December 17, 2015

DATA BREACH

MaineGeneral Health Suffers Cyber-Attack

MaineGeneral Health (MaineGeneral), located in Augusta, Maine, notified employees and patients last week that personal information and protected health information was compromised in a cyber-attack last month. The health care provider system was notified by the FBI on November 13 that its information was located on an external website not accessible to the general public.

The compromised information of an unknown number of individuals included names, addresses, and telephone numbers of certain employees and prospective donors, as well as dates of birth and emergency contact names, addresses, and telephone numbers of patients referred for radiology services by one physician since 2009.

Although MaineGeneral indicates that no Social Security numbers or financial information is known to have been compromised, the investigation is ongoing, and therefore, MaineGeneral is offering affected individuals one year of credit monitoring and identity restoration services as a precaution.

— Linn Foster Freedman

Alleged VTech Hacker Arrested

We previously reported that VTech suffered a data breach exposing millions of children's and their parents' personal information. The South East Regional Organised Crime Unit in the UK has announced that it has arrested a 21-year-old man allegedly involved in the hacking and have detained him in Bracknell, Berkshire. The authorities further stated that they had seized electronic items from the suspect.

— Linn Foster Freedman

MacKeeper Exposes 13 Million Users' Data

Kromtech, the manufacturer of MacKeeper, software that is designed to keep Macintosh computers secure, announced this week that a security vulnerability exposed the usernames, email addresses, and other personal information of over 13 million users.

The vulnerability was discovered by a security researcher, who published the vulnerability online and notified Kromtech of the issue. According to the researcher, the data was publicly available on the open web. Kromtech fixed the hole after being notified of the vulnerability and reiterated to customers that no payment information or other sensitive information was involved. Lesson? Even software designed as a security product might not be secure enough.

— Linn Foster Freedman

Georgia Secretary of State's Office Exposed 6 Million Voters' SSNs

It is frustrating for citizens to continue to watch state and federal governmental agencies announcing massive data breaches of citizens' personal information. Here is another.

On Tuesday, December 15, 2015, the Georgia Secretary of State's office released a much-awaited report concerning a data breach that occurred on October 13, 2015, but wasn't publicly disclosed until November 18, 2015.

The breach happened when the Georgia Department of Revenue requested sensitive data, including Social Security numbers, dates of birth, and drivers' license numbers of voters, so it could match it to entries in its database. This alone is disturbing. Citizens should be able to rely on governmental entities to use best practices in accessing, collecting, and maintaining citizens' Social Security numbers and only ask for the minimum amount necessary. The reason why all of this sensitive data was being requested has not been made public.

An employee of the Secretary of State's office contacted an outside vendor to respond to the request. The vendor uploaded the data to an existing statewide voter file that should not have contained the information. The employee shared his user ID with another employee. That employee accessed the file that contained the sensitive information and burned the information onto CDs and emailed the voter list that wrongfully contained the sensitive information to a list of 12 groups that routinely receive voter information, including state political parties and media organizations, including the *Atlanta Journal-Constitution* and *Georgia GunOwner Magazine*.

The CDs were recovered or destroyed. Nonetheless, a class action lawsuit was filed for the breach and a Georgia congressman has requested that the FTC investigate the breach.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Update on Recent Cyber Prosecutions/Stings

The feds keep chipping away at those thieves and hackers, and we are pleased to showcase the recent results of their hard work.

Computer Hacking and Sexual Extortion

On December 9, 2015, the U.S. Attorney's Office of the Northern District of Georgia announced that a former U.S. State Department employee employed at the U.S. Embassy in London pled guilty to

perpetrating a widespread, international e-mail phishing, computer hacking, and cyberstalking scheme against hundreds of women in the United States and abroad. Using e-mail passwords obtained by phishing, he hacked into hundreds of victims' e-mail and social media accounts, stole thousands of sexually explicit photographs, and threatened at least 75 victims that he would release their photos and other personal information unless they agreed to his "sextortionate" demands.

He "tormented" his victims, mostly young females, with a focus on members of sororities or aspiring models, by "threatening to humiliate them unless they provided him with sexually explicit photos and videos."

He posed as an employee of an "account deletion team" for a well-known e-mail service provider and sent phishing emails to thousands of women warning them that their e-mail account would be deleted if they didn't give him their password. If they gave their password, he then hacked into their e-mail account and social media account and searched for sexually explicit photographs. If he found them, he searched for personally identifiable information about them, including their home and work addresses, school and employment information, and names and contact information of family members.

He then threatened the women that if they didn't give him photos or videos, he would release the photos. If they refused to comply, he would tell them that he knew where they lived and did in fact send some of the information, to family members.

He successfully hacked into 450 online accounts belonging to at least 200 victims. He will be sentenced on February 16, 2016. The U.S. Attorney's Office reminds anyone who believes they are a victim of hacking, cyberstalking, or "sextortion" should contact law enforcement.

Employee Theft of Trade Secrets

Last week, the U.S. Attorney for the Southern District of New York and the New York FBI Office announced that Xu Jiaqiang has been arrested for theft of a trade secret of proprietary source code from his former employer.

According to the allegations, Xu worked as a developer for an unnamed software company and had access to proprietary software and underlying source code of a clustered file system. The company only provided access to the proprietary code to authorized individuals.

Xu resigned from the company and started communicating with undercover law enforcement officers posing as financial investors looking to start a big data storage company. He sent the officers code from his previous employer and remotely installed the proprietary software on networks set up by the FBI, which was confirmed to be functioning software of the previous employer.

Xu admitted to undercover law enforcement that he had used the code to build a copy of the proprietary software to sell to customers. He has been charged with one count of theft of a trade secret, which carries a maximum sentence of ten years in prison. He is being prosecuted by the U.S. Attorneys' Terrorism and International Narcotics Unit and the National Security Divisions' Counterintelligence and Export Control Section. Impressive work!

On Tuesday, December 15, 2015, the U.S. Attorney of the District of New Jersey announced that three alleged hackers from Florida, New Jersey, and Maryland were charged with a "wide-ranging computer hacking and identity theft scheme that compromised the personally identifiable information (PII) of millions of people and generated more than $2 million in legal profits."

The individuals were charged with conspiracy to commit wire fraud and conspiracy to commit fraud with electronic mail.

The allegations include writing computer programs that conceal the origin of the email in order to bypass

spam filters. They allegedly hacked into the email accounts of individuals and seized control of the mail servers of corporations. Further, they created custom software "that leveraged vulnerabilities in the websites of a number of corporations," which allowed them send out spam that looked like it came from the company. Finally, they stole confidential business information of corporations, including databases containing millions of individuals' PII, one of which was the employer of one of the alleged hackers. The hacker gave access to the employer's system to the other hacker through a remote administration tool so they could steal the names, addresses, telephone numbers, and email addresses of former, current, and potential customers.

The hackers face a maximum of five years in prison and a fine of greater than $250,000 or twice the gain or loss from the offense for conspiracy to commit fraud and related activity in connection with computers, 20 years in prison and a similar fine for conspiracy to commit wire fraud, and 5 years in prison and the same fine for conspiracy to commit fraud and related activity in connection with email.

There is also a request for forfeiture of close to $300,000 in bank accounts, a 2006 Ferrari convertible, and a 2009 Cadillac SUV.

Destroying, Altering, and Falsifying Medical Records

On December 10, 2015, a former Department of Veterans Affairs nurse pled guilty in the Southern District of Florida to "destroying, altering and falsifying records and committing computer fraud." He faces up to 20 years in prison.

The nurse caused damage to the Miami VA Medical Center's computer system when he falsified the medical records of a 76-year-old veteran with whom he had a treating relationship. The patient died, and the nurse tried to cover up the poor quality of treatment he received by attempting to falsify the records. He will be sentenced on February 19.

Member of "NullCrew" Pleads Guilty

The U.S. Attorney's Office in the Northern District of Illinois announced on December 8, 2015, that a member of the hacking group "NullCrew" pled guilty to charges that he "helped launch cyber-attacks on corporations, universities and governmental entities throughout the world."

He pled guilty to one count of intentionally damaging a protected computer without authorization, which carries a maximum of 10 years in prison. He admitted that he participated in at least seven cyber-attacks while a member of NullCrew, including one against a large Canadian telecommunications company and another against a U.S. state. He will be sentenced on March 9, 2015.

We highlight these prosecutions for several reasons. First, the facts are important to understand, as they are real-life scenarios that happen every day against individuals and companies and can serve as lessons to learn from. Second, law enforcement is working hard to combat cybercrimes, and victims might want to consider bringing law enforcement into investigations and collaborate with the government to combat cybercrime. Finally, it is good to know that the thieves and hackers are seeing and feeling the consequences. We will continue to update you on the good work of law enforcement in bringing these thieves and hackers to justice.

— Linn Foster Freedman

Computer Fraud and Abuse Act Update: Second Circuit Sides with a Narrower Reading

The controversy over what is a "computer crime" under the Computer Fraud and Abuse Act (CFAA) is

now settled for New York, Connecticut, and Vermont. In a case we have been watching on the blog for months, *United States v. Valle*, the Second Circuit held that the CFAA should be read narrowly.

The Court summarized the CFAA issue:

"[W]e must determine whether an individual 'exceeds authorized access' [under 18 U.S.C. § 1030(a)] to a computer when, with an improper purpose, he accesses a computer to obtain or alter information that he is otherwise authorized to access, or if he 'exceeds authorized access' only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access."

Interestingly, the court concluded that the CFAA's text, history, and purpose actually supports *both* sides of the debate. Still, the court was "obligated to 'construe criminal statues narrowly so that Congress will not unintentionally turn ordinary citizens into criminals'" (citations omitted).

This criminal case will also impact civil cases. The CFAA creates a private cause of action that some employers have used in lawsuits against employees for alleged misuse of employer data. Now, employers' ability to do so in New York, Connecticut, and Vermont is more limited.

The court noted that this is an "issue of first impression" in the Second Circuit and that it has "sharply divided our sister circuits." The Second Circuit's decision to finally choose a side in the controversy makes it more likely that the Supreme Court will one day settle it once and for all.

— *Nuala E. Droney*

Medical Informatics Data Breach Litigation Centralized and Transferred

We previously reported on the multiple data breach litigation suits filed against Medical Informatics Engineering, Inc., following a data breach in May 2015.

On December 10, 2015, the United States Judicial Panel on Multidistrict Litigation centralized the nine pending suits—five pending in the Northern District of Indiana, one in the Southern District of California, one in the Southern District of Indiana, one in the District of Kansas, and one in the Western District of Washington, along with twelve related actions pending in the Middle District of Florida and the Northern and Southern Districts of Indiana, and transferred them to the Northern District of Indiana.

The Court reasoned that the majority of the actions are pending in the Northern District of Indiana, that is where the Medical Informatics is headquartered, "and where many of the healthcare providers (and individuals) affected by the data breach are located."

— *Linn Foster Freedman*

HIPAA

University of Washington Medical School Pays OCR $750,000 for Data Breach

The Office for Civil Rights (OCR) announced on Monday, December 14, 2014, that it has settled a HIPAA investigation with the University of Washington Medical School involving a data breach in October of 2013.

The breach occurred when an employee in the billing office clicked on an email attachment that contained malware and exposed 90,000 patients' personal information, including 76,000 patient names, medical records, and account balances and 15,000 patients' Social Security numbers, telephone numbers, and dates of birth.

In addition to paying the hefty fine, the medical school has agreed to conduct annual risk analyses and report to OCR its risk management plans for the next two years.

We have seen an increase in employees exposing systems to malware through clicking on attachments or website links from work stations. This case illustrates again how important it is to keep your employees aware of the latest risks that can affect your system and how with one click they can expose high-risk data with dire consequences.

— Linn Foster Freedman

CYBERSECURITY

NIST Seeks Comments on Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed and issued its voluntary "Framework for Improving Critical Infrastructure Cybersecurity" (Framework) in response to a 2013 Executive Order in February of 2014. It was developed in collaboration with industry, academia, and state and federal government officials. It has been widely praised and used as a valuable tool for companies to assess and respond to cybersecurity risk in their organizations.

On December 11, 2015, NIST issued a Request for Information to receive feedback on the use of the Framework, including specific questions about:

- the variety of ways in which the Framework is being used to improve cybersecurity risk management,
- how best practices for using the Framework are being shared,
- the relative value of different parts of the Framework,
- the possible need for an update of the Framework, and
- options for the long-term management of the Framework.

The comment period is from December 11, 2015, through February 9, 2016. Comments will be used to enhance the Framework and to assist with developing the agenda for a Framework workshop being planned for April 6 and 7, 2016, at NIST.

— Linn Foster Freedman

Cybersecurity and Resiliency: The Financial Sector's "New Frontier"

"The Internet has a dark side," Deputy Treasury Secretary Sarah Bloom Raskin remarked while addressing senior-level banking executives at this year's Clearing House Annual Conference. Raskin focused her comments on malicious cyber activity, pointing out that weaknesses in the financial sector's complex interconnected system attract bad actors like water "drawn to cracks in a foundation."

While commending the recent adoption of cybersecurity norms by G-20 leaders, Raskin acknowledged that proactive efforts by financial executives is essential to strengthening the country's financial infrastructure. She then offered a three-part cybersecurity checklist for in-house counsel, compliance officers, security personnel, and others looking to stave off cyber-attacks:

1. Ensure that cybersecurity is part of the institution's "genetic code" by embedding cybersecurity processes into governance, control, and risk management systems.

2. Engage in basic essential security practices such as requiring multi-factor authentication, restricting high-level access to privileged users, and mandating regular patching of software. These and other essential practices can prevent up to 80 percent of all known incidents.

3. Be prepared for the worst by creating a response and recovery playbook for serious cyber incidents. The playbook should direct the company's response when a cyber incident happens: who does what and when, and who reports to whom, as well as provide guidelines addressing when to involve law enforcement and executive management, and when to inform clients and customers.

With the continuing if not accelerating impact of technology on the financial services sector, cybersecurity and resiliency become ever more critical to the well-being of our financial system. Treasury Secretary Raskin's "cybersecurity checklist" offers some direction for financial institutions beginning their journey into this "new frontier"

Treasury Secretary Raskin's biography is available here.

— Norman H. Roos and Scott M. Baird

FAA Announces Streamlined Drone Registration Process

On Monday, December 14, the Federal Aviation Administration (FAA) announced a "user-friendly" online aircraft registration system for owners of drones (or more officially called "small unmanned aircrafts") that weigh more than 0.55 pounds but less than 55 pounds. This registration is a statutory requirement that applies to all types of aircrafts. Anyone who has owned a drone prior to December 21, 2015, must register with the FAA no later than February 19, 2016, and all others who purchase or use a drone after December 21, 2015, must register before the drone's first outdoor flight. The paper registration process still exists for those drone operators under 13 years old (to ensure compliance with the Children's Online Privacy Protection Act). Each person who registers their drone with the FAA will need to provide their name, home address, and email address. After registration is complete, the operator will receive a Certificate of Aircraft Registration/Proof of Ownership and the unique identification number provided must be marked on the drone. The registration is valid for three years and costs $5 (the FAA is waiving the registration fee from December 21, 2015, to January 20, 2016, to encourage registration).

An FAA representative said, "Make no mistake: unmanned aircraft enthusiasts are aviators, and with that title comes a great deal of responsibility." Have fun holiday shopping for drones and visit the website for details.

— Kathryn M. Rattigan

DATA PRIVACY

Online Trust Alliance Releases Smart Device Privacy and Security Checklist for Consumers

Here's a question: do you review each smart device's policies and terms before you purchase the device? Probably not. However, when you pick out or receive a smart device, you really need to be aware of the privacy and security options (and compromises) that come along with each. To help consumers out with those decisions this holiday season, the Online Trust Alliance (OTA) issued its "Smart Device Purchase and Set-Up Checklist." Check it out here. Here are just a few of their recommendations:

- Use a firewall
- Disable remote access to smart devices when you are not using them.
- If you cannot opt out of sharing data with third parties or are not provided the option of opting in, consider alternative smart devices.
- Find out if security software patches are provided for the life of the products.
- Use a username and password that does not identify you or your family or the model of the device.
- Disable your microphone and camera when not in use.
- Reset the device to factory settings before you sell or give away your device.

The OTA estimates that over 50 million smart devices will be sold and gifted this holiday season, including not only mobile phones but also fitness trackers, kitchen appliances, and speakers that recognize you when you walk into a room so that your personal music choice can follow you around your house. Senior Director of Internet of Things (IoT) at Symantec, Brian Witten, says, "While people are aware that they need to have security on their connected devices, they don't always take the necessary steps to protect themselves. Until device manufacturers build security into their products, the responsibility relies with the consumer." So if you are on the market for a connected smart device (or you think Santa may be delivering one this year), make sure to check out the OTA's helpful tips.

— Kathryn M. Rattigan

WEEKLY PRIVACY TIP #14

Record Destruction: An Overwhelming Problem

This week's tip is applicable to both individuals and businesses, and is a headache for both. Lately, it seems that everyone I talk to is lamenting about what a hassle document retention and destruction is, both personally and professionally. For good reason. Like other areas of law (such as data breach notification laws), every state has its own requirements about how long records must be retained and no two states are the same. They are hard to keep track of and many of the laws are antiquated.

In response to the disorganized legal requirements, individuals and companies tend to keep records, both paper and electronic, much longer than legally required or necessary. Some have told me that they keep records "forever."

An important part of a data privacy and security program is to destroy records in accordance with the protocols established by an up-to-date record retention policy. This policy, which should be developed with the advice of counsel, should spell out what documents can be destroyed, when that destruction can occur, and when the threat of litigation or the issuance of a litigation hold notice requires suspension of

scheduled destructions. And though it seems overwhelming, there are really good reasons to focus on data retention and destruction now.

First, as a longtime litigator, I have seldom seen a piece of paper come back to help a client in litigation. Folks, there is a reason there is a term known as a "smoking gun." Absent a litigation hold requiring the preservation of documents, keeping materials longer than the time frames provided in your record retention policy more often than not will not help you in litigation.

Second, the cost associated with storing documents forever, both in paper and electronic form, is unnecessary if you implement and follow a thoughtful record retention policy, complete with defined destruction protocols, and will even help your bottom line. Of course, work with counsel to make sure your program complies with applicable laws and includes provisions for the suspension of destruction protocols upon the issuance of a litigation hold notice.

Third, many old documents or electronic data include high-risk data that is no longer included on forms or other documents for best practice, including full Social Security numbers, medical insurance numbers, drivers' license numbers, and health information. Keeping old paper records or electronic data (including old back-up tapes) increases the risk of a data breach because if they are lost or stolen, notification to individuals and regulatory authorities may be required because of the type of data included. This would not happen if you properly destroy them.

Think of old documents and electronic data like any other asset that is no longer needed. When you upgrade the furniture in your home or office, you don't send the old furniture to storage. You give it away, sell it on Craig's List, or throw it away. The same is true of old data that is no longer needed (well, don't sell it on Craig's List!) But you see my point—if you don't need it, and it's not subject to a litigation hold, follow your record retention policy's requirements to properly dispose of that paper and electronic data so it no longer poses a risk to you.

So get that dusty record retention program out, dust it off, update it as necessary, and get that program working for you. And while you are at it, get rid of the old stuff out of your home filing cabinet too.

— Linn Foster Freedman and Andrea Donovan Napp

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.
