Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

February 25, 2016

DATA BREACH

Radiology Regional Center Paper Medical Records Fall Out of Back of Truck

In the category of "Seriously—not again?" Radiology Regional Center, located in Fort Myers, Florida, notified over 480,000 individuals and the Office for Civil Rights that their medical records, including names, dates of birth, addresses, telephone numbers, Social Security numbers, health insurance numbers, and medical assessments fell out of the back of a truck when the driver failed to lock the door. The records were being transported by a vendor to an incinerator for disposal.

It is reported that the records were blowing down the street, and staff of Radiology Regional Center frantically retrieved the records as they were blowing in the wind. They are offering identity theft protection services to the almost half a million patients.

Needless to say, they are now using a different vendor for transporting protected health information for disposal.

The sad message is that, although we are seeing an increase in electronic hacking contributing to data breaches, paper records continue to be a high risk for data breaches. Both paper and electronic records are an integral part of a risk management program.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Bitcoin Miners Butterfly Labs Agree to Settlement with FTC

The Federal Trade Commission filed a complaint against Butterfly Labs, alleging that it charged customers for Bitcoin mining machines (BitForce) and then failed to deliver them until they "were practically useless, or in many cases, did not provide the computers at all." Over 20,000 customers did not receive the BitForce computers they had purchased.

The FTC further alleged that Butterfly was using the machines personally before delivering them to the customers who had purchased them.

According to the settlement, Butterfly is prohibited from taking up-front payment for Bitcoin machines or any other products used to mine virtual currency, unless they are delivered within 30 days of purchase.

Although the monetary judgment against Butterfly Labs totaled $38,615,161, the payment was suspended due to inability to pay. It is required to pay $15,000, and the rest will be paid if it misrepresented its financial condition.

— Linn Foster Freedman

ASUS Settles with FTC over Insecure Home Routers

ASUS TeK Computer, Inc. (ASUS) has agreed to settle with the FTC over allegations that "critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk." The FTC further alleges that the routers' insecure cloud services compromised consumers' connected storage devices, which exposed their information on the Internet.

Consistent with other FTC orders, the consent order with ASUS requires it to develop and maintain a "comprehensive security program subject to independent audits for the next 20 years."

The allegations by the FTC included information obtained by a malware researcher who discovered vulnerabilities in the routers that gave hackers the ability to get into the router's web-based control panel and change security settings without the owner's knowledge. Further, the company allowed users to keep and use default login credentials on every router with the username and password set to "admin". Obviously, this is not the best security measure.

Finally, the FTC complaint outlines that hackers were able to use tools available on the internet to locate ASUS routers, exploit the vulnerabilities to gain access to almost 13,000 consumers' connected storage devices, exposing their personal information to unauthorized access.

The proposed settlement is open to public comment until March 24, 2016.

As with other settlements and consent orders agreed to by the FTC, lessons can be learned by the facts of this case. The FTC continues to be focused on data security, specifically looking at the Internet of Things, connected devices, and vulnerabilities that can expose consumers' private information. Companies in this industry might wish to reexamine security measures and address any vulnerabilities that may exist in products.

— Linn Foster Freedman

Data Brokers Settle with FTC for Selling Consumers' Information to Scammers

SiteSearch, John Ayers, LeapLab, and Leads Company (the defendants) settled with the Federal Trade Commission (FTC) for "knowingly provid[ing] scammers with hundreds of thousands of consumers' sensitive personal information."

SiteSearch will pay $4.1 million default judgment, while the other defendants' monetary obligations are suspended based on inability to pay. Those defendants are prohibited from selling or transferring any personal information to third parties and misleading consumers about the terms of payday loans, and they must destroy all consumer data in their possession within 30 days of entry of the final order.

The defendants collected consumers' names, addresses, phone numbesr, employers, Social Security numbers, and bank account numbers, including their bank routing numbers through online payday loan applications. After collecting this data, the defendants sold almost 95 percent of these applications for $0.50 each to third parties (nonlenders) who did not need the information for any legitimate purpose but instead, in some instances, used the information to withdraw thousands (even millions) of dollars from consumers' accounts. The lesson here is not only for businesses collecting consumer data, but also for consumers: be careful who you give your personal information to and always monitor your bank accounts.

— Kathryn M. Rattigan

Fiat Chrysler Seeks Dismissal of Class Action over Hacking

Fiat Chrysler asked a federal court in Illinois last week to dismiss the proposed class action against it, asserting that inadequate security puts vehicles at risk for hacking after two security researchers were able to take control of a Jeep Cherokee and wrote about it in *Wired* magazine.

Fiat stated that it patched the vulnerability days after the article is published and hacking is no longer possible. In addition, Fiat alleged that the plaintiffs were unable to prove that they were injured or damaged. The plaintiffs allege that the possibility of hacking could cause accidents and injuries to owners and that the vulnerability has decreased the vehicles' value.

— Linn Foster Freedman

Wendy's Faces Class Action over Data Breach

We wrote about Wendy's investigation into a data breach at its chain restaurants at the beginning of January, and now Wendy's faces a class action over that same breach. The suit claims that Wendy's negligently exposed customers' credit card information, and lead plaintiff, Jonathan Torres, claims that hackers used his stolen credit card information to charge almost $600 in fraudulent purchases. The complaint states, "Wendy's could have prevented this data breach. While many retailers, banks, and card companies responded to recent breaches by adopting technology that helps make transactions more secure, Wendy's has acknowledged that it did not do so."

In addition to damages under the Florida Unfair and Deceptive Trade Practices Act, Torres seeks judgment requiring Wendy's to put adequate security measures in place as well.

— Kathryn M. Rattigan

FCRA Claims against CoreLogic Are Here to Stay, for Now

The alleged Fair Credit Reporting Act (FCRA) violations against CoreLogic National Background Data LLC (CoreLogic) won't be going away. A Virginia federal court ruled that CoreLogic's business does indeed fall under the FCRA, stating, "The undisputed documentary evidence from [CoreLogic] establishes that, in practice, [CoreLogic] has freely recognized that the background checks that it provides are indeed 'consumer reports' pertaining to individual consumers within the meaning of the FCRA."

Lead plaintiffs, Tyrone Henderson and James O. Hines, Jr., allege that CoreLogic sabotaged their employment opportunities when Henderson's potential employer mistook another person's criminal background check for his and when Hine's potential employer thought that he was a registered sex offender in Indiana when in fact he had no such offenses on his record.

CoreLogic claimed that because they create background check documents and then sell access to the information to screening companies, which then in turn sell the background checks to employers, CoreLogic is not covered by the FCRA. However, the court found that this "logic" (no pun intended) is flawed in that the FCRA promotes accuracy and fairness in consumer reports. So if you are a business that prepares consumer reports (even if you aren't providing them directly to employers or financial institutions), be aware of the FCRA requirements.

— Kathryn M. Rattigan

CYBERSECURITY

New Malware Steals Banking Credentials and Holds Data Ransom

Researchers at Palo Alto Networks have reported that a malware dubbed Xbot is targeting devices in Australia and Russia but predict that the malware may become widespread.

This is particularly worrisome as it attacks Android versions prior to 5.0, and using a technique called activity hacking, it targets online banking information. When a user attempts to launch an app, the malware launches a different app and the user has no idea that the launched app was redirected to a different one. Xbot displays an interface that overlays the real app and the user has no idea that it has happened. It is almost like an internal skimming device.

According to Palo Alto Labs, it has identified seven different fake interfaces of popular banks in Australia that use official app login interfaces and logos.

Xbot can also steal personal data from the device, including contacts and telephone numbers.

But wait, there's more. Xbot can also display an interface that notifies the user that the device has been infected with CryptoLocker, a well-known ransomware. The hackers request payment of $100, to be paid through a fake PayPal site. Xbot can actually encrypt the files on the device's external storage, so it has a double whammy affect—malware AND ransomware.

Although it is reported to be of limited use in only two countries at this time, as we have seen with other malware and ransomware, it doesn't take long for it to become a threat everywhere.

— Linn Foster Freedman

MFA – Multi-Factor Authentication

Every morning we sit down at our computers and provide our credentials to the network: user name and password. Because it has become such a ubiquitous part of modern life, we have a user name and password to everything, we even have password management applications. This system of challenge and response is designed to prove to the system who you are or authenticate you as a valid user. As discussed in a previous blog post, who you are and what you do also may determine your permissions within the system if Role Based Access Controls are in place.

Multi-factor authentication (MFA) is a method of more securely verifying the identity of a user of any given system. The *multi-factor* comes from requiring more than one piece of identifying information. In the challenge response example above, you know your user name and password. MFA requires two or more pieces of information from the following categories:

- Knowledge: something you know (user names, passwords, PIN)
- Possession: something you have (secure token, bank card, cell phone)
- Inheritance: something you are (fingerprint, retina, biometric)

A subset of MFA is two-factor authentication (2FA), which is a widely implemented version. Originally patented in the early 1980s for use with automated teller machines, customers need their bank card, and they need to know the PIN (something they know and something they have). Two-factor authentication has become extremely common, especially in the Internet and 'app' space. A common method of 2FA is when providers text a code to your mobile phone after a successful challenge and response. Something you know is your user name and password; something you have is your mobile phone.

Most service providers support 2FA but you may need to request that it be enabled for your account. You can check if your provider supports 2FA by checking here.

— Sean Lawless

Crypto-Ransomware Dubbed Locky Hits US Computers in Emails

Just another ransomware to worry about—Locky, a ransomware that attacks systems with malicious macros, has logged almost a half a million sessions in the U.S.

The infection happens through an email that looks to be an invoice and has a Word attachment—the supposed invoice. The Word document attached to the email includes malicious macros that then are able to encrypt documents, images, and archives and rename them. A message then pops up requesting that the victim go to a Tor network and pay the hackers in Bitcoins.

As we continue to see and experience more and more versions of ransomware, it continues to be important to identify the patterns and provide education to employees so they don't fall victim to the scheme and put your business at risk. In this form of ransomware, the subject line of the email reads: "ATTN: Invoice J-98223146" and the message says "Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice." Spread the word to read all emails carefully and recognize this one as especially important for your staff.

— Linn Foster Freedman

DATA PRIVACY

Does Employees' Use of Apps Lead to Violations of Workplace Policies?

The constant and evolving release of new apps used by employees both personally and in the workplace continue to present challenges to employers in the implementation and execution of workplace policies designed to protect employees, particularly those involving sexual harassment, anti-discrimination, and bullying. These challenges are no longer limited solely to social media websites such as Facebook, Instagram, LinkedIn, and the like. Indeed, bulletin board apps enable employees to post comments to public message boards. Regardless of the stated purpose of an app designed to allow workers to communicate about the terms and conditions of their employment, employees' use of these platforms may result in inappropriate conduct that violates other employer policies.

Employers are beginning to see an increase in harassment complaints stemming from employees' use of apps. In particular, apps that create message boards onto which employees add individual comments often result in an increasingly hostile thread of negative or threatening comments. The "piling on" of comments often leads to online bullying or shaming that translates into workplace discord or legal claims of harassment or discrimination.

The NLRB's protection of speech occurring on social media platforms is well established. Indeed, as previously posted, the Second Circuit held in *Three D, LLC d/b/a Triple Play Sports Bar and Grille v. National Labor Relations Board* that employees' Facebook postings are protected under the National Labor Relations Act. There has not, however, been significant judicial guidance regarding the implications of employees' use of apps in the workplace that result in harassment or bullying claims. These evolving technology and resulting legal issues warrant review by employers to defuse potential workplace conflict stemming from the often intersecting areas of personal and work-related speech.

— Rachel V. Kushel

HIPAA

HHS Releases HIPAA Guidance on Care Coordination and Case Management

In its third release of HIPAA guidance over the past few weeks, the Department of Health and Human Services (HHS) released "The Real HIPAA: Care Coordination, Care Planning, and Case Management Examples" to assist covered entities and business associates in determining what disclosures of protected health information are permitted under HIPAA.

The blog post gives examples of disclosure of protected health information for care coordination (e.g. a hospital discharging a patient to a rehabilitation facility); care planning by a provider (e.g. hiring a vendor to provide the services, with a business associate agreement in place); and case management by a payer (e.g. the payer hires a health management company to provide nutritional advice to its members with a business associate agreement in place).

The guidance provided by HHS is easy to read and understand and is very helpful with practical examples that providers can understand. We will continue to watch for these helpful tips and keep you apprised as they are published.

— Linn Foster Freedman

Deadline to Self-Report 2015 HIPAA Breaches Is Monday, February 29

As we stated in last week's *Insider*, Monday, February 29, 2016, is the last day to self-report under 500 breaches of unsecured protected health information to the Office for Civil Rights (OCR) through the online breach notification form on the OCR's website. Don't miss the deadline!

— Linn Foster Freedman

DRONES

FAA Sued by TechFreedom over Drone Registration Requirements

Nonprofit organization TechFreedom filed a petition against the Federal Aviation Administration (FAA) this week over the FAA's regulatory requirement of the registration and $5 fee for drone hobbyists. President of TechFreedom said, "Whether or not requiring drone registration is a wise policy, the rules the FAA rushed out before Christmas are unlawful. The agency bypassed the most basic transparency requirements in administrative law: that it provide an opportunity for the affected public to comment on its regulations. That means the FAA could not fully consider the real-world complexities of regulating drones."

TechFreedom's suit stems from the FAA's rule, which was released in December of last year, requiring drone users to register their name, address, and email address with the FAA, pay a registration fee, and obtain a certificate of registration with an identification number for their drone. TechFreedom says that the FAA is only permitted to require registration of aircrafts, not of the people operating them. This is surely only the beginning of the fight against the FAA's regulation of drones. We will keep following the stories as they unfold.

— Kathryn M. Rattigan

FAA Warns Drone Users: Registration IS Required

Recently, the Federal Aviation Administration (FAA) has been reminding drone users that they could face fines of up to $27,500 (and possibly even jail time!) for failing to register their drones. The **February 19 deadline** has come and gone, and the FAA says "failure to register an aircraft may result in regulatory and criminal sanctions."

As of February 19, 368,472 drones were registered with the FAA, which surpasses the number of airplanes registered with the FAA. However, there are many complaints (and even a few lawsuits) against this registration process. Yet, the FAA defends its position and states that it has the authority to regulate all "aircrafts" flown in the United States. Now that this deadline has passed, it will be interesting to see just how strong the FAA's enforcement will be.

— Kathryn M. Rattigan

PRIVACY TIP #23

Home Security Systems Vulnerable to Hacking

A Forbes reporter was able to hack into a home alarm system in San Francisco using a browser and "easily-guessable passwords." The hacking was with permission of the owner but allowed him to make his point—that he could unlock the doors and turn off the alarm while he was sitting in London.

According to the Forbes reporter, Thomas Fox-Brewster, technical researchers at IOActive told him that SimpliSafe, a U.S. company that sells alarm systems using cellular technology, "is actually leaving houses open to burglars with rudimentary hacking skills."

The researchers have concluded that by using basic hardware and software that harvests PINs and turns off alarms, and can be bought for between $50 and $250, the SimpliSafe alarm system can be hacked, opening homes supposedly secured with the system. This is despite the fact that according to its website, it is BBB A+ rated and recommended by Fox News, NBC, Good Housekeeping, and Fortune.

Apparently, when you do research on this topic, home and business alarm systems using smart phones can be subject to hacking vulnerabilities, and this issue is not unique to SimpliSafe.

Privacy Tip for this week? If you are using a home alarm system app on your smartphone and depending on it to secure your home or business, check out the security of the alarm system to see how effective it is. Sometimes good old dead bolts are pretty effective by themselves or in combination with an electronic system.

— 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.