September 24, 2015

DATA BREACH

OPM Admits 5.6 Million Fingerprints Stolen During Breach

The Office of Personnel Management (OPM) reported yesterday that fingerprint data stolen during the breach of almost 22 million Americans' data is estimated to be 5.6 million instead of the original estimate of 1.1 million. The increase was due to the discovery of an archived record containing 4.5 million sets of fingerprints that had not been detected earlier during the investigation of the data breach. Although the total figure of the number of individuals affected by the hacking stands at close to 22 million individuals, this means that another 4.5 million individuals' fingerprints have actually been accessed by the hackers.

The significance of this information for national security is being investigated by an interagency group comprised of the FBI, Department of Homeland Security and other intelligence agencies. Of note is how the hackers can use the fingerprints using existing technology and developing means to prevent misuse of the fingerprint data in the future.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Excellus Blue Cross Blue Shield Sued For Data Breach Announced Last Week

Within days of Excellus Blue Cross Blue Shield's (Excellus) announcement that its data had been accessed by a hacker through a "sophisticated" cyber-attack, two law firms teamed up to file a proposed class action suit last Friday against Excellus on behalf of three named plaintiffs. The suit seeks to certify both a nationwide and New York state class of plaintiffs. The suit includes allegations of negligence and breach of contract, and further alleges that two years of credit monitoring for children who were affected by the breach is insufficient.

The suit was filed in U.S. District Court in Rochester and seeks unspecified damages.

Meanwhile, the CEO of Excellus has been questioned by New York state Senator Michael Nozzollo, whose district includes Rochester, NY, where Excellus is located, and he has posted his list of questions to Excellus on his website.

— Linn Foster Freedman

Auto Dealer Settles with FTC for Violations of the Fair Credit Reporting Act

Tricolor Auto Acceptance (Tricolor), a Texas based auto dealer has agreed to settle with the Federal Trade Commission (FTC) for violations of the Fair Credit Reporting Act (FCRA). Tricolor will pay the FTC $82,777 in penalties, which has been approved by a federal judge in the Northern District of Texas.

The FTC alleged that Tricolor violated the Furnisher Rule, which requires companies that provide information to credit reporting agencies to establish and implement written policies and procedures that ensure the accuracy of the consumer information provided to the agencies. Further, the FTC alleged that Tricolor failed to properly investigate consumers' disputes about their credit information. In doing so, Tricolor failed to ensure the accuracy of consumer credit reports.

In its press release announcing the settlement, the FTC stated "An inaccurate credit report can have a huge impact on consumers' ability to make purchases, be hired and more…This case makes it clear that businesses must take the proper steps to make sure the information they provide to credit bureaus is accurate."

Companies who furnish consumer credit information to credit reporting agencies would benefit from reviewing existing, and implementing new written policies and procedures governing the process of ensuring the accuracy of the information prior to sending it to credit reporting agencies, as well as other requirements set forth in the Furnisher Rule.

— Linn Foster Freedman

Businesses Rejoice But Poster Beware: Yelp Ordered To Identify Anonymous Reviewer

Many business suffer the misery and frustration of a harshly negative, anonymous online review. That anonymity, critics argue, frees the reviewer from worries about the need for accuracy and, worse yet, encourages the spiteful posting of false accusations designed to drive away customers. In competitive markets, the targeted business has no choice but to fear that a rival is behind the posting.

Last week, a Massachusetts judge gave businesses in the Commonwealth some relief by ordering Yelp to reveal the identity of an anonymous reviewer who posted disparaging comments about a local jewelry store. Yelp is among a handful of websites that have become ubiquitous in the consumer space. Yelp is often used to identify a business to fill a need or want, and many customers will not patronize a business unless the Yelp reviews are favorable. At the same time, businesses have recognized the importance of this social media tool and place Yelp stickers in their front windows proclaiming "People Love Us on Yelp" while at the same time personally asking customers to post positive reviews.

In a case of first impression in Massachusetts, the San Francisco-based Yelp opposed the third-party subpoena it received in the civil defamation lawsuit that the jewelry store owner has brought against "Customer Doe." Although the anonymous poster claimed in her review that the owner "lacked ethics" and had "ripped off many other vulnerable and desperate women who had to sell their jewelry," Yelp refused to remove the post because it "appeared to reflect the user's personal experience and opinions" and refused to identify the poster. Yelp's objection was based principally on the First Amendment, citing consumers' rights to use anonymity as a shield against retribution. The Boston judge disagreed, ordering Yelp to disclose its information about the user, who has since moved to Colorado and whom the store is no doubt poised to name as a defendant in its case.

— Edward J. Heath

INTERNET OF THINGS

Fitbit Announces its New HIPAA Compliance Program

Now even the fitness tracker you wear on your wrist is compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Fitbit's Corporate Wellness team is one of the fastest growing sectors of the company, and Fitbit voluntarily took this "proactive step" to implement a HIPAA compliance program so that it could broaden the company's ability to work with all different types of employers who seek to implement wellness programs in the workplace.

While Fitbit Wellness does not currently receive protected health information (PHI) as defined and regulated under HIPAA, Fitbit underwent a third-party audit for HIPAA compliance, and will now be able to sign HIPAA Business Associate Agreements with covered entities, including self-insured employers, health plans, and corporate wellness organizations. Fitbit Wellness Vice President and General Manager, Amy Donough, said, "HIPAA compliance is very specific to how data is being used, and specifically around PHI and health information generally. That's not the data we share or create today, but it will become important as we continue to grow."

Additionally, Fitbit Wellness obtains employee permission to share Fitbit data such as steps and active minutes with their employers prior to any disclosure.

One of the largest employers that will be working with Fitbit Wellness is Target Corp., which will offer Fitbits to its 335,000 employees across the country to encourage health and wellness and host fitness competitions among its employees. While it is a bit comforting to know that Fitbit finally recognizes the sensitivity of the information it collects (even if it isn't PHI quite yet), we continue to watch the wearable device market for its privacy and security practices as more and more data is collected and disclosed.

— Kathryn M. Rattigan

Automakers Receive Request for Information Letters About Vehicle-to-Vehicle Communications' Privacy

This week, Senator Ed Markey and Senator Richard Blumenthal sent letters to 18 automakers requesting an update on vehicle-to-vehicle communications' (V2V) privacy and security. The Senators are seeking information on each automaker's "efforts to protect the privacy and security of the cars [they] sell." Back in December 2013, the Senators had sent letters to the same automakers to gather "information about the technologies and capabilities of new vehicles as well as efforts to protect consumer privacy and security." This new request for information letter seeks "an update to the information you provided regarding your company's protections against threat of cyber-attacks or unwarranted invasions of privacy" within automobiles. The Senators also request that the automakers supply information on "any changes to [the] company's vehicle fleet or characteristics, policies, practices and experiences."

The Senators introduced the Security and Privacy in Your (SPY) Car Act back in July 2015, hoping to spark the interests of the National Highway Traffic and Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to set forth federal standards for privacy and security of V2V communications. This second set of request for information letters merely adds to the ongoing efforts of the Senators to protect consumers' privacy and safety on the roads.

Responses are due by October 16, 2015. We will keep you updated on the response and report from the automakers. For now, keep driving.

— Kathryn M. Rattigan

CYBERSECURITY

NIST Issues Draft Framework for Cyber-Physical Systems

On September 18, 2015, the National Institute of Standards and Technology (NIST) issued its draft Framework for Cyber-Physical Systems (CPS), which is "intended to provide a methodology for understanding, designing and building CPS including those with multiple applications." CPS are smart systems that interact between physical and computational components. These interconnected and integrated systems "can provide new functionalities to improve quality and life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use." In addition, they include the Internet of Things (IoT) technologies. CPS systems include smart buildings, health care and fitness devices, smart phones and unmanned cars, all of which use motion and movement sensors.

The draft was issued by the Cyber-Physical Systems Public Working Group and its goal is to provide a framework for developers to be able to create new CPS that can work seamlessly with other smart systems using the same definitions and vocabulary.

NIST is requesting comments to the draft through comment forms that can be accessed here.

— Linn Foster Freedman

WEEKLY PRIVACY TIP #2

Protecting Your (and Your Employees' and Customers') Social Security Numbers

Social Security numbers are one of the highest risk data elements known to mankind.

A Social Security number in combination with a name and date of birth (which are publicly accessible) in the hands of a bad person can wreak havoc on an individual and/or a company. Those data elements can be used to open credit card accounts, utility accounts, sold on the black market and ruin one's credit and identity.

It is amazing how nonchalant some people and companies still are about the use and disclosure of Social Security numbers, and how often people ask for them when they aren't necessary. Privacy tip for individuals--protect your Social Security number like you protect your children--fiercely. Don't give it to your doctors unless you are on Medicare or Medicaid--they don't need it (and hopefully the government will stop using them too). Don't fill it in just because it's included on a form. Push back and find out exactly why whomever is asking for it really needs it. Convenience is not a good answer. There is great matching software on the market that can be used to identify you instead of asking for your Social Security number.

Privacy Tip for companies--protect your employees' and customers' Social Security numbers like you protect your own--fiercely. Find out where they are in your company and put security measures in place to protect them. Don't ask for Social Security numbers if you don't absolutely need them. If you do, lock them up, limit access to them, and don't fax them or send them to others if they don't need them. Don't send them in regular mail or in unsecured email. Train your employees that if they are receiving Social Security numbers from others outside the company and they don't need them, to ask the other company

to stop sending them. As soon as they are received by your company they are your responsibility and increase your risk.

We are all in this together--fighting the bad guys--so let's all help protect each other to make it more difficult for them. We can make a difference if we all use best practices and protect each other.

— 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

---