Robinson+Cole

Data Privacy + Security

August 20, 2015

Data Privacy + Security Insider

DATA BREACH

Ashley Madison Hackers Release Hacked Data and Offer Advice to Users to Make Amends

On Tuesday, August 18, hackers calling themselves the Impact Team, which claim responsibility for hacking the extramarital affair website Ashley Madison (view related blog post), and stealing information of up to 37 million people, posted 9.7 gigabytes of data to the dark web using an Onion address accessible only through the Tor browser.

The posted files include account and login information of approximately 32 million users of the site. Payment and credit card information from the past 7 years was included in the data dump, with names, addresses, email addresses, amount paid and the last four digits of the credit card used.

It has been reported that thousands of the email addresses may be false as they end in .gov or .mil, and one address may have even belonged to Tony Blair. The site does not require email verification to sign up.

The hackers posted the data stating "TIME's UP! Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles (view related Ashley Madison fake profile lawsuit); 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters. Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it."

ALM refused to take the sites down following the warnings from the hackers and promised to increase security--maybe a little late.

Recent reports are that the data is legitimate and that anonymous users have verified that they have found themselves in the data dump, including their names, addresses, email addresses and last four digits of their credit card. 32 million people. Ouch. For the 7 million users whose information was not included in the data dump--make amends and go buy a lottery ticket.

— Linn Foster Freedman

IRS Auditor Loses Flash Drive Exposing SSNs of Almost 12,000 People

Katy Independent School District (ISD) was randomly audited by the IRS on August 5th. In order to conduct the audit, the IRS auditor had a flash drive with the names, addresses, birth dates and Social Security numbers of almost 12,000 ISD employees and former employees on it. The problem? It was unencrypted and the auditor lost it. Actually, the reports say the auditor "misplaced" it. The IRS' response? "The IRS takes the security of taxpayer information very seriously and actively works with the Treasurer Inspector General for Tax Administration when issues involving sensitive information arise." How about an IRS protocol that prohibits taxpayer information on any mobile devices? How about basic security measures that ensure that an auditor doesn't use an unencrypted flash drive with thousands of individuals' SSNs on it? File this away in the "I don't make this stuff up" category. The federal government needs to implement security best practices to protect our information if it is going to criticize and enforce best practices on the private sector. Who will protect the teachers of Katy ISD here?

The flash drive has not been recovered, and the ISD is offering the affected individuals with three years of credit monitoring. Very nice of the ISD to protect its employees when the incident wasn't the ISD's fault.

— Linn Foster Freedman

IRS Admits 334,000 Victims of Fraudulent Tax Refunds Due to Security Flaws on Website

Not only did the IRS lose a flash drive with 12,000 school workers' Social Security numbers on it in Texas (view related post), it admitted on August 17th that its initial estimate that 110,000 taxpayers' personal information was used to file false tax returns this year is... well...actually 334,000 data breaches and upwards of 390,000 US households. The fraudulent tax returns were filed after intruders were able to use the "Get Transcript" online app to access taxpayers' sensitive data by guessing at security questions. The questions included information that could be found on publicly available websites, such as a previous address.

A Treasury Department Inspector General's Report from September of 2014 showed weaknesses in the IRS's enterprise information security program, the protection of tax information and implementation of an enterprise risk management program.

The IRS stated that it will mail letters to 220,000 individuals and 170,000 households notifying them of the breach and credit monitoring services.

— Linn Foster Freedman

IRS Declares Identity Protection Services Not Taxable

The IRS announced last week that the value of identity theft protection services are not taxable and do not have to be included in gross income calculations for tax purposes.

Identity theft continues to be the number one consumer complaint to the Federal Trade Commission each year, and with the increases in data breaches, this complaint will not dissipate. It is common for

companies who suffer a data breach to offer credit monitoring or fraud resolution services to mitigate the potential for individuals to become victims of identity theft.

This ruling is consumer friendly and gives guidance to millions of Americans (and their tax planners) who have been offered these services in the wake of massive data breaches.

— Linn Foster Freedman

ENFORCEMENT+LITIGATION

Target and Visa Reach $67M Settlement

Visa, Inc. announced on August 18th that it has reached a settlement with Target for $67 million to reimburse Visa for costs associated with the Target data breach in late 2013, including issuing millions of new cards to affected consumers.

Target was unable to reach a similar proposed settlement with MasterCard (view related posts Proposed Settlement and Settlement Rejected) several months ago as MasterCard did not receive enough support from banks and credit unions.

— Linn Foster Freedman

FTC Settles False Safe Harbor Allegations with Thirteen Companies

The FTC has made it clear over the past year that it is serious about companies' compliance with the US-EU and US-Swiss safe harbor programs, and has publicly stated that it is randomly reviewing company websites to ensure compliance and requesting information and documents that back-up the self-certification.

On Monday, August 17, the FTC emphasized its point when it issued a press release that it has agreed to settle with thirteen companies over allegations that the companies misled consumers that they were certified members of the safe harbor frameworks. The companies had either let their certifications lapse or had never applied for membership in the programs at all, but had listed the Safe Harbor certification mark on their websites.

Self-certification for the safe harbor frameworks is required on an annual basis, so companies may wish to review their safe harbor certifications now to make sure they are current and re-certify as necessary.

— Linn Foster Freedman

Shareholders Sue Mobile Security Firm for Failing to Disclose Hacking Incident Before IPO

MobileIron, Inc. was sued late last week by shareholders in a proposed class action for allegedly failing to disclose a hacking incident just weeks before its initial public offering (IPO).

The suit, filed on behalf of investors who participated in the IPO, alleges that MobileIron violated the Securities Act when it hid a hacking incident before the IPO, which caused the share price to drop

dramatically following the disclosure of the incident.

The MobileIron product was designed to assist companies with managing and securing mobile devices and applications. The security incident was reported in the media the week following the IPO, which indicated that the software's vulnerability allowed the perpetrator to send emails that appeared to come from MobileIron and could completely wipe employees' mobile devices. The stock price tanked following the news reports, which led to the lawsuit.

— Linn Foster Freedman

Seventh Circuit Rules Hospital System is Not a Consumer Reporting Agency Under FCRA

Is a hospital a "consumer reporting agency"? Can a health care provider be liable under the Fair Credit Reporting Act (FCRA) in the event of a data breach? The Seventh Circuit Court of Appeals recently considered these significant questions in the case of *Tierney v. Advocate Health & Hosps. Corp.* (7th Cir., No. 14-3168, August 10, 2015). The defendant, Advocate Health, an Illinois-based health system, experienced a significant data breach in July 2013, in which four desktop computers containing data relating to four million patients were stolen from Advocate's administrative offices. The plaintiffs, who had been victims of the data breach, brought claims for willful and negligent violation of FCRA. FCRA requires "consumer reporting agencies" to "maintain reasonable procedures" to prevent the disclosure of "consumer reports" to unauthorized third parties.

In ruling that Advocate did not meet the definition of a "consumer reporting agency," the Seventh Circuit closely examined each element of the statutory definition, while also making a refreshingly simple observation: "Advocate is . . . a 'network of affiliated doctors and hospitals that treat patients'—not a credit or consumer reporting company." Hospitals and other health care providers already facing extensive regulation of their privacy and data security practices under HIPPA, HITECH and various other sources of federal and state law will be relieved to know that at least one federal circuit court has decided not impose another layer of regulatory compliance on their operations.

— Christopher J. Librandi

DATA PRIVACY

Delaware Enacts a Series of Privacy Laws

Delaware recently enacted four privacy laws--the Online and Personal Privacy Protection Act (DOPPA), the Student Data Privacy Protection Act (SDPPA), the Victim Online Privacy Act (VOPA) and the Employee/Applicant Protection for Social Media Act (ESMA).

DOPPA prohibits website operators from marketing material to minors that may "appeal to the prurient, shameful, or morbid interest of minors" including alcohol, tobacco, firearms, electronic control devices, fireworks, tanning equipment or facilities, dietary supplements, lottery, Internet gambling or lottery, body piercing, branding, tattoos, drug paraphernalia, or tongue splitting.

It further requires all operators of commercial websites or offers apps to conspicuously post its privacy policy for consumers. The Consumer Protection Division will promulgate regulations outlining what must be included.

Finally, DOPPA protects the personal information of digital book services by prohibiting the book service

to disclose user's information to law enforcement, the government or other third parties except under certain circumstances. This law becomes effective on January 1, 2016.

SDPPA is modeled after California's Student Online Personal Information Privacy Act. It prevents operators of websites, online or cloud computing services, mobile services and mobile apps from selling or using student data for targeted marketing or to amass student data into a profile that can be used for non-educational purposes. The law becomes effective on August 1, 2016.

VOPA prohibits the public posting or display of any identifiable information of victims of crime. The prohibition includes the victim's address or telephone number. Criminal penalties apply if the law is violated, and aggrieved persons can also seek civil damages. This law becomes effective 90 days after its passage (August 7, 2015).

ESMA is similar to other state laws that have recently been enacted prohibiting employers from requiring employees or applicants to disclose their passwords or account information to social media sites to the employer.

— Linn Foster Freedman

Canada's Amendments to PIPEDA Now Largely in Force

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) has been amended by The Digital Privacy Act (the DPA). DPA updates PIPEDA and modernizes Canadian data privacy and security law. DPA is now largely in force, except for certain provisions, which will come into force at a later date by order of the Governor in Council. The key amendments include mandatory breach notification and enhanced consent requirements.

Security Breach notification. Under the DPA amendments, Canada now requires organizations to notify affected individuals and the Privacy Commissioner of Canada if their personal information is lost or stolen and the theft or loss creates a "real risk of significant harm." "Significant harm" is defined as including, among other harms, financial harm, humiliation, damage to reputation or relationships and identity theft. Organizations must consider the sensitivity of the information, the probability of misuse, and any other prescribed factors when determining whether a real risk exists. Records of data breaches must be maintained and produced by an organization upon the Commissioner's request. Once the accompanying regulations are finalized and adopted, the breach notification provisions will become effective. Before the adoption of DPA, data breach notifications were voluntary. The number of data breach notices in Canada is expected to increase as a result of this new requirement, as only Alberta currently requires breach notification. In the United States, we saw the visibility of data security rise with the adoption of state breach notification laws which resulted in people receiving multiple notices of a breach suffered by organizations.

Valid Consent Requirements and Exceptions. A second significant amendment to PIPEDA is the requirement to obtain a "valid consent" to collect, use or disclose personal information. The pre-DPA rules required consent of an individual to be "reasonably understandable by the individual." Now, under the DPA amendment, for the consent to be valid, it must be "reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." DPA also includes several new exceptions to the consent requirement, such as expanded rights of a company to collect, use and disclose personal information as part of a merger or M&A transaction.

Organizations should review and as appropriate update their template consent forms. However, there is ongoing and unanswered discussion in the business community about the effect of the DPA consent requirement on the validity of consents obtained prior to DPA's adoption. Of particular concern is whether

pre-DPA consents must be redone, at least in cases of certain sub-groups such as children or senior citizens where there is a concern about whether the group members understand the consequences of giving consent as required by the regulation.

One unanswered question is whether the Canadian Privacy Commissioner will require the consents under DPA to be bilingual to be valid. The Commissioner on several occasions advocated for bilingual privacy policies and related documents. This prior advocacy suggests that dual language requirements for consents could be required. The answer may hinge on whether a bilingual consent would aid an individual's understanding of why their personal information was being collected and/or disclosed.

— Kathleen M. Porter

Internet of Things Framework Introduced by the Online Trust Alliance for Our Connected World

On August 11, 2015, the Online Trust Alliance (OTA) released an Internet of Things (IoT) Trust Framework (the Framework), which presents guidelines for IoT manufacturers, developers, and retailers. The Framework was designed by a group of multi-stakeholders formed in January 2015, including ADT, AVG Technologies, Microsoft, Symantec, TRUSTe, Verisign, and over 100 other IoT experts. Craig Spiezle, Executive Director and President of OTA, said, "The rapid growth of the Internet of Things has accelerated the release of connected products, yet important capability gaps in privacy and security design remain as these devices become more and more a part of everyday life." The Framework addresses only two key categories of IoT devices: home automation devices and consumer health and fitness wearables.

Specifically, some of the Framework's highlights are:

- Privacy Policies: "The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable to the user. Such policies must disclose the consequences of declining to opt-in or opt-out of policies, including the impact to usage of key product features or functionality."
- Limit Disclosures: "Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for specified purposes."
- Encrypt: "Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications and the cloud utilizing Wi-Fi, Bluetooth and other communication methods."
- Test: "Manufacturers must conduct penetration testing for devices, applications and services."
- Mitigate: "Manufacturers must publish and provide timely mechanisms for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, account compromise, etc."

For the list of guidelines, click here.

Public comments on the Framework are due to the OTA by September 14, 2015. The OTA is also developing tools and methodologies that will formalize the Framework and ultimately lead to a voluntary Code of Conduct and certification program for IoT manufacturers, developers and retailers.

— Kathryn M. Rattigan

CYBERSECURITY

Protecting Financial Institutions in Cyberspace—U.S. Financial Regulators Come Up With a New Tool Kit to Stem Cyberthreats

The Federal Financial Institutions Examination Council (FFIEC) has recently developed a new tool to help U.S. financial institutions combat the increasing volume and sophistication of cyber attacks. To blunt threats to a financial institution's computers, computer systems, electronic communications network and infrastructure, the FFIEC's June 2015 Cybersecurity Assessment Tool is designed to help financial institutions identify their cybersecurity risks and determine their cybersecurity "maturity" across five "domains".

The Cybersecurity Assessment Tool is consistent with FFIEC's IT Examination Handbook, the National Institute of Standards Cybersecurity Framework, and industry accepted cybersecurity practices. The Tool provides institutions with a process to inform management about the institution's risks and cybersecurity preparedness—thereby affording management the ability to adjust their institution's risk profile and preparedness to appropriate levels.

The Tool is designed to serve as a measurable and repeatable assessment process and consists of two parts: [1] Inherent Risk Profile—the institution's inherent risks before implementing controls; and [2] Cybersecurity Maturity—the institution's current state of cybersecurity preparedness for each of the following "domains": Cyber Risk Management and Oversight; Threat Intelligence and Collaboration; Cybersecurity Controls; External Dependency Management; and Cyber Incident Management and Resilience.

By reviewing the Inherent Risk Profile and the Maturity levels across the five domains initially and periodically (as significant operational and technological changes occur), management should be better equipped to either reduce the levels of risk or increase the level of controls in each of the domains. FFIEC makes note of the fact that the Tool is intended to complement, not replace, an institution's risk management process and cybersecurity program.

FFIEC membership is comprised of the principals of the Federal Reserve Board, FDIC, NCUA, OCC, CFPB, and State Liaison Committee.

— Norman H. Roos

NIST Draft Report: International Cybersecurity Standardization Needed

An interagency working group led by The National Institute of Standards and Technology (NIST) and The Department of Commerce recently published a draft report (the Report) recommending that the U.S. government increase its efforts to develop international cybersecurity standards by coordinating with other governments and the private sector.

Historically, U.S. standard setting efforts have been led by private organizations, with invited participation from government officials, industry and academia. With the Cybersecurity Enhancement Act of 2014 and President Obama's executive order directing NIST to coordinate with other federal agencies on cybersecurity strategies, NIST has been at the forefront of cybersecurity standards development in the U.S. For example, the private sector is using and quoting the principles for the development of proper information security practices that were developed by NIST for the federal government. Meanwhile, in the Report and elsewhere, NIST continues to advocate for more participation and collaboration between government and the private sector on cybersecurity standards.

The Report advocates for international cybersecurity standards to be developed through active

participation and collaboration among the U.S. government, foreign governments and domestic and foreign private industry. The Report identifies four key reasons why the U.S. government should want to develop and use international cybersecurity standards:

- To enhance national and economic security and public safety
- To ensure standards and assessment tools for the U.S. government are technically sound
- To facilitate international trade
- To promote innovation and competitiveness

The Report includes a helpful supplement (the Supplement) which summarizes current international cybersecurity standardization efforts and catalogues U.S. government and private-sector engagement in these efforts. The Working Group also makes suggestions on how federal agencies can more effectively participate in these ongoing international efforts.

Public comments on the Report are due by September 24, 2015. The Report and the Supplement can be found on the NIST website: http://www.nist.gov.

— Kathleen M. Porter

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.
