Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

October 1, 2015

DATA BREACH

Systema Software Exposes Information of 1.5 Million on Amazon Web Service

Systema Software, which provides software solutions for claims management, is investigating a breach (although it was discovered, accessed and confirmed by an independent third party) involving information of 1.5 million people, including 1 million residents of Kansas. The information, including names, addresses, phone numbers, social security numbers, claims data, drug test results, medical services provided, dates of treatment, claimant ID numbers, payment information, rejection of claims, and details of how the insurance carriers would defend certain claims, were posted to the cloud via Amazon Web Services.

According to the individual who discovered the breach, the posted data included details of "more than 5 million financial transactions, over 1,000 entities that had data exposed, and hundreds of thousands of injury reports." In addition, the data included "tons of financial transaction data, bank accounts with routing numbers, and check numbers." The posting appears not to have been caused by hackers, but instead by human error.

Systema Software contends that only the one individual had gained unapproved access to the data storage system. Nonetheless, this isn't the first story about human error causing highly sensitive data to become exposed and posted on the Internet. It is important to put procedures in place to mitigate this risk in an organization.

— Linn Foster Freedman

Hilton Hotel Properties Investigating Possible Credit Card Breach

It has been reported that Hilton Hotel Properties (Hilton), including Embassy Suites, Doubletree, Hampton Inn and Suites, and Waldorf Astoria, is investigating credit card fraud alerts from banks, which have been alerted by credit card companies that fraudulent activities have been detected with the common point of sale at Hilton Hotel Properties' restaurants, coffee bars, and gift shops. The fraudulent card activity may date back to November of 2014, but reportedly does not include the reservations system. Hilton has confirmed that it is investigating the reports.

— Linn Foster Freedman

DATA SECURITY

Mortgage Bankers Association Releases Guidance

Recently, the Mortgage Bankers Association released "The Basic Components of an Information Security Program" for small- and medium-size companies in the mortgage industry that may not have the resources to stay well informed about all of the laws, regulations, regulatory guidance, security frameworks, and best practices that have been issued by various government or private entities.

The whitepaper, authored by members of the MBA Residential Technology Forum Information Security Workgroup, describes critical risks that the mortgage industry faces, and provides practical steps to mitigate them, beginning with instituting an information security program and a regular self-assessment of that program. "We understand that some organizations have limited resources to accomplish this, so while recommending that organizations incorporate all sections in this document as part of a basic program, there are 'absolutely necessary' steps that most regulators and standards organizations regard as critical and that the authors believe should be made a priority," states the whitepaper. Accordingly, the whitepaper recommends that corporate security should be prioritized by senior management and its continued development should be encouraged.

— Kathleen E. Dion

SAFE HARBOR

EU Endorsement of Safe Harbor Will Be Decided on October 6

Last week (September 23, 2015), Advocate General Yves Bot (AG), an adviser to Europe's highest court, issued a nonbinding opinion that the agreement between the EU and the U.S. for data transfers from the EU to the U.S. should be deemed invalid by the European Court of Justice.

The opinion declared that the European Commission's 2000 decision to endorse the Safe Harbor Agreement, which allows companies to transfer data of Europeans to the U.S., provided that they self-certify to adhere to EU privacy laws, should be declared invalid because it does not adequately protect Europeans' privacy rights. The safe harbor program is presently used by approximately 4,500 companies.

The crux of the argument was based on the NSA's comprehensive access to data. The AG said, "Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter." The criticism includes Europeans' inability to challenge law enforcement and national security agencies from accessing their data.

In response, the U.S. Mission to the European Union issued a statement on Monday (September 28, 2015) stating that the AG relied on inaccuracies in the underlying case against Facebook pending in Ireland. "The United States does not and has not engaged in indiscriminate surveillance of anyone, including ordinary European citizens. Moreover, the advocate general's opinion fails to take into account that—particularly in the last two years—President Obama has taken unprecedented steps to enhance transparency and public accountability regarding U.S. intelligence practices, and to strengthen policies to ensure that all persons are treated with dignity and respect, regardless of their nationality or place of residence."

The European Court of Justice has announced that it will issue its opinion on October 6th. We are watching closely, because if the Safe Harbor program is declared invalid, companies that rely on safe harbor certification will have to determine compliance in the wake of the declaration. We will keep you

posted.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

SEC Brings First Cybersecurity-Related Enforcement Action

The Securities and Exchange Commission (SEC) recently settled its first cybersecurity-related enforcement action against a Missouri-based registered investment adviser, R.T. Jones Capital Equities Management, Inc. (Investment Advisor). The Investment Advisor was censured and fined $75,000 for failing to have acceptable written policies and procedures regarding its customer records and information in place prior to a 2013 data breach incident that compromised names, dates of birth, and social security numbers—personally identifiable information (PII)—of thousands of the Investment Advisor's clients. It is worth emphasizing that the censure and fine were imposed despite the fact that there is no evidence the breach resulted in harm to those individuals whose PII was affected.

The Investment Advisor offered web-based investment portfolio allocation services to its clients, who could enroll and log into the services using their PII. The services were hosted on a third-party web server. In 2013, it was discovered the server was being hacked from China. The Investment Advisor engaged two cyber-forensic firms to investigate, but neither firm could determine whether PII was accessed or taken. The Investment Advisors also notified those affected of the breach and offered them credit monitoring services.

Notably, the individual data and PII on the server was not encrypted, nor was there a firewall on the server. Additionally, although its services were offered to about 8,000 clients, the Investment Advisor maintained the PII of more than 100,000 individuals on the server.

SEC Rules

In 2000, the SEC adopted Regulation S-P, which implemented certain Gramm-Leach Bliley Act and the Fair Credit Reporting Act provisions for SEC-regulated entities, including registered broker-dealers, investment advisers, and investment companies. Rule 30 of Regulation S-P (Safeguard Rule) requires regulated entities to establish written safeguards "reasonably designed to insure the security and confidentiality of customer records and information, protect against anticipated threats to the security or integrity of those records and information, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."

In 2014, and again in 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) published Risk Alerts announcing it would be conducting industry examinations on cybersecurity, with a focus on risk identification and preparedness assessments. Similar to annual cybersecurity practice reviews in the insurance and other regulated industries, the OCIE is focused on understanding how and why cybersecurity breaches occur in order to promote and enforce minimum appropriate safeguards against known or anticipated threats or hazards.

Applying the Lessons

First and foremost, the Safeguard Rule requires investment advisors and others regulated by the SEC to have in place written policies and procedures addressing the security and confidentiality of customer records and information. The settlement order demonstrates that the SEC will impose a fine for failing to have these policies and practices in place, even if there is no demonstrated harm or damage. The settlement order against the Investment Advisor reveals some of the components a regulated entity

should expect OCIE staff to be looking for in an entity's cybersecurity policies and practices as part of an OCIE examination in 2015 and beyond. These components include conducting periodic risk assessments and having written incident response procedures, as well as using firewalls, encryption, and other technology to restrict access and further protect PII. In addition, the settlement order emphasizes the importance of making thoughtful decisions about the use and storage of PII when it questions the Investment Advisor's decisions about storing the PII of 100,000 individuals on a third-party web server, when 90% of those individuals did not enroll in the web-based services. Finally, the Risk Alerts highlight that the minimum requirements of these policies and procedures has evolved over time, and will continue to do so, based on developing industry and company-specific risks and security incidents.

In the Matter of R. T. Jones Capital Equities Management, Inc., the settlement order is available here.

— Kathleen M. Porter

Fiat Moves to Dismiss Proposed Class Action Suit

Late last week, Fiat filed a Motion to Dismiss the proposed class action against it following reports of hacking into vehicle information systems and its announcement that it was recalling 1.4 million Dodge, Ram and Jeep vehicles in order to install a software patch. The National Highway Traffic Safety Commission is investigating.

The Motion contends that the Plaintiffs' speculative fear that there is a potential for their cars to be hacked is not enough to confer Article III standing, and hypothetical harm is not an "injury in fact" for the Plaintiffs to be able to bring suit.

— Linn Foster Freedman

HIPAA

OCR Announces Launch of Phase 2 of HIPAA Audits

Although the Office for Civil Rights (OCR) has indicated in the past that it would start its next round of HIPAA audits, apparently it means business now. In the wake of an Inspector General report that the OCR was merely investigating data breaches and complaints, the OCR sent a letter to the Inspector General last week indicating that it is moving forward with Phase 2 of its audit program in early 2016.

The audits will concentrate on high risk areas and pervasive non-compliance based upon the Phase 1 audits, will include onsite visits and desk reviews, and will include both covered entities and business associates. In addition, the OCR will be updating its audit protocols and "refining the pool of potential audit subjects." It is anticipated that over 350 entities will be included in the audits.

In anticipation of launching Phase 2, OCR has chosen FCi Federal as the vendor to conduct the audits. As with Phase 1, the audits will commence with a data request, although the next audits will no doubt focus on data security. Now is the time to get ready for a HIPAA audit, and both covered entities and business associates would be well served by reviewing their HIPAA compliance program to make sure they can pass the test.

— Linn Foster Freedman

GEOLOCATION

Boston's MBTA Joins the Bluetooth Beacon Bus – It Will Now Track the Movement of its Riders

If you don't think you are being tracked as you move around Target or Macy's or even through a local museum, you must not have a smartphone. Many companies are now using beacons – or stationary devices that measure the movements of people carrying smartphones, through Bluetooth or Wi-Fi transmissions, to understand the movements of consumers and build marketing campaigns based on consumer location. On September 23, 2015, the Massachusetts Bay Transportation Authority (MBTA) announced that it too will join the beacon bus. Boston's MBTA will start tracking public-transit riders using these beacons. Specifically, the MBTA will track users through Gimbal Bluetooth Smart beacons, so if you turn your Bluetooth off you should be out of range. Nevertheless, the MBTA said that it will not be collecting or using personally identifiable data, and it will also use a "secure, closed network" to track its riders.

The goal of this new tracking? The MBTA hopes to find ways to improve communications with riders and other MBTA technology. Additionally, and perhaps most concerning, it hopes to find out "how brands can increase engagement and interactions with commuters based on proximity." This is just a pilot program that the MBTA hopes to roll out for a year before determining its usefulness and the potential for more effective communications.

— Kathryn M. Rattigan

CYBERSECURITY

Comment Period Extended for NIST Cybersecurity Practice Guide

The National Institute of Standards and Technology (NIST) has announced that due to stakeholder feedback, the period to submit comments for the draft guide, "Securing Electronic Health Records on Mobile Devices" has been extended from September 25, 2015 to October, 23, 2015. The guide provides a detailed architecture to assist with securing health records on mobile devices. The solution uses NIST standards and best practices, and follows the HIPAA Security Rule. Stakeholders can submit comments online.

— Linn Foster Freedman

Cybersecurity + Law Enforcement: The Cutting Edge Symposium

Friday, October 16, 2015
RWU Law | Bristol, Rhode Island

Cybersecurity, encryption, and government surveillance are daily challenges for public officials, corporations, and lawyers. On October 16, the Roger Williams University School of Law will present *Cybersecurity and Law Enforcement: The Cutting Edge*, featuring U.S. Senators Sheldon Whitehouse and Jack Reed, Representative Jim Langevin, the Federal Trade Commission's Jessica Rich, Google's David Lieber, data privacy lawyer Linn Foster Freedman and Assistant Attorneys General Leslie Caldwell (Criminal Division), and John Carlin (National Security Division). Key players in cyberlaw's future, along with other experts from government, academia, and the private sector, will highlight the risks and propose

solutions for these situations:

- The massive hack at the federal Office of Personnel Management has exposed sensitive personal information of over 21 million public employees and others involved in security clearances;
- Ongoing and escalating cyber intrusions resulting in daily data breaches of well-known companies such as Target and Anthem have worried consumers, angered regulators, and attracted the plaintiffs' bar;
- Litigation and enforcement actions and the interplay between private industry and the government in sharing information about cyber intrusions;
- Edward Snowden's disclosures about the National Security Agency have ignited a national debate about the balance between privacy and national security;
- Apple and other firms have embraced end-to-end encryption to keep data secure, triggering law enforcement concerns about "going dark" in the battle against cybercriminals.

Check the symposium website for agenda and registration details.

— Linn Foster Freedman

WEEKLY PRIVACY TIP #3

Know How Apps Are Constantly Accessing and Using Your Location

Everyone loves their smartphone. Everyone loves the newest app. Angry Birds has lots of company now. But most people don't know the back end of apps and how they are accessing, using and selling your data. Why? Because no one reads the Privacy Policy and Terms of Use to figure out how they are accessing and using your data.

The most common features of apps that affect your privacy are the use of the microphone, location based and geolocation services, and access to personal data, such as photos, contacts and health information. Whether you care or not, you should at least be aware of the data apps have access to, are using and selling, and make an educated choice about whether you want them to have access or not. This week, we will focus on apps' use of your location through location based services.

First, you need to know which apps have requested to track you (and to which you agreed) when you downloaded the app. Touch settings on your phone and go to Privacy. Location based services is listed and is automatically on when you buy an iPhone. Why? Because Apple wants access and has access to your location and requires it for Find Your iPhone. But this means that Apple knows where you are at all times and is selling that data to advertisers so they know which cities you visit, which restaurants you go to, which supermarkets you visit and in general, your minute by minute location. If you browse down location based services, the apps that are following your every step are listed there. Some allow the app to only follow your location when you use their app, but many others automatically track you whether you are using their app or not.

Sound creepy to you? Then my suggestion is to turn your location based services off unless you are using a particular app that requires it. When you are finished using the app, turn your located based services off again. If it is off, none of your location data is being accessed, used or sold by the app

developer.

When you download an app, read the fine print on how they are going to access and use your data, including location based services. I have refused to download apps if they won't give me a choice about using my location. There is usually another app that does the same thing and respects my privacy.

Real story: a friend downloaded a trendy retail app and as she was walking by one of their stores in a mall that was located in another state than where she lived, the app pinged her to tell her that they were having a sale in that location and since she was walking by, she should stop in and check out the sale. Needless to say, it freaked her out and she called me to find out how they knew she was in that mall. Of course, she had her location based services on, and had agreed for the app to use her location based services at all times when she downloaded it. She hadn't read the pop up information, and just clicked "I agree."

And if you aren't creeped out, just be aware of what apps are asking for and doing with your data, and make educated choices when you allow access to your location.

— 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

---