
**April 28, 2016**

**UPCOMING EVENT**

**Recent Trends in Cyber Intrusions — A View from the Insiders**

Although sharing information may alleviate companies from "going it alone" and can give them the heads up about intrusions so they can adequately prepare and respond, private companies are understandably nervous about giving cyber intrusion information to the government and exposing vulnerabilities. Can they trust the government to keep business information strictly confidential? How does the government protect the information?

Join us on Tuesday, May 3, 2016, at Brown University in Providence, Rhode Island, for this panel discussion with Peter F. Neronha, U.S. Attorney for the District of Rhode Island; David C. Aaron, Trial Attorney, U.S. Department of Justice National Security Division, Counterintelligence & Export Control Section; Linn F. Freedman, Chair of Robinson+Cole's Data Privacy + Security Team; a FBI Cybercrimes Agent; and a Secret Service Agent.

Registration begins at 7:30 a.m. and the program runs from 8 to 10 a.m. Continental breakfast will be provided.

For more information and to register, click here.

*Co-hosted by Brown University Executive Master in Cybersecurity and Robinson+Cole. Robinson+Cole and Brown University are not affiliated.*

**CYBERSECURITY**

**Ransomware Gets Even More Nightmarish with Jigsaw**

We have been alerting all of our readers to the nightmares of ransomware, and that the health care industry is a prime target.

Just when you thought it couldn't get any worse, a new strain of ransomware, known as Jigsaw, originally known as *BitcoinBlackkmailer.exe*, was reportedly built on March 23, 2016, and released within a week. The way it works is that if a victim downloads the malware, a malicious code encrypts the user's files, sets up a scary locked screen with the face of Billy the Puppet from the movie Saw, tells the user that the files are encrypted and that they are being held to a ransom, to be paid in virtual currency, such as Bitcoin.

What is really scary about this form of ransomware is that the threat is not only that all of the files are

encrypted, but also, after Billy the Puppet is displayed on the screen, the victims are told that if they don't pay the ransom files will be deleted every hour.

According to a reports, only a few files are deleted within the first 24 hours, but then several thousand files are deleted every day until payment is made. The files are deleted while the victim is watching because a victim who attempts to close the system or turn off the computer, is told that 1000 files will be deleted when they start the computer back up "as a punishment."

The malware is reportedly for sale on Tor for $139, but security experts note that the malware is not that sophisticated and can be reverse engineered and analyzed. However, it is important to note how creative hackers are getting in making our lives more difficult in protecting data.

*— Linn Foster Freedman*

---

**FireEye Report Shows PoS Attacks Have Compromised More Than 20 Million Cards**

FireEye recently issued a report that indicates that bank card data of over 20 million individuals has been compromised since 2014. According to the report, point-of-sale attacks that have affected the retail and hospitality industries will continue while companies are in the process of implementing chip-and-pin cards, and fraudsters are targeting magnetic card systems in the interim.

According to FireEye, it has seen 20 million stolen credit cards available for sale in the underground marketplace by a group dubbed FIN6 for $21 apiece, which all told could rake in over $400 million. These cards were stolen in one incident, and the victims were mostly from the U.S.

The malware used to compromise the data was Grabnew, which is also known as Vawtrek and Neverquest. Who comes up with these names anyway?

*— Linn Foster Freedman*

---

**Hackers Responsible for Ruthless SpyEye Trojan Sentenced to 24.5 Years**

The Department of Justice has announced that two hackers who built and sold the Trojan called SpyEye, which caused close to $1 billion in banking losses, have been sentenced for a combined 24.5 years in federal court in Atlanta.

According to evidence presented in court, provided by the able investigation of the FBI, the Department of Justice, and international cyber and digital crimes agencies, SpyEye was the "preeminent malware banking Trojan from 2010-2012, used by a global syndicate of cybercriminals to infect over 50 million computers, causing close to $1 billion in financial harm to individuals and financial institutions around the globe."

The hackers, from Russia and Algeria, designed SpyEye to automate the theft of online banking credentials, credit card information, usernames, passwords, PINs, and other personal information. It secretly infected the computers and allowed the hackers to remotely control the computers. Once they got control of the computer, they were able to remotely access the computers without authorization, transmit the personal information, and steal money from the accounts.

One of the hackers sent over one million spam emails containing strains of SpyEye and other malware to computers in the U.S. The FBI had reason to believe that, a short time after one of the hackers' arrest, he was planning to release SpyEye 2.0, which "if released, would have been one of the most prolific and undetectable botnets distributed to date…."

Another one for the good guys!

*— Linn Foster Freedman*

---

**Indiana Governor Announces Formation of Indiana Executive Council on Cybersecurity**

Indiana Governor Mike Pence announced last week the formation of the Indiana Executive Council on Cybersecurity through an Executive Order. The Council, comprising of 23 members from public and private organizations, is designed to be a public-private partnership to work together to protect the state from online threats.

In announcing the Council, the Governor stated, "While risk can never be completely eliminated, Indiana will employ all available tools to manage cyber threats." The Council will include subject-matter experts from a broad and diverse array of disciplines and will be chaired by the executive director of the Indiana Department of Homeland Security.

Bringing subject matter experts together in a state to work toward information sharing to combat cyber-threats seems like a no-brainer and will no doubt be replicated by other states.

*— Linn Foster Freedman*

---

**DATA BREACH**

**Wyoming Medical Center Victim of Phishing Scheme Affecting 3,184 Patients**

Phishing incidents in February that may have compromised the data of 3,184 patients, including their names, dates of birth, medical records and account numbers, dates of service, and medical information is causing Wyoming Medical Center in Casper, Wyoming, to notify the patients of the incident. Luckily, according to the medical center, no financial information or Social Security numbers were included in the information that was accessed for 15 minutes by the hacker, who was able to get access into two organizational accounts and obtain administrative credentials.

The facts of this case are a good learning tool for any industry. An employee of the medical center opened a phishing email and clicked on an attached link on February 22, which provided the hacker access to that employee's emails, which contained patient information (and could obtain any type of information depending on the employee's job function). A second employee opened a phishing email three days later, allowing a second unauthorized access to that employee's emails.

According to the medical center, the IT system was able to detect the compromise as the employees' compromised accounts sent spam emails to other medical center employees, and they were able to stop the compromise quickly. Nonetheless, the 15 minutes of unauthorized access led to the medical center notifying almost 3,200 patients, which shows just how fast a compromise can happen.

Phishing continues to be a huge issue for businesses, and multiple attempts and compromises are not uncommon with sophisticated spear phishing attacks. Continue to be on the lookout for these phishing schemes, and provide your employees with training and tools to combat them.

*— Linn Foster Freedman*

---

**Update on the Panama Papers**

The International Consortium of Investigative Journalists (ICIJ) announced that on May 9, it will release selected data purported to be leaked or stolen from the internal records of the Panamian law

firm Mossack Fonseca. ICIJ plans to release this selected data in a searchable database. The release is expected to cover 200,000 companies and other organizations organized under 21 jurisdictions across the globe which are widely considered to be tax havens. These jurisdictions include Hong Kong, Nevada, Switzerland, Singapore, Panama, and the Cayman Islands. The selected data is also expected to identify people associated with these companies and organizations, who reportedly live in more than 200 countries and territories.

Once the searchable database is made available, users will be able to search for particular companies, organizations, and individuals. The ICIJ has said they will not include sensitive personal information in the database, such passports and telephone numbers.

Our earlier post on the Panama Papers can be viewed here.

*— Kathleen M. Porter*

---

**ENFORCEMENT + LITIGATION**

**Facebook Argues Motion to Dismiss in 'Happy Birthday' Message Campaign TCPA Class Action**

On April 25, 2016, Facebook Inc. (Facebook) pled with a California federal judge, asking that the court dismiss the claims filed against the social media giant for its alleged Telephone Consumer Protection Act (TCPA) violations. We wrote about this class action when it first surfaced back in February, and now Facebook hopes that the court will grant its motion to dismiss based on the fact that its 'happy birthday' messages are permissible under the TCPA. Facebook argued that the TCPA is meant to protect against telemarketing and robocalls not against personalized messages alerting its users about their friends' birthdays. Facebook said in its motion to dismiss, "This sort of message—that identifies a specific individual with a specific connection to plaintiff and relates to a specific event on a specific date—is a far cry from the type of impersonal, en masse communications that the [TCPA] prohibits." Additionally, Facebook argued that the TCPA requires the use of an "automated telephone dialing system," and its birthday messages are sent only after a user inputs their own telephone number into Facebook. This is also why Facebook argues that even if these messages fell under TCPA regulations, they have received consent from their users. Facebook also questions the lead plaintiff's standing, but much like the rest of us, they are awaiting a decision from the U.S. Supreme Court in *Spokeo Inc. v. Robins*. We will follow this case and see what the California judge decides.

*— Kathryn M. Rattigan*

---

**Debt Collector, Portfolio Recovery Associates, to Pay $18 Million to Settle TCPA Violations**

Portfolio Recovery Associates LLC (Portfolio Recovery) agreed to pay $18 million to end multi-district litigation against the debt collection company for its alleged violations of the Telephone Consumer Protection Act (TCPA). The claims against Portfolio Recovery alleged that the company made autodialed telephone calls to consumers without their consent. All consumers who received an autodialed call to their cell phone between December 2013 and July 2013 will receive part of this settlement. Over 7.3 million consumers are set to receive settlement notices. Of that $18 million, the class representatives asked the court to approve attorneys' fees of $5.4 million and costs of $3.3 million or about 48 percent of the total settlement amount. Each class representative will receive $6,250 service awards. The lengthy settlement papers read, "While each of the parties respectively believe they would have prevailed on the merits had the case not settled, they each have concluded that settlement was preferable to the uncertainty and risk attendant with litigation the case further."

*— Kathryn M. Rattigan*

## BITCOIN + VIRTUAL CURRENCY

### Bitstamp Obtains First Payment Institution License in the World

Bitstamp, the third largest Bitcoin exchange in the world and located in Luxembourg, announced on April 25, 2016, that it has obtained a payment institution license from Luxembourg, which means it is the first nationally licensed Bitcoin exchange in the world.

The license was obtained through the European Union's passport program, which gives reciprocity for companies that obtain a license in one European state to operate in others. Therefore, with the Luxembourg license, Bitstamp will be licensed in all 28 European countries starting on July 1, 2016.

Simultaneously, Bitstamp announced that it is launching euro-Bitcoin trading, so customers can exchange euros for Bitcoin on a fully licensed exchange, which many believe will expand relationships with banks so Bitcoin will become mainstream in the financial services industry and not associated with hackers only.

Bitstamp is required to undergo annual audits, and has implemented procedures to meet regulatory requirements, including anti-money laundering and know your customer rules required of financial institutions. It took two years to prepare and obtain the license.

The licensure of Bistamp has been hailed as making "blockchain history," and is spurring conversations about worldwide policy on blockchain technology, including in the United States.

*— Linn Foster Freedman*

## DATA PRIVACY

### Update on the U.S. - EU Privacy Shield

As we previously reported, this February, United States (U.S.) and European Union (EU) negotiators announced the "U.S.-EU Privacy Shield" as a replacement to the U.S. Safe Harbor. Many U.S. companies relied on the Safe Harbor to transfer data from the EU to the U.S. The Privacy Shield negotiations were accelerated in response to the European Court of Justice's judgment late last year declaring the Safe Harbor to be an inadequate framework for transferring such data under Directive 95/46/EC (EU Privacy Directive), based on the Max Schrems case and in response to the Edward Snowden revelations about U.S. government authorities accessing data.

The Privacy Shield's ultimate adoption requires approvals at different levels within the EU. The approval process will take several months, or even longer, and approval is not a foregone conclusion. Most recently, the EU Article 29 Working Party, a committee of EU data-protection regulators, issued an opinion criticizing the Privacy Shield for failing to adequately restrict U.S. government access to EU's citizens data and include important components of the EU's data-protection regime. While the Article 29 Working Party's opinion is not binding on the European Commission (EC), it does potentially slow the momentum for the Privacy Shield's adoption by member states and the EU itself. It also provides opponents of the Privacy Shield with a powerful weapon to use in the court action they have threatened to bring to challenge the Privacy Shield.

In the interim, U.S. companies who still need to transfer data out of the European Union are looking for answers and alternatives. As a first step, companies should know that the U.S. Department of Commerce continues to administer the Safe Harbor program, both to process new submissions for self-certification to the Safe Harbor Framework and to accept any existing certified company's annual reaffirmation.

However, several European data protection authorities have encouraged U.S. companies to explore the alternative arrangements available under the EU data protection regime. These alternative arrangements which permit the transfer of data from the EU into the U.S. include:

- Companies can adopt approved "model contract" terms to use as a stand-alone agreement, or as an addendum to or even a section in, an existing agreement. Some EU countries require that these model contracts be registered with the local data protection authority (DPA). Any changes to the model contract terms require approval of the local DPA which can take significant time.
- Data transfers within a company group structure could rely on Binding Corporate Rules (BCR). BCR are a binding set of rules a company agrees to be bound by with respect to personal data. BCR require local DPA approval from the EU country where the data is being transferred. This approval process takes from 12 to18 months, and perhaps longer as more companies are opting for this arrangement.
- Another option is to keep the relevant data inside the EU. This means that any review or processing of that data must occur within the EU. While this is often the only option in urgent situations, such as an investigation involving employee practices or a regulator issue, it may not be a practical option for some companies. It would require travel and expense.
- Under the EU data-protection regime, the relevant data may be transferred out of the EU to the U.S. with the individual's consent. However, implementation is tricky as what constitutes valid "consent" is different in each EU country and cannot be "coerced." Many DPAs consider it to be coercion to ask an employee for "consent" to transfer HR data out of the EU.

While we are in this period of transition, data protection authorities have said they will continue to investigate cases, particularly in response to complaints, and to exercise their powers in order to protect individuals.

We continue to monitor the developments with the Privacy Shield closely and will update you when changes occur, including development on the EU General Data Protection Regulation (GDPR), which replaces the EU Privacy Directive. The EU Parliament approved GDPR on April 14. The next steps are for the GDPR to be published in the Official Journal of the EU this June. The GDPR enters into force 20 days after such publication. The GDPR will apply, and enforcement will commence, two years from the date of entry into force, expected to be in early July, 2018.

*— Kathleen M. Porter*

---

**House Committee Examines Student Data Privacy Concerns**

The House Committee on Education and the Workforce recently held a hearing to evaluate federal policies affecting education research and student privacy. At issue is whether and how Congress will update the 1974 Family Educational Rights and Privacy Act (FERPA), which protects student education records and provides how state and local education agencies collect and maintain data on their students. FERPA has been widely criticized for its outdated definition of a "student record" and its failure to keep pace with new ways that student information is being collected.

Witnesses discussed the competing interests between the need for researchers to access student data to improve classroom instruction, and the importance of respecting student privacy and keeping student information safe. Rachel Stickland, co-chairwoman of the Parent Coalition for Student Privacy, stated that parents should be informed up front about the type of student data that is being collected and how it is used. She also argued that parents should be able to choose to have their child's data stored out of the state data system. Jane Hannaway, professor of public policy at Georgetown University in Washington, disagreed, arguing that allowing parents to remove their child's data from state systems at their discretion would provide researchers with faulty data.

Over the past year, several lawmakers have attempted to revamp the student data privacy laws. Thus far, none of them have gained any traction.

*— Kathleen E. Dion*

---

**HIPAA**

**Raleigh Orthopedic Clinic Settles with OCR for $750,000 for Lack of Business Associate Agreement**

Consistent with the settlement the OCR agreed to with North Memorial Health Care of Minnesota, [view related post] the Office for Civil Rights has settled its investigation of Raleigh Orthopaedic Clinic, P.A. (Raleigh Orthopaedic) for $750,000. The OCR alleged that Raleigh Orthopaedic "potentially" violated HIPAA "by handing over protected health information for approximately 17,300 patients to a potential business partner without first executing a business associate agreement."

The investigation commenced following a self-report of a data breach from April 30, 2013. The investigation showed that Raleigh Orthopedic intended to give X-Ray films to a third party to transfer the images to electronic media and then harvest the silver from the films. Raleigh handed over the X-Rays to the third party without entering into a business associate agreement with the third party.

On top of the fine, Raleigh Orthopaedic must "establish a process for assessing whether entities are business associates…" among other requirements.

The lesson from this case is to focus on vendor relationships and vendor management, including implementing a process that any vendor or third party that is going to receive PHI execute a business associate agreement. Other important considerations for vendor management include, but are not limited to, review of the vendor's data privacy and security practices, the vendor's risk assessments and risk management, confirmation of insurance, and indemnification obligations.

*— Linn Foster Freedman*

---

**PRIVACY TIP #32**

**Online Banking Privacy**

I am no doubt one of the few individuals in the world that does not have an online banking account. I just know too much. Although banks have some of the highest security measures of any industry, they are also prime targets for fraudsters, and your money is at risk with the increase of sophisticated malware and ransomware (see related article above about the SpyEye).

There are many advantages to online banking and most people are fans and make fun of me for not banking online, so this week's tips are geared toward protecting yourself while online banking.

- Do not share your login information with ANYONE ELSE (except for your estate planning attorney as part of your digital assets).
- Review your bank statement frequently to make sure there are no discrepancies. If you believe there is a discrepancy, change your password immediately and call the fraud department of your bank.
- Use a complex username and password and don't write them down. This means not using your name, date of birth, or any other easily guessed or obtained information about you through social media or social engineering. Change your password frequently.
- Don't use the same password that you use for other sites.

- Disable auto-complete features or the ability to save your password on your computer when online banking.
- Log off and close your browser when you are done banking, and don't keep the program running.
- Be careful about which computer you use. If you are unfamiliar with the computer or it is someone else's, it may be compromised and may not have up-to-date security measures.
- Use account activity alerts.
- Update security measures and patches for your computer and use a secure browser compliant with SSL standards.
- Do not download files, install software, open email attachments or click on website links from unfamiliar sources.
- Be aware of phishing and pharming schemes.
- Do not provide your username or password to anyone that asks for it via email. Your bank will not be asking for your credentials via email.
- Most banks send you a letter to your home address when you change your credentials. Open those letters when they come to your home and read what they say. Don't assume they are marketing materials.
- If you receive a letter from your bank indicating that you opened an online account, or changed your username or password and you didn't, contact the fraud department of your bank right away.

These are just a few basic tips. To get more information about how you can protect yourself, check out the FDIC's Bank Customer's Guide to Cybersecurity, FDIC Consumer News Special Edition—Winter 2016, which was just issued on March 8, 2016.

Banks and regulators are trying to prevent online fraud and theft while consumers enjoy the convenience of online banking, but they can't do it without consumers' help. Use these tips and stay vigilant to protect yourself from online banking fraud.

*— Linn Foster Freedman*

---

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.