Robinson+Cole

Data Privacy + Security

July 23, 2015

Data Privacy + Security Insider

DATA BREACH

[“Life is short. Have an affair.”® and Have Your Data Hacked and Leaked]

Hackers calling themselves “The Impact Team” announced on July 15th that it has compromised the extramarital affair site AshleyMadison.com, and companion sites Cougar Life and Established Men, including absconding with up to 37 million users’ financial records. The sites promised that for an extra $19.99, users could completely remove their site usage history and personally identifiable information from the site, but the hackers stated that users’ real names and addresses aren’t scrubbed and have been compromised. The hackers proved the point by releasing some of the users’ data online and announcing, “[F]ull Delete netted ALM $1.7mm in revenue in 2014. It’s also a complete lie. Users almost always pay with credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important information the users want removed.” The hackers further demanded that Ashley Madison and Established Men be taken off line permanently, or “we will release all customer records, including profiles with all the customers’ secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails…with over 37 million members, mostly from the US and Canada, a significant percentage of the population is about to have a very bad day, including many rich and powerful people.” 37 million very nervous users. But really, why would anyone think their information can be kept safe in these times?

The parent company of the Ashley Madison site has confirmed the intrusion, calling it a “criminal act.” It has issued a statement indicating that it is investigating the intrusion, and working with forensic experts and law enforcement. Early reports surmise that a culprit was either an employee or a contractor. It acknowledged the breach, but stated “[A]t this time, we have been able to secure our sites, and close the unauthorized access points.” But 37 million users, who have used sites touted to assist with extramarital affairs, alleged prostitution, cougar dating, gay dating, swapping for swingers, and overweight dating have had their data compromised. Ouch.

— Linn Foster Freedman

[UCLA Health System Announces Data Breach Affecting 4.5 Million Patients and Medical Providers]

Adding to the long list of cyber hacking victims, the UCLA Health System announced on Friday (July 17, 2015) that it confirmed on May 5, 2015, that a cyber-attacker had accessed parts of UCLA Health’s

network back to September of 2014. The information accessed included 4.5 million patient names, addresses, dates of birth, Social Security numbers, medical record numbers, Medicare and/or health plan ID numbers and medical information, as well as information on UCLA providers who sought privileges at any UCLA Health hospital. The UCLA system includes Ronald Reagan UCLA Medical Center; UCLA Medical Center, Santa Monica; Mattel Children's Hospital UCLA; and Resnick Neuropsychiatric Hospital at UCLA.

Not only are the HIPAA breach notification regulations applicable here, UCLA has not provided any public information regarding the sensitive psychiatric information that may have been accessed from the Resnick Neuropsychiatric Hospital, which could include substance abuse treatment information protected by 42 C.F.R Part 2 and regulated by the Substance Abuse and Mental Health Services Administration, as well as state laws that apply to highly sensitive health information regulated by state authorities.

UCLA is working with the FBI and a forensic firm in an ongoing investigation and is offering free identity theft recovery and restoration services and credit monitoring for affected individuals.

This is not the first time UCLA has had HIPAA issues. In July of 2011, it settled alleged HIPAA violations with the Office for Civil Rights for $865,500 and entered into a Resolution Agreement and Corrective Action Plan following an OCR investigation. The allegations were that employees repeatedly and without permission examined the health information of patients (rumored to be famous individuals) between 2005 - 2008.

— Linn Foster Freedman

Seventh Circuit Overturns Neiman Marcus Data Breach Class Action Dismissal

In an unusual turn for recent data breach class action cases, the Seventh Circuit this week found that a likely threat of identity theft is sufficient for a proposed class to have standing to sue Nieman Marcus for a cyber-hacking incident that affected 350,000 card holders in January of 2014.

The lower Court dismissed the case in September of 2014 as the plaintiffs failed to demonstrate concrete injury to establish Article III standing. The Seventh Circuit reversed stating that a "substantial risk" of harm is sufficient for standing. The Court noted that 9,200 of the affected cards had been fraudulently used after the hacking.

In addition, the Court stated that "allegations of future harm can establish Article III standing if the harm is 'certainly impending' but 'allegations of possible future injury are not sufficient' citing *Clapper v. Amnesty Int'l USA*. The Court found that although the plaintiffs were reimbursed for any fraudulent charges, and that there is presently no indication that their identities have been stolen, the plaintiffs have spent time and money replacing cards and monitoring their credit score, which is enough of a material factual dispute to withstand a Motion to Dismiss. It held that "[A]t this stage of the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach."

— Linn Foster Freedman

DATA SECURITY

FTC Provides Data Security Guidance To Businesses Based on Lessons from Past Enforcement Actions

On June 30th, the Federal Trade Commission (FTC) published a guide titled *Start With Security: A Guide for Business*, providing 10 lessons learned from the over 50 enforcement actions brought by the FTC against companies that failed to adequately protect consumer data. The lessons and advice offered by the FTC guide are certainly common-sense, but present a good refresher for businesses looking to adopt "best practices" to secure customer data and protect against system breaches.

1. Start with security
2. Control access to data sensibly
3. Require secure passwords and authentication
4. Store sensitive personal information securely and protect it during transmission
5. Segment your network and monitor who's trying to get in and out
6. Secure remote access to your network
7. Apply sound security practices when developing new products
8. Make sure your service providers implement reasonable security measures
9. Put procedures in place to keep your security current and address vulnerabilities that may arise
10. Secure paper, physical media, and devices

For each of the above 10 lessons, the FTC guide provides specific advice and examples of cases where business failed to adequately protect data, resulting in enforcement actions. From a business policy perspective, the key takeaway is for businesses to be aware of the risks associated with collecting, using and accessing customer data. Collect only the data about your customers you need, ensure that access to sensitive data is strictly limited to necessary individuals within your business, and implement systems covering all phases of data's life cycle.

— Benjamin C. Jensen

Auto Manufacturers' Alliance Create Information Sharing and Analysis Center for Cyber-Threats

Twelve automakers that make up the Alliance of Automobile Manufacturers (AAM) have agreed to form an information sharing and analysis center (Auto ISAC) that will facilitate the sharing of cyber security data to stay abreast of the latest hacking threats to vehicle data. AAM is hopeful that the Auto ISAC will be operational by the end of the year. The worthy goal of the Auto ISAC is to "further enhance the industry's ongoing efforts to safeguard vehicle electronic systems and networks" by distributing cyber threat information to AAM members through a hub. The Auto ISAC will serve as "a central hub for intelligence and analysis, providing timely sharing of cyber threat information and potential vulnerabilities in motor vehicle electronics or associated in-vehicle networks." AAM sees expansion possibilities with other businesses involved in the automobile industry, including auto parts suppliers, telecommunications providers, and strategic partners.

This effort follows the AAM's adoption of data Privacy Principles.

The automakers involved in the AAM include BMW Group, Fiat Chrysler Automobiles, Ford Motor Company, General Motors, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche Cars North America, Toyota, Volkswagen Group of America, and Volvo Car Corporation.

— Linn Foster Freedman

Department of Education Requests Emergency Review of Guaranty Agencies' Security Over Student Financial Aid Information

On July 16, 2015, the Department of Education issued a request through notice to the Office of Management and Budget (OMB) for emergency clearance so that Federal Student Aid (FSA) can initiate a formal security assessment program of the 28 independently owned Guaranty Agencies that are involved in the collection and transfer of data of students and families supported by federal student aid programs. The assessment is designed to "ensure the continued confidentiality and integrity of data entrusted to FSA by students and families" and will identify security deficiencies of the Guaranty Agencies based upon NIST publications. It appears through the notice that the Guaranty Agencies will be required to conduct a security self-assessment and attestation to FSA.

Although approval was requested by July 20, 2015, comments to the proposal will be accepted through September 14, 2015.

— Linn Foster Freedman

TELEPHONE CONSUMER PROTECTION ACT

FCC Issues TCPA Guidance In Its Declaratory Ruling

In response to requests from businesses and attorneys general for more guidance on the Telephone Consumer Protection Act (TCPA), the Federal Communications Commission (FCC) released guidance on June 18, 2015, regarding robocall blocking, autodialers, and recycled telephone numbers, and on July 15, 2015, the official Declaratory Ruling and Order (FCC 15-72) was published in the federal register. The FCC said that the ruling "clos[es] loopholes and strength[ens] consumer protections already on the books." The ruling provided the following clarity under TCPA regulations:

- **Green Light for 'Do Not Disturb' Technology**: "Service providers can offer robocall-blocking technologies to consumers and implement market-based solutions that consumers can use to stop unwanted robocalls."
- **Empowering Consumers to Say 'Stop'**: "Consumers have the right to revoke their consent to receive robocalls and robotexts in any reasonable way at any time."
- **Reassigned Numbers Aren't Loopholes**: "If a phone number has been reassigned, companies must stop calling the number after one call."
- **Third-Party Consent**: "A consumer whose name is in the contacts list of an acquaintance's phone does not consent to receive robocalls from third-party applications downloaded by the acquaintance."

Additionally, the ruling affirmed the definition of an "autodialer" under the TCPA as "any technology with the capacity to dial random or sequential numbers." The ruling also affirmed that text messages are afforded the same protections as telephone calls to wireless telephone numbers, and that equipment used to send Internet-to-phone text messages qualifies as an autodialer. Lastly, the ruling once again clarified that autodialed and prerecorded telephone calls and text messages to consumers from financial institutions and health care providers are exempt from TCPA regulations, but that financial and health care institutions cannot send marketing or debt collection telephone calls or text messages without prior express consent from the consumer, and consumers have a right to opt-out from permitted telephone calls and text messages at any time.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

Class Action Filed Against UCLA Following Data Breach

We previously reported that UCLA suffered a data breach affecting 4.5 million patients. Days following the announcement of the breach, plaintiffs filed a proposed class action lawsuit against UCLA, alleging that UCLA should have seen the attack coming and that they "knew or should have known of the risks inherent in maintaining their customers' nonpublic personal and health information." The suit accuses UCLA and its board of regents of fraud, invasion of privacy, negligence, violation of various California laws and breach of contract.

— Linn Foster Freedman

Vendor Who Built Maryland's Health Exchange Site Settles for $45 Million

Maryland Attorney General Brian Frosh announced yesterday that Noridian Healthcare Solutions LLC will pay the State of Maryland $20 million up front and $5 million over the next 5 years for a total of $45 million to settle allegations that the work it performed on building the Maryland Health Connection website was subpar.

The crux of the settlement is a result of the crash of the Maryland Health Connection on October 1, 2013, when thousands of Maryland residents were trying to sign up for benefits. According to the AG, "[T]his company never delivered on what it promised, and, as a result, tens of millions of taxpayer dollars were wasted, and thousands of Marylanders suffered delays and frustration." The site had to be completely redeveloped with new technology.

— Linn Foster Freedman

CYBERSECURITY

Connecticut Legislation Establishes Strategic Partnerships In Cybersecurity

On July 10, 2015, Governor Malloy signed into law Special Act No. 15-21 – An Act Establishing Strategic Partnerships in Cybersecurity. The Connecticut legislation directs the Department of Labor, in conjunction with the Department of Economic and Community Development, to conduct an analysis of the state's cybersecurity sector. Specific objectives expressly required to be included within the analysis are identifying public and private industry stakeholders that utilize cybersecurity professionals and barriers to the expansion of cybersecurity initiatives in the state.

The analysis is to be completed by October 1, 2015. After the analysis is submitted to certain joint committees of the General Assembly, a forum is to be convened on cybersecurity initiatives by December 1, 2015. The legislation then requires the Department of Economic and Community Development to submit a plan for growth of the cybersecurity sector by February 1, 2016. The plan is to include policy recommendations to support the growth of the cybersecurity sector, identify market opportunities and best practices for such expansion, and how to advise the state's public schools to prepare students for employment in the area of cybersecurity.

This legislation is another example of Connecticut's recent focus on combating cybersecurity threats. We will keep you advised of compliance initiatives resulting from this legislation.

— Brian Wheelin

DRONES

U.S. Navy First To Launch and Recover Underwater Drone In Military Operation

We have been watching the growth of drones in the sky and the FAA and states' attempts to regulate them. Now we will start watching the growth of underwater drones.

The USS North Dakota submarine sailed into Groton, Connecticut earlier this week following a two-month deployment to the Mediterranean Sea. Why is this news? Because the mission was a success—it was the first time the Navy has launched and recovered an underwater drone, also known as an unmanned undersea vehicle, or UUV in a military operation. The mission confirmed that submarine-launched drones can be used for divers and special forces in undersea operations. But that's all the Navy would say.

— 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

---