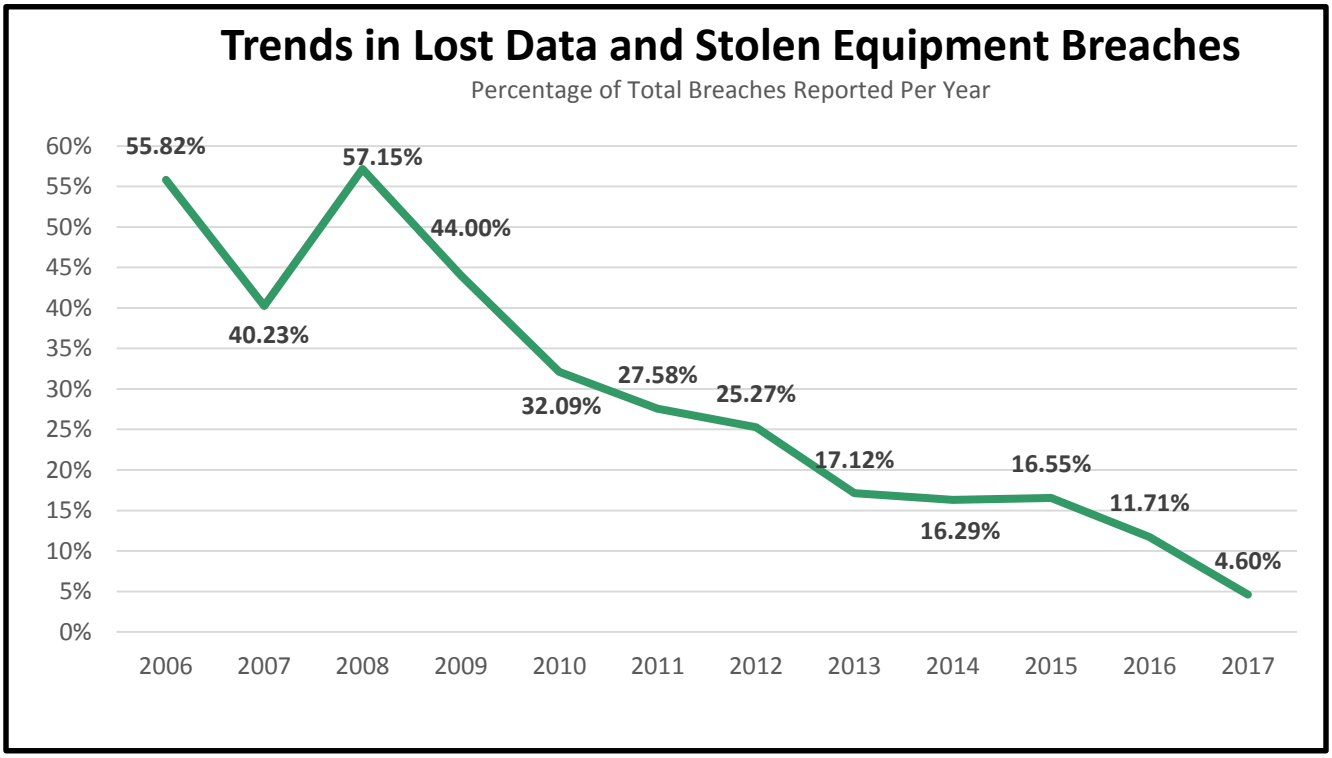

Trends in Accidental Release and Display Breaches
Percentage of Total Breaches Reported Per Year
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
17.44%
18.39%
17.46%
25.00%
34.80%
33.43%
32.80%
39.57%
34.47%
29.05%
16.94%
12.82%
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

Lost-in-Transit or Stolen Equipment

Data breaches can also occur when physical property is lost or stolen. Property types can include printed materials such as medical record folders or hardware such as laptops or external hard drives. This type of breach often occurs when flash drives are lost in the mail. Jobs that involve traveling with consumers' personal data – such as home healthcare providers or anyone carrying a laptop with sensitive information – have a high risk of data breaches from lost or stolen equipment.

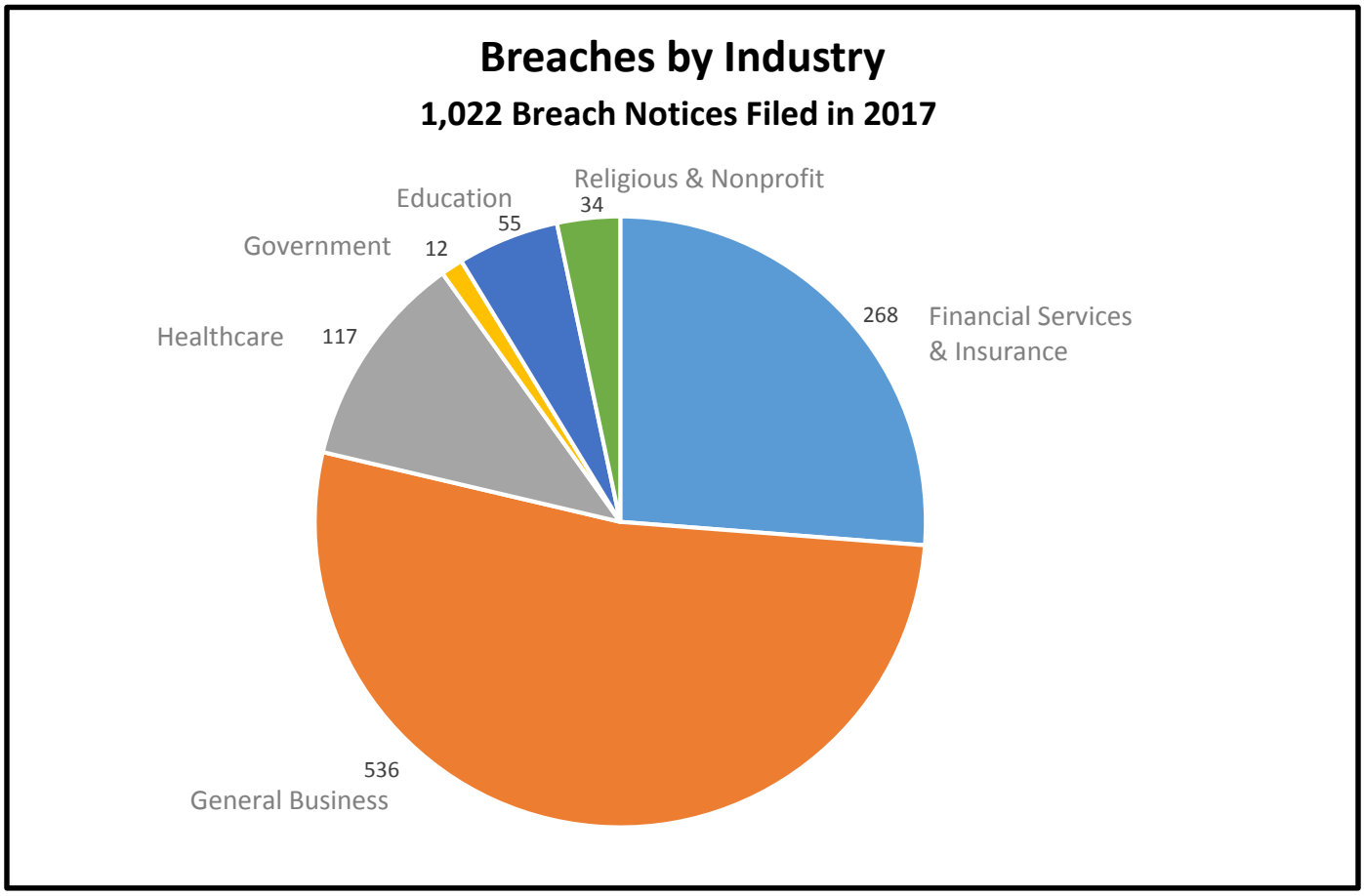
In North Carolina last year, companies reported 47 instances of lost or stolen equipment to the Department of Justice.



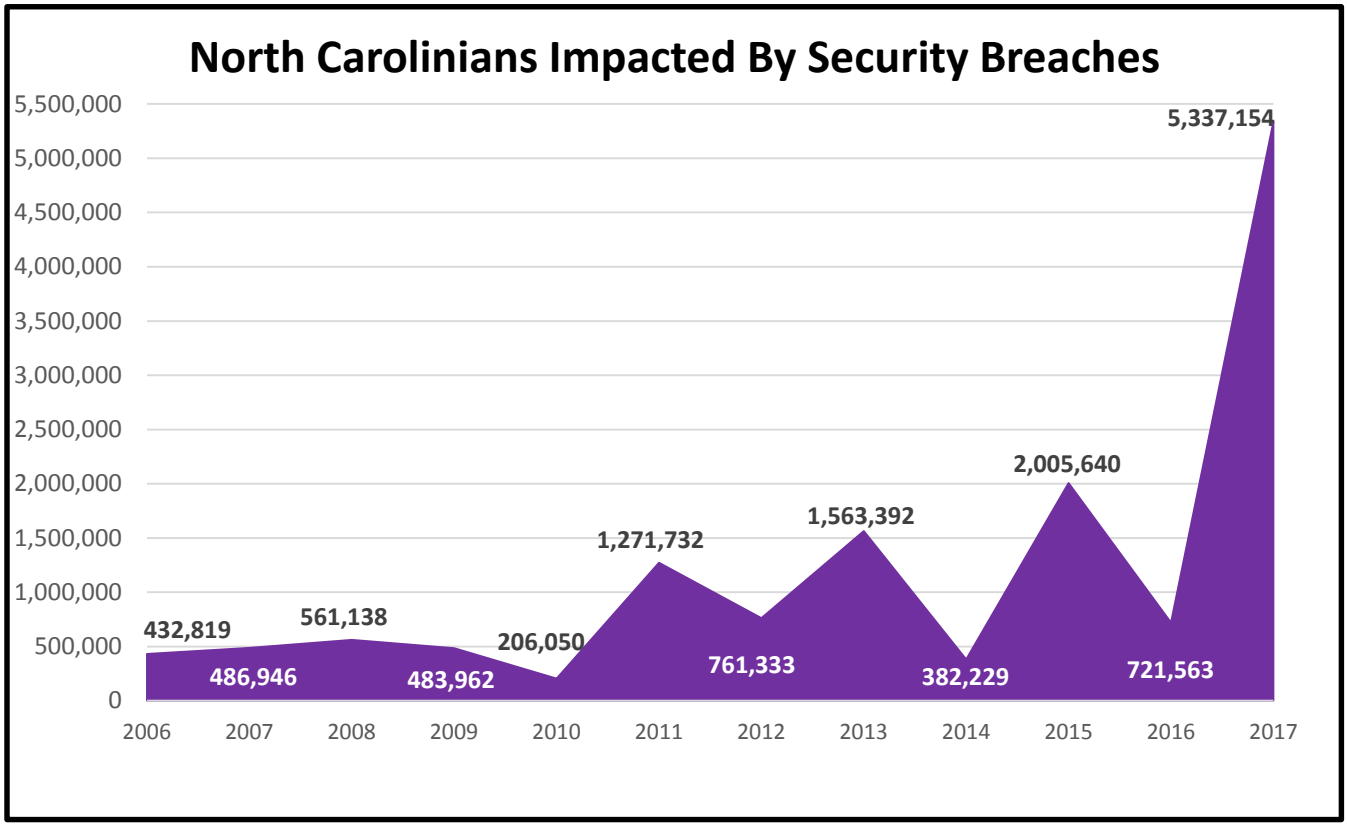


Discussion

Data breaches can come in many forms and affect a variety of industries. More than half of the data breaches reported this period came from the retail and general business category. The financial services and insurance sector has also seen a large number of breaches, accounting for 26% of those reported in 2017. While the health care industry is generally more susceptible to physical breaches, cybersecurity breaches – including ransomware attacks – are becoming increasingly common. Health care breaches accounted for approximately 11% of the total breaches reported in 2017.



As technology becomes more sophisticated and companies rely on larger stores of data, security breaches are becoming more common and affecting more and more North Carolinians. In 2006 – the first year North Carolina companies were required to report data breaches to the Department of Justice – companies reported 86 instances. By 2017, that number jumped to 1,022. The number of North Carolinians affected annually has increased from fewer than 500,000 in 2006 to more than 5.3 million affected by security breaches in 2017.



Conclusion

The trends in security breaches to the Department of Justice show data security to be an increasing threat for North Carolinians. Security breaches put North Carolina consumers at risk of identity theft and financial fraud. Data security can be a challenging task for many businesses as more companies rely on larger amounts of data and as hackers become increasingly sophisticated. But protecting consumers' sensitive, personal information must be a top priority for all organizations.

Attorney General Stein is working to protect North Carolina from fraud and privacy invasion. He has held companies accountable when they fail to protect consumer information, winning more than $500,000 for the state in 2017 from data breach settlements with Nationwide and Target. He has worked to educate North Carolinians about data security with a variety of outreach efforts. The Attorney General's fraud alerts provide pertinent information directly to consumers about data breaches and other scams.

Consumers should also take steps to protect their own information from scammers. Understanding the methods scammers use to steal personal data – such as phishing – is an important first step. Consumers should always exercise caution when sharing any personal information by first verifying websites and companies. Talking about data security risks and tips with others may save a loved one from accidently exposing their sensitive information to criminals.

For more information on security breaches in North Carolina, tips for protecting your data, and data breach report forms, visit the North Carolina Department of Justice online at www.ncdoj.gov/identitytheft.