February 18, 2016

DATA BREACH

Hollywood Presbyterian Medical Center Hit by Ransomware and Pays Ransom to Restore EMR

Many have predicted that health care providers will continue to be targeted by hackers in the next few years. To illustrate the point, Hollywood Presbyterian Medical Center has been hit hard by a ransomware attack.

According to the Medical Center, its electronic medical record system has been offline for almost two weeks as a result of a ransomware attack. Although it was originally reported that the hackers demanded $3.6 million in Bitcoin payment, the hospital released its official statement on February 17 stating that hospital employees notices "issues" accessing the computer network on February 5.

The IT department responded and confirmed a malware attack. The malware "locked access to certain computer systems and prevented us from sharing communications electronically." The Medical Center is working with law enforcement and computer experts.

The Medical Center flatly denied paying 9,000 Bitcoins—the equivalent of $3.4 million—and stated that "the amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000." The Medical Center confirmed that it paid the ransom.

Apparently, as we have seen in other cases, the hackers' word was good, and once the ransom was paid, the hackers restored the system to working order. According to the Medical Center, the electronic medical system was restored on February 15.

Nonetheless, the incident took a toll on the Medical Center, with reports that it was working off of paper records and diverting patients to other providers. The health care sector took a hard hit last year with data breaches, and it does not look like it will be any better in 2016.

— Linn Foster Freedman

Hacker Has Possession of 9,000 Department of Homeland Security Employee Information through Social Engineering and Threatens to Release Data of 20,000 FBI Employees

Boasting on a Twitter account, a hacker has claimed that he accessed over 9,000 Department of Homeland Security employees' demographic information, including names, email addresses, telephone numbers, and titles.

The hacker claims that he obtained access to 1 TB of data directly from the Department of Justice. The hacker explained that he gained access to a compromised DOJ email account, and he tried to log on to the staff portal but was denied. So he called the appropriate department at the DOJ and told them he was a new employee and didn't know how to log on to the portal.

The helpful person on the other end of the line asked him if he had a token code, and he said no, so "they said that's fine—just use our one."

The hacker was given a code that allowed him access to the DOJ intranet, which contained personnel files of almost 10,000 employees.

The hacker further boasted that he will be releasing details about over 20,000 FBI employees today.

Social engineering is getting easier and easier, which is why it is so important for everyone in the company and/or department to understand why it is essential to verify identities before providing essential log-on information, wire transfer instructions, or other activities that have been used to defraud companies.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Apple Ordered by Federal Magistrate Judge to Assist with Unlocking San Bernardino Shooter's iPhone

Apple was ordered by a federal magistrate judge to provide "reasonable technical assistance" to federal investigators to unlock the password and access the encrypted data on a specific iPhone 5c used by Syed Farook, one of the San Bernardino shooters. The iPhone, owned by Farook's employer, the San Bernardino County Department of Public Health (County) and provided to him as an employee, was recovered from the family's vehicle. While the County consented to requests to search the cellphone's contents, and a warrant was obtained to do so, the government's motion stated that Apple refused to voluntarily provide assistance.

Investigators believe the cellphone data may provide valuable information about Farook and his wife's travels and who they communicated with, including individuals that may have provided assistance to plan the shootings. Additionally, investigators have been able to obtain backup versions of Farook's iCloud data up to about six weeks prior to the shootings. The government believes Farook may have disabled the iCloud feature at that time, leaving the only data on the iPhone itself.

However, investigators have been unsuccessful in completing the search of the recovered iPhone because they cannot figure out the password to access the phone's data. The government wants Apple to provide assistance to bypass this iPhone's auto erase function and to allow an unlimited number of passwords to be tried to unlock the phone. The government's motion argued that only Apple had the technical means to assist the government in completing this search.

The court's order gave Apple five days to object if Apple believed that complying with the order would be "unreasonably burdensome." Almost immediately, Apple issued an open letter on its website, arguing that complying with this order would weaken encryption for all iPhone users. Apple's argument is that, once a backdoor method or key to unlock the data is known, the government will want to use this method or key to access the encrypted data on other cellphones. Additionally, Apple argued that hackers would find a way to exploit this backdoor key to steal data. The White House responded to Apple's argument by confirming that the Department of Justice is seeking access to the data on Farook's iPhone; it is not

asking Apple to jeopardize the security of cellphone products generally by creating or providing a backdoor to encrypted data. Many believe that Apple's engineers could take this single iPhone and unlock it with software and other tools available to them.

Readers can view the order here and Apple's response here.

— Kathleen M. Porter

Dave & Buster's Faces FCRA Class Action for Alleged Background Check Violations

Joseph Alvarez filed a class action against Dave & Buster's restaurant chain earlier this year in Florida alleging that it used background checks for employment decisions without providing a copy of the report to the applicants, in violation of the Fair Credit Reporting Act (FCRA). Alvarez applied for a job as a line cook at Dave & Buster's Orlando, Florida, location, and after the restaurant received a background check with negative implications about Alvarez, it withdrew the offer for the position. However, Dave & Buster's never provided a copy of the consumer report used in this decision-making process. Alvarez's complaint said that Dave & Buster's "willfully violated [the FRCA] requirements in systematic violation of plaintiff's rights and the rights of other punitive class members." Alvarez's complaint further alleges that the restaurant chain frequently uses background checks for decisions in termination, reduction of hours, position changes, hiring, and promotions. "This practice violates one of the most fundamental protections afforded to employees under the FCRA, and also runs counter to longstanding regulatory guidance," the complaint said.

The FCRA requires all companies to notify individuals when a background check is conducted and also if the results indicated are going to have a negative effect on their employment. Companies are also required to provide a copy of the report to the applicant so that the individual has the opportunity to correct any errors.

Alvarez's class action includes all employees and job applicants that have had their employment affected negatively over the last five years and that were not provided the required FCRA disclosures, and seeks statutory damages (which could be up to $1,000 per violation) plus punitive damages.

— Kathryn M. Rattigan

Patients Provide Cell Phone Number to Hospital, Debt Collection Calls Are Okay under TCPA

The 6th Circuit upheld the 2014 Ohio federal court's decision in *Mais v. Gulf Coast Collections Bureau,* stating that two hospital patients who provided their cell phone numbers to the hospital where they sought treatment, in effect, provided consent in accordance with the Telephone Consumer Protection Act (TCPA) to receive automated calls from the debt collection agency. The court said, "In sum, we find *Mais* persuasive and adopt its conclusion that consumer may give 'prior express consent' under the FCC's interpretations of the TCPA when they provide a cell phone number to one entity as part of a commercial transaction, which then provides the number to another related entity from which the consumer incurs a debt that is part of the parcel of the reason they gave the number in the first place." This is an important ruling for hospitals (and all health care providers) who ask for the patient's cell phone number on intake forms. Remember, not only is it okay to use a patient's cell phone number in this particular instance, but if you ask for consent using TCPA-compliant language directly on your intake forms, you can be even more sure that you are on the right side of the TCPA.

— Kathryn M. Rattigan

‘Happy Birthday to You,’ Facebook Hit with Class Action over Text Message Reminders

“Today is [Facebook friend’s] birthday. Reply to post a wish on her Timeline or reply with 1 to post ‘Happy Birthday!’” Facebook, Inc. (Facebook) faces a class action in California federal court for alleged violations of the Telephone Consumer Protection Act (TCPA) by sending its users unsolicited, automated text messages to remind the users of their friends’ birthdays. Lead plaintiff, Colin R. Brickman, alleges in his complaint that users who have clearly indicated in their Facebook account settings that they do not consent to receive text messages are still getting text messages from the social media giant. “Despite plaintiff’s express lack of consent, Facebook sent birthday announcement texts to plaintiff’s phone in violation of [the TCPA]... which protects the privacy rights of individuals to be free from receiving unwanted text message spam on their cellular phones.”

Brickman believes that the text messages are being sent to drive interaction on the social media website by its users and in turn generate more advertising revenue for Facebook. Brickman further states that this is what makes these text messages "telemarketing messages" and therefore a violation of the TCPA. The suit seeks $500 per violation in statutory damages. We will follow this to see if the court deems the ‘happy birthday’ messages as a sneaky telemarketing ploy.

— Kathryn M. Rattigan

HIPAA

HHS/OCR Releases Guidance for Mobile Apps and Health Information Exchange and “Fact Sheets”

The Office for Civil Rights has provided additional educational materials for app developers through the app developers portal that it developed last fall.

The new material is intended to assist health care entities and software developers to learn from different scenarios that explain when HIPAA applies to mobile health apps and when it doesn’t. In particular, there is often confusion on whether HIPAA applies when consumers are using smartphones to collect, maintain, and transfer health information.

The scenarios and guidance are useful tools for app developers to use when determining whether HIPAA applies. However, whether HIPAA applies or not, privacy and security is an important consideration when developing any app that is tied to health information.

OCR also issued fact sheets that detail scenarios on permitted access, use, and disclosure of protected health information that may have been confusing in the past. These fact sheets are a roadmap of how the OCR views permitted uses and disclosures of PHI and are very helpful for compliance.

The OCR has said that it will be issuing guidance on cloud computing this year, which has been a topic of confusion for many entities and will be welcomed. We will alert you when these new guidelines are released.

— Linn Foster Freedman

Deadline for Reporting 2015 Data Breaches to OCR Quickly Approaching

Pursuant to HIPAA/HITECH, covered entities are required to report breaches of unsecured protected health information that occurred in 2015 and affected less than 500 individuals to the Office for Civil Rights no later than 60 days after the end of the calendar year.

To be safe, covered entities may wish to complete their online reporting through the OCR reporting website by Friday, February 26, 2016.

Tips for reporting:

- Prepare the answers to the questions presented on the online reporting site in advance and not on the fly, to reduce the chance of an error or misunderstanding.
- Space out reporting different incidents over several days so you can concentrate and give your full attention to each one.
- Give each incident you are reporting on the appropriate time and energy necessary to convey accurate information.
- Prepare the answers carefully and assume that each one will be scrutinized with a critical eye.
- Print the completed report for your records and keep it for six years.

— Linn Foster Freedman

CYBERSECURITY

The FBI's "Cyber's Most Wanted"

We've all heard of the FBI's "Most Wanted" list, but fewer people know that the FBI has a special most wanted list just for computer criminals. The FBI's "Cyber's Most Wanted" list features the its most wanted computer criminals on the run today.

The current list consists of 20 men, all charged with some type of federal cyber-related crime. Each entry reads like a computer crime spy novel. The charges include computer hacking, trade secrets theft, computer fraud, and wire fraud. Many were allegedly involved in complicated international conspiracies aimed at harvesting and using individual victim's personal information and/or companies' electronically stored intellectual property.

The majority of Cyber's Most Wanted have close ties to other countries, including Russia, the United Kingdom, China, Vietnam, Germany, El Salvador, and Romania. It includes salesmen, telecommunications managers, software programmers, network engineers, restaurateurs, Internet entrepreneurs, and members of the People's Liberation Army of the People's Republic of China.

The FBI's website is complete with downloadable PDF posters featuring the "Cyber's Most Wanted" mug shots and personal photos, physical descriptions, and aliases. Aliases range from the simple ("Mike Shields") to the absurd ("UglyGorilla"). The FBI offers rewards as high as $3 million for evidence that leads to their capture or conviction.

We will be featuring periodic profiles of the stories behind the Cyber's Most Wanted. To download your own copy of the FBI's "Cyber's Most Wanted" click here.

— Nuala E. Droney

GAO Report: EINSTEIN Not Meeting Stated Objectives

According to a recent GAO report, the Department of Homeland Security's (DHS) National Cybersecurity Protection System, commonly referred to as EINSTEIN, is not meeting its stated objectives. The purpose of EINSTEIN is to protect federal civilian executive branch agencies from cyber-attacks. EINSTEIN monitors traffic to and from these agencies to identify malicious activity, serves as an intrusion detection system, and provides DHS with threat information that can be used to help both the government and the private sector to manage cyber risk. EINSTEIN uses a signature-based intrusion detection system that compares network traffic to known malicious behavior (signatures). The GAO report noted that, while a signature-based system is capable of preventing attacks from known threats, it is not structured to prevent against unknown attacks, such as "zero days" that exploit an existing vulnerability in a product. The GAO report also noted that DHS had not yet fully developed the tools for information sharing, such as tools that will notify affected entities of suspected malicious activity. In response to the GAO report, representatives from DHS stated that the program has been effective in identifying significant incidents and has improved detection of hackers within the system. DHS representatives also emphasized that EINSTEIN is intended to be one of many tools used by the federal government to prevent and detect against cyber-attacks. In his recent budget proposal, President Obama requested $471.1 million for EINSTEIN to enable the system to maintain its current capabilities and invest in new technologies and analytics.

— Pamela Del Negro

PRIVACY TIP #22

ACLU of California Releases Practical Privacy Guidance for Businesses

The ACLU of California has published the Third Edition of *Privacy & Free Speech: It's Good for Business*, a 42-page "roadmap" of how businesses can promote privacy and free speech and be a leader in respecting individuals' privacy and the right to free speech. The gist is that being a leader in protecting individuals' privacy rights will lead to customer satisfaction and revenue, while avoiding regulatory enforcement and litigation. Take a look at page 2, which outlines all of the "hot water" companies get into when not protecting the privacy of consumers, while others are praised for valiant efforts to respect the privacy of its customers.

It is only 42 pages and is a quick, but impactful read.

The guidance urges companies to "make your privacy practices stand out" and "give your users a platform to speak freely" and gives practical suggestions on how to make that happen. The examples of when companies made the right and wrong decisions on how to use consumers' data and the results are easy to understand and in stark contrast to each other.

As a consumer, take a look at the guidance and keep these principles in mind when doing business with companies. It may impact your decision on which company to give your business to.

As a company, take a look at the guidance and evaluate whether the guidance makes sense and may

have an impact on your bottom line.

— 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.