Robinson+Cole

Data Privacy + Security

August 13, 2015

Data Privacy + Security Insider

DATA BREACH

United Airlines Suffers Network Breach—Same Hackers as OPM Suspected—Dark Motives

United Airlines has confirmed that it has suffered a data and network breach that occurred during the same time frame as the OPM breach. Investigators suspect the same Chinese state-sponsored hackers are responsible for both breaches. One theory being advanced about the connection between the two breaches is that the Chinese state-sponsored hackers are targeting specific databases in order to cross reference and index federal employees' travel so the information can be quickly searchable and can be used to determine U.S. intelligence priorities.

It is reported that the United Airlines hackers obtained flight manifests that included passenger names and other personal information, flight paths and origins and destinations. The scary part about it is that United is a primary airline operating out of Dulles International Airport, which is the closest to CIA headquarters. The OPM information, cross-referenced to flight manifests of federal employees may give China a tremendous amount of information about where certain federal employees are traveling to obtain intelligence. The sophistication of hackers, particularly state-sponsored hackers cannot be over emphasized.

— Linn Foster Freedman

Fred's Inc. Discloses Data Breach to SEC

In its most recent filing with the Securities and Exchange Commission (SEC), Fred's Inc. disclosed this week that a security firm found malware in its system that was designed to lift customer credit card information. Although it appears from reports that the hackers may have had access to customer credit card information, the security firm did not find any evidence that the credit card information actually left Fred's system. There is no indication that Fred's has notified any customers of the incident.

Nonetheless, Fred's indicated in its SEC filing that it is unable to estimate the cost of the breach, and that it may incur future liabilities if it has to reimburse credit card companies for costs and in the event that litigation ensues.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Second Class Action Suit Filed Against Medical Informatics

We previously reported that Medical Informatics Engineering, Inc. was sued over a data breach that occurred in May and affected over 4 million individuals. Thereafter, Indiana AG Gregory Zoeller advised all Hoosiers to freeze their credit to protect themselves.

Late last week, a second proposed class action suit was filed against Medical Informatics in California federal court alleging that the proposed class is at risk of identity theft. The suit further alleges that the class has suffered actual injury, including identity theft, invasion of privacy, cost of monitoring credit accounts and the value of their personal information. In a different twist, the named plaintiff alleges that her information has value and can be sold to third parties, and therefore, it is a form of currency that has been devalued as a result of the breach.

We will continue to watch and report on the progress of these suits as they develop.

— Linn Foster Freedman

CareFirst BlueCross BlueShield Sued for Hacking Incident

Not to be left out, plaintiffs filed suit against CareFirst BlueCross Blue Shield late last week for the hacking incident the insurer suffered in May, which resulted in unknown intruders gaining access to names, dates of birth, email addresses and subscriber identification numbers of approximately 1.1 million members. CareFirst has indicated that the incident did not include a compromise of members' Social Security numbers or credit card information.

Despite this, plaintiffs allege in the complaint that they had a reasonable expectation that their personal information and health information would be kept confidential. Although the plaintiffs allege that the plaintiffs have been damaged "and have lost or are subject to losing money and property" as a result of the incident, it will be interesting to see what actual damages are alleged to have been suffered when Social Security numbers were not exposed.

Further, the plaintiffs allege that their personal information can be used by identity thieves "to perpetrate a variety of crimes that harm the victims," but the case does not explain how the information involved can actually be used or has been used against the named plaintiffs.

This is another case we will be watching and reporting on as this area of the law develops, and class action lawsuits become the norm following data breaches.

— Linn Foster Freedman

OPM Update: OPM Hit With Another Class Action Suit—This One Filed by a Judge

Ho hum. Another class action filed against OPM for its massive data breach. The interesting fact here? The suit's named plaintiff is a Judge with the Social Security Administration. On Friday, August 7, Social Security Administration Judge Teresa J. McGarry hit the OPM with its latest proposed class action suit alleging that OPM was aware of its security deficiencies and did nothing to cure them, which will "have consequences that will last for years to come." McGarry further alleges that hackers are already selling OPM login credentials online.

The suit requests damages to compensate the affected individuals for current and future losses and injunctive relief to update OPM's security measures.

— Linn Foster Freedman

Data Processing Company Hit With Class Action Lawsuit for Data Breach and Judge Denies Class Certification the Next Day

Advanced Data Processing, Inc. and Intermedix Corp. were sued in federal court in Florida last week for violating the Health Insurance Portability and Accountability Act (HIPAA) for failing to protect the health information of "potentially millions" of individuals.

Plaintiffs allege that for several months in 2012, an employee of Intermedix viewed health information of patients that used ambulances without authorization. This information, including patients names, dates of birth, Social Security numbers and health insurance information was then given or sold to others who used the stolen information to file fraudulent tax returns with the IRS and obtain refunds.

Significantly, plaintiffs allege that they were not told of the incident, and that Intermedix merely posted a notice about the incident on its website in 2014 that was not prominent on the website. Plaintiffs allege this did not constitute notice as most of the members of the proposed class did not have a relationship with Intermedix, which processes claims for health care providers. The named plaintiff was taken by an ambulance to a hospital in California in 2012, but did not learn of the incident until April of 2015. He alleges that he has been the victim of identity theft as a result of the incident.

Plaintiffs immediately moved to certify the class and the Judge denied the Motion the next day saying it was premature.

— Linn Foster Freedman

Anti-Robocalling Statute Banning Automated Political Calls Found Unconstitutional

On August 6, 2015, the Fourth Circuit upheld a lower court's decision that the South Carolina anti-robocall statute was unconstitutional. The South Carolina robocall statute targeted automated telephone calls that were political in nature, which the court found was not content neutral. The court cited a recent decision by the U.S. Supreme Court which held that a regulation on speech is subject to strict scrutiny as "content-based" or intermediate scrutiny as "content neutral." The Court held, "Under the content-neutrality framework set forth in *Reed v. Town of Gilbert*, we find that the anti-robocall statute is a content-based regulation that does not survive strict scrutiny."

This decision stems from the 2010 arrest of political consultant, Robert C. Cahaly, who set up an automated opinion polling system to ask whether Nancy Pelosi should be invited to campaign. While the charges were dropped, Cahaly filed suit against state officials on claims that his constitutional rights were violated.

— Kathryn M. Rattigan

Northern District of California Requires a Warrant to Access Cell Phone Geographic Information

We previously reported that government access to cellphone geographic information or CSLI without a warrant has become a vigorous debate between the government, defense attorneys, and the federal bench. In a lengthy opinion, Judge Lucy Koh of the Northern District of California joined those who held that the Fourth Amendment applies to CSLI. Prior to this ruling, the government contended that it need only meet the lesser "reasonable suspicion" standard set forth in the Stored Communications Act to obtain this data. Judge Koh rejected this analysis and, relying on the Supreme Court decisions concerning attaching a GPS device to a car (*United States v. Jones*) and searching mobile phones (*Riley v. California*), held that individuals have a reasonable expectation of privacy in the historical CSLI generated by the cellphones.

Judge Koh also held the "third party doctrine" did not apply to this information. The "third party doctrine" holds that people do not have a reasonable expectation of privacy for information voluntarily given to a third party. By contrast, Judge Koh concluded, CSLI is not voluntarily provided because in order to consent to the government acquisition of CLSI, the cell phone user would have to read the privacy policy of "every service provider in the country."

It is not clear if this ruling will be appealed by the government. If so, the Ninth Circuit may join the current circuit split about government access to this information. This circuit split, however, may be resolved by the U.S. Supreme Court, if it grants the *certification* petition that was just filed appealing the 11th Circuit's ruling in *U.S. v. Davis*.

— Kathleen E. Dion

CYBERSECURITY

FDA Issues First Medical Device Hacking Alert

Reportedly for the first time ever, the FDA recently issued a declaration that hospitals should not use a medical device manufactured by Hospira Inc. because of security flaws that could allow hackers to penetrate hospital computer networks, commandeer the pumps and manipulate the dosage given to patients. There has been no reporting hacking incident, but the warning about a specific device shows the increased vulnerability of medical devices to security compromises and the FDA's concern over the security features of devices within its jurisdiction.

— Linn Foster Freedman

HHS IT Security Found to be Weak

The House of Representatives Energy and Commerce Committee issued a report late last week that the information security of the Department of Health and Human Services (HHS) has substantial weaknesses. Several incidents that occurred between 2012 and 2014 indicated that several agencies were compromised or attacked without the agency's knowledge.

In one instance, the report criticized the FDA's ability to mitigate low level threats, leaving it vulnerable to more sophisticated cyber-attacks. This in the wake of the FDA issuing hacking alerts about medical devices and HHS enforcing security lapses of health care providers. The government criticizes and commences enforcement proceedings against businesses and health care providers for lax security measures, but reports such as this show that the government is having a difficult time with security, just like everyone else.

— Linn Foster Freedman

SOCIAL MEDIA

Maine Joins the Mainstream With New Social Media Law

Joining more than 20 other states, and many of its sister states in the Northeast, Maine has passed a social media law that prohibits employers from requiring employees or applicants to provide them with their social media account information and passwords. This social media law was not passed in the traditional fashion of passage by the legislature and then signed by the Governor. Instead, it was included in a batch of 65 bills that Governor Paul LePage tried to veto, but was unable to do so because the legislature adjourned. The Maine Supreme Court issued an opinion last week that the 65 bills were now law, including the social media law.

Consistent with other state social media laws, employers under the Maine law can be fined, depending on the number of violations of between $100 and $500 per violation.

The law takes effect in October, so companies in Maine—take note and get ready for the compliance date.

— Linn Foster Freedman

DATA SECURITY

Encryption: What is it, Why do it!

Encryption is a basic term used to describe the act of encoding data, files, and digital communications such that only those with the cipher could read or understand the information. Think back to the decoder ring you got in your cereal box; the messages it decoded were encrypted. There are many different encryption algorithms used today (3DES, AES, etc.). The technical aspects of encryption are less important to attorneys practicing data privacy and security law than the actual application of encrypting your sensitive data. Below are four common areas where data breaches occur and where you should be particularly conscious of your use of encryption.

USB & Portable Drives:

USB keys or thumb drives pose an enormous risk to data privacy and security. These small devices are easily lost or misplaced. Can you quickly and easily identify which of your devices have sensitive data stored on them? Any portable device that is used to store client data of any kind should be encrypted. Both Windows and MacOS have a method of quickly and easily encrypting such devices.

File Sharing & Transfer sites:

Today it is very common for attorneys and clients to share and transmit large files via cloud based services like Dropbox, Google Drive, etc. Not all of these services are equal. In fact, many of these sites have multiple service levels. There is a difference between Dropbox and Dropbox for Business for instance. You want to be sure that any file sharing site you use not only encrypts your files in transport (as you upload them to the site) but also in rest as your files are stored in the cloud.

Email:

Most email communication today uses Transport Layer Security (TLS) to encrypt the message in transit. If you are sending sensitive information via email you want to make sure that not only your organization is using TLS but that the recipient's mail servers are configured to use TLS as well. There are also many methods of encrypting an individual email message prior to sending it via your organization's email system.

Laptops:

Have you or a colleague ever left our laptop on the plane or had it stolen out of your car? A simple user name and password is not enough to keep the data contained on your hard drive safe. Your laptop's hard drive should be encrypted in order to prevent unauthorized access to your sensitive data.

**** Please contact your IT Department for more information about your organization's policies and preferred methods of encrypting your data for each of these areas. ****

— *Sean Lawless*

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.
