Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

December 30, 2015

DATA BREACH

Hyatt Corporation Notifies Customers of "Malware Activity"

Hyatt Corporation announced on December 23, 2015, that it recently identified malware on computers that operate its payment processing systems. It stated that, as soon as the activity was discovered, an investigation was launched and cyber security experts were engaged.

Very little detail was provided, including when the malware was on the system, how many cards may have been exposed, or which properties were compromised. Hyatt suggests that customers review their payment card account statements closely and report any unusual activity to the card issuer. Further, it stated that, while the investigation is ongoing, updates will be posted here.

— Linn Foster Freedman

Quincy Credit Union ATMs Compromised in Skimming Scheme

Hundreds of Quincy Credit Union (Massachusetts) customers reported that unauthorized ATM withdrawals were made from their accounts over the holiday weekend. Officials now believe that skimmers were placed on ATMs in early December. As is typical, the thieves waited until a weekend (and a holiday one at that) to make withdrawals because they knew it would take longer for the missing money to be noticed.

At first, the credit union blocked customers' account access until it could check accounts. As of now, stolen amounts have been restored and new ATM and debit cards have been issued as warranted. Most of the withdrawals were made from ATMs in the New York City area. The investigation into this security breach is ongoing.

It is not easy to detect a skimmer, a device glued or taped over an existing ATM machine's card slot and/or keyboard. Skimmers are used to grab account information from a card's magnetic strip and to capture PIN numbers as they are entered using a small camera or a keyboard overlay.

Because they are hard to detect, many consumers check an ATM for any signs of a skimmer or other tampering before entering a debit card. Generally, ATMs are solidly built with no fragile parts. Don't use an ATM if you see or feel something that looks flimsy or loose or if the ATMs or keyboard design or card slot feel loose or looks different somehow. To reduce the chances of a camera reading your PIN, cover your hand when entering your PIN number.

When possible, use an ATM that is in a busy public location or within a bank or retail store. Also, when you can, use an ATM during the weekday. It is typically harder for a thief to install and retrieve a skimmer during the day when businesses around it are open. Thieves generally install and retrieve skimmers at night and on weekends. Of course, notify the bank or the police if you have any concerns about a particular ATM.

Click here to view a related news article.

— Kathleen M. Porter

HIPAA

ProPublica Releases HIPAA Helper

A damning series of reports by ProPublica has revealed that, based upon its analysis of federal data, "hundreds of health providers nationwide" have repeatedly violated HIPAA between 2011 and 2014.

According to the report, the Veterans Administration was the most frequent violator of HIPAA, with 220 violations between 2011 and 2014. (This estimate is based upon complaints that resulted in corrective action plans or the Office for Civil Rights (OCR) providing technical assistance.)

The report noted that the OCR received almost 18,000 complaints about privacy violations in 2014, primarily through its online complaint portal, which is a dramatic increase from approximately 7,500 complaints in 2009.

Following its analysis and report, ProPublica announced that it has launched HIPAA Helper, which "allows users to look up reports of privacy violations by provider for the first time."

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Former Morgan Stanley Financial Advisor Sentenced

Just before Christmas, a New York federal judge sentenced Galen Marsh, the former Morgan Stanley financial advisor who downloaded client data to his home computer without permission, to three years of probation. He pled guilty to one count of unauthorized computer access.

Marsh admitted to downloading and illegally accessing Morgan Stanley client information so he could see how other financial advisors invested money in order to advance his career.

Prosecutors alleged he conducted 6,000 searches in the database, accessing clients' confidential information, and then uploaded the information to his personal computer. The information made its way to YouTube, which Marsh blamed on Russian hackers.

Although Marsh did not receive jail time, in addition to probation, he agreed to pay Morgan Stanley $600,000 in restitution.

— Linn Foster Freedman

Hacker of Celebrity Victims Arrested

The U.S. Attorney in the Southern District of New York has announced that Alonzo Knowles (aka Jeff Moxey) was arrested last week for his alleged hacks into celebrity e-mail accounts.

According to the U.S. Attorney, Knowles hacked into the email accounts of three professional athletes and a movie actress, stole their Social Security numbers, personal videos, and unreleased scripts of a popular television show. He then tried to sell them to a radio host. The radio host checked into the deal with the television network and then introduced Knowles to an undercover agent. Knowles proceeded to tell the agent that he had a list of 130 emails and telephone numbers of celebrities and that the celebrities were unaware that he had hacked into their accounts.

He further boasted that he had used two methods to hack into the accounts—a virus that allowed him to control the celebrity's device or a phishing email telling them the account had been hacked and telling them to supply their passwords. He showed the agent screen shots of an actor's passport and Social Security number.

The case is still under investigation. This is another example of the same phishing scheme that many fall prey to and is a reminder to be suspicious of any e-mails or texts that ask for a password.

— Linn Foster Freedman

Neiman Marcus Requests Dismissal of Data Breach Case (Again)

We previously reported on the ongoing litigation between Neiman Marcus and class action plaintiffs as a result of the data breach during the holidays in 2013 (related post here). The breach involved the credit card information of up to 350,000 customers.

Although the Seventh Circuit Court of Appeals overturned Neiman Marcus's successful dismissal of the putative class action litigation in September, which many have commented is an "outlier" decision, the plaintiffs were allowed to file an amended complaint. Neiman Marcus moved to dismiss, saying that the plaintiffs have not suffered any injury and did not "overpay" or would not have shopped at the store if they knew inadequate security measures were in place to protect their personal information. This is a fairly new theory presented by plaintiffs in data breach litigation and we will be watching the outcome of this case very closely.

— Linn Foster Freedman

FTC Files Brief in LabMD Appeal

We previously reported that the Federal Trade Commission (FTC) lost its case against LabMD alleging that LabMD had inadequate security measures to prevent an alleged data breach (related post here).

The FTC appealed the decision and filed its appellate brief on December 22, 2015. The brief can be accessed here.

— Linn Foster Freedman

NLRB: Employers Cannot Block Employees from Recording or Taking Photos in the Workplace

The National Labor Relations Board (NLRB) in a 2-1 decision, ruled against blanket employer policies banning employees from taking photos or recordings in the workplace. Such policies would, in the view of the NLRB have a chilling effect on an employee's ability to record or photograph workplace safety violations or actions that were discriminatory.

Whole Foods' unsuccessful argument to the NLRB was that its policy allowed for a free and open discussion in the workplace without concerns of statements appearing on the Internet. But the NLRB found that a blanket ban went too far, as it was "essential" in many cases to have a photo or video in order to prove a violation of an employee's rights.

It is important to note that anyone taking pictures or video in the workplace or elsewhere is still subject to any applicable state laws requiring consent from one or more of the individuals being recorded or photographed. For example, some states require that all parties to a conversation give consent, whereas other states require consent by only one party, which could be the photographer or videographer.

The National Labor Relations Board's decision overturned an administrative law judge's decision in favor of the supermarket chain. Whole Foods must revise or revoke its current policy and communicate to its employees when it has done so.

See Whole Foods Market, Inc., 12/24/2015, 363 NLRB No. 87.

— Kathleen M. Porter

CYBERSECURITY

Moody's Issues Cyber Risk Report

Moody's Investors Service (Moody's) recently announced that is has issued a report entitled "Cross-Sector-Global: Cyber Risk of Growing Importance to Credit Analysis," which outlines the threat of cyber-attacks and how they can affect a company's credit.

According to its press release, Moody's views material cyber threats "in a similar vein as other extraordinary event risks, such as a natural disaster, with any subsequent credit impact depending on the duration and severity of the event."

The report identifies factors to look at when determining a credit impact as a result of a cyber threat, varying types of cyber threat actors, and the motives around the cyber threat.

This is another reason for entities in all industries to consider placing cybersecurity on the top of the priority list for 2016.

— Linn Foster Freedman

HEALTH INFORMATION TECHNOLOGY

Digital Health Funding Hits $4.3 Billion in 2015

A new report from Rock Health states that digital health funding in 2015 reached $4.3 billion from 180 merger and acquisition deals in the past year, primarily with IPOs in the first half of 2015. This represents seven percent of venture funding in 2015 and only includes deals over $2 million.

The specific findings include that the average deal size was $15.6 million, the six largest deals totaled nearly $1 billion, and five digital health companies went public in 2015.

The bottom line is that funding of digital health remains strong.

— Linn Foster Freedman

Telehealth

We previously reported on the case between Teladoc, Inc., and the Texas Medical Board (Board) (related post here). The medical board issued regulations requiring doctors to see patients in person before prescribing medication. Teladoc sued the Board over the regulations and the Board moved to dismiss the lawsuit. Judge Robert Pitman recently denied the Board's Motion to Dismiss so the case will proceed.

— Linn Foster Freedman

E-DISCOVERY

Back to Basics: Litigation Hold Notices

The recent amendment to Federal Rule of Civil Procedure 37(e) makes clear that document preservation is not something to be taken lightly. Issuing a litigation hold notice is the first crucial step in the preservation process. A litigation hold notice is a document usually sent by counsel that alerts individuals likely to be in possession of documents or other materials potentially relevant to a dispute of their obligation to retain those materials. Notably, the issuance of a litigation hold expressly suspends the protocols of any record retention policies (and a good record retention policy should expressly provide for this possibility).

Although there is no "one size fits all" document, a good litigation hold should include, at minimum, a description of the matter (including the relevant time period); a description of the substance of the data to be preserved; a description of the types of data to be preserved (papers, e-mails, electronic documents, etc.); an explanation of the obligation to preserve and the consequences for failing to do so; an express directive to cease any document destruction; instructions on whom to contact with any questions, and an acknowledgement that the individual has read, understands, and agrees to be bound by the hold. The exact contours of the hold notice should be tailored to the individual case and entity.

Litigation holds are typically issued early in the litigation process—frequently before a complaint is even

served. In protracted litigation, consider reissuing the hold periodically for the life of the action. Each time the notice is reissued, consider whether the scope of the initial hold notice has changed as additional facts have developed. Also, assess whether any additional individuals should be added to the hold. In addition to individuals who are likely to have substantive documents in their possession, a separate litigation hold notice should also be sent to the IT staff responsible for system maintenance and any scheduled purges. This often overlooked step is critically important and will be one of the first questions asked in the event a preservation issue arises.

— Andrea Donovan Napp

PRIVACY TIP #16

Top Privacy Tips for 2015

In response to our clients, colleagues, readers, and friends' requests, we started publishing weekly privacy tips 16 weeks ago. We hope that you have found them to be helpful, both in your personal and professional life.

We will continue to publish our weekly tips in 2016. Here is a recap of our tips in 2015, with the links to the full articles for your easy reference. Happy New Year to all, and we look forward to working with you in 2016!

DATA PRIVACY TIP #1
Password Management

DATA PRIVACY TIP #2
Protecting Your (and Your Employees' and Customers') Social Security Numbers

DATA PRIVACY TIP #3
Know How Apps Are Constantly Accessing and Using Your Location

DATA PRIVACY TIP #4
What do I do When I Get a Letter Informing Me of a Data Breach?

DATA PRIVACY TIP #5
Retail Store Reward Cards

DATA PRIVACY TIP #6
Protecting Your Child's Identity

DATA PRIVACY TIP #7
Who is Listening to Your Conversations through Your Smartphone Microphone?

DATA PRIVACY TIP #8
How Teachers can Assist Students to be Safe Online

DATA PRIVACY TIP #9
Destroying Prescription Information

DATA PRIVACY TIP #10
What are Digital Assets and Why Should I Care?

DATA PRIVACY TIP #11
Receiving a Gramm-Leach-Bliley Privacy Notice

DATA PRIVACY TIP #12
Credit Card Safety During the Holidays (Use Cash!)

DATA PRIVACY TIP #13
Web Trackers: What Others May Know about Your Online Footprint

DATA PRIVACY TIP #14
Record Destruction: An Overwhelming Problem

DATA PRIVACY TIP #15
Protecting Your Privacy During Holiday Travel

— 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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---