Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

**August 4, 2016**

**DATA BREACH**

**Banner Health Begins to Notify 3.7 Million Patients This Week of Data Breach from Cyber-attack**

Phoenix, Arizona-based Banner Health (Banner), reportedly one of the largest health care organizations in the country, began notifying up to 3.7 million patients this week of a data breach of its computer system that processes food and beverage purchases at some of its locations. The intrusion was initiated on June 17 and discovered by Banner on July 7.

The intrusion started with the compromise of credit card transactions used to purchase food and beverages, including cardholders' names, card numbers, expiration dates, and internal verification codes between June 23 and July 7. According to Banner, no payment card payments used to pay for medical services were compromised.

But it doesn't stop there. On July 13, Banner discovered that the attackers may have gained access to patient information, health plan member and beneficiary information, and patient and health information. The patient and health plan member information that may have been compromised includes names, addresses, dates of birth, physicians' names, dates of service, claims information, health insurance information, and Social Security numbers. The physician and provider information that may have been compromised includes names, addresses, dates of birth, and Social Security numbers.

Banner operates in seven states: Alaska, Arizona, California, Colorado, Nebraska, Nevada, and Wyoming.

*— Linn Foster Freedman*

---

**Kimpton Hotels Investigates Credit and Debit Card Breach**

Kimpton Hotels and Restaurants (Kimpton) has announced that it is investigating a point-of-sale credit and debit card breach affecting approximately two dozen of its properties in the U.S.

This makes Kimpton just another large hotel chain in the past two years that has become the victim of point-of-sale malware that allows the hackers to capture credit and debit card information remotely. The information is also sold to other criminals who buy goods and gift cards with the stolen card information.

Kimpton advises customers who have frequented one of its properties to check their credit and debit card statements to make sure there are no fraudulent charges and to notify their bank if they notice any

fraudulent charges on their statements.

The number of credit and debit cards affected is presently unknown.

*— Linn Foster Freedman*

---

**CYBERSECURITY**

**Warning Issued to Businesses about Pokemon GO App**

The International Association of Information Technology Asset Managers (IAITAM) has issued a warning to businesses, alerting them to the risks posed by employees downloading the Pokemon GO app on a company-issued phone.

The warning urges companies to prohibit the downloading of the app on any devices used for company business, including phones or tablets subject to bring-your-own-device programs.

The IAITAM is concerned about the security of the business information that could be accessed by using the popular app and urges companies to keep the app off of any device that connects to the company's network.

The concerns include data breaches due to the information that can be accessed through the app, knockoff versions that have been reported to be infected with malware, and allowing the use of the game, which may encourage employees to download risky apps that could affect the organization's data and risk management processes.

IT security professionals in companies may wish to take heed of the IAITAM warnings and get ahead of the security risks posed to their organizations before too many employees download the app.

*— Linn Foster Freedman*

---

**FCC Seeks Public Comment for Proposal to Issue Data Security Rules for Wireless Car Communication**

The Federal Communications Commission issued a notice last week notifying the public that it is accepting comments on the petition filed by Public Knowledge and the Open Technology Institute at New America, which requests a rulemaking process and emergency stay against car manufacturers that prevent them from putting cars that can communicate with each other into the market.

The concern of the group is that after the hacking of several models of cars in the past year [see related posts here, here, and here), the use by car manufacturers of similar technology in new models presents "cybersecurity and privacy vulnerabilities" to the personal information collected by cars, as well as security vulnerabilities that allow cars to be infected with malware.

The group is requesting that specific rules be issued that require data privacy and security measures be included in the technology of new models of cars that will prevent hackers from being able to hack into cars' wireless systems and governing the communication between cars on the road.

According to the group, "To date, the one thing that has prevented cyberterrorists from creating a 'car zombie apocalypse' by infecting thousands of cars with malware designed to crash them into crowds or

one another has been the inability of cars to communicate with each other."

*— Linn Foster Freedman*

---

**NIST Recommends against SMS as Second Authentication Factor**

On July 29, Paul Grassi, the senior standards and technology advisor at the National Institute of Standards and Technology (NIST), posted an unusual blog regarding the new draft NIST Special Publication 800-63-3: *Digital Authentication Guideline*. The main issue that has created significant commentary by the press and businesses is NIST's "deprecation" of using SMS (text messages) as a second authentication factor. SMS has been adopted by many companies as the primary second authentication factor. The NIST Special Publication, if adopted in its current form, applies to U.S. federal government Agencies and their contractors, but many companies follow NIST standards closely. Mr. Grassi explains in his post that the risk that NIST has identified with SMS is that SMS may no longer be attached to a mobile phone. With voice-over IP (VoIP) and other Interned-based services, SMS is now interoperable with multiple services. "An SMS sent from a mobile phone might seamlessly switch to an internet message delivered to, say, a Skype or Google Voice phone number. Users shouldn't have to know the difference when they hit send—that's part of the internet's magic." However, while that makes it easier for the user, NIST believes that it increases the security risk to an unacceptable level. Even if the SMS could be associated with a particular device, NIST states that there is a risk of the SMS being intercepted by a malicious actor. Mr. Grassi goes on to explain that "deprecation" means that SMS may be used for now, but "it's on its way out." This will eventually cause businesses to reevaluate the risks associated with SMS and most likely change their authentication operations and require individuals to learn new ways of interacting with online services.

*— Richard M. Borden*

---

**ENFORCEMENT + LITIGATION**

**FTC Reverses ALJ's Decision in LabMD Case**

In November 2015, Chief Administrative Law Judge (ALJ) D. Michael Chappell ruled that the Federal Trade Commission (FTC) failed to show that LabMD, Inc.'s (LabMD) data security practices caused harm to consumers, stemming from an alleged data breach, and therefore recommended dismissal of the case against LabMD [view related post].

Last week, the FTC issued its Opinion and Final Order, reversing the ALJ's initial decision dismissing the FTC's charges against LabMD. The FTC wrote in its press release that, by reversing the ALJ ruling, the FTC "concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice that violated Section 5 of the [FTC] Act." The FTC stated that the ALJ "applied the wrong legal standard for unfairness" and that LabMD's security practices were "lacking even basic precautions to protect the sensitive consumer information maintained on its computer system." The FTC stated that LabMD "failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees; and never deleted any of the consumer data it had collected."

While the FTC continually contends that Section 5 of the FTC Act permits the FTC to challenge any and all unfair and deceptive acts or practices in or affecting commerce, the FTC's decision in this case is very concerning to companies, as it greatly expands the notion of "unfair and deceptive trade practices," as there arguably was no evidence that any consumer was harmed in this case. The FTC's argument was that the FTC does not need to wait for a consumer to be harmed before it starts an enforcement action.

Even more concerning is the fact that the public record shows that the data was never even accessed except by a company (Tiversa) that was trying to hack into systems, including LabMD's, in order to drum up business.

The ironic part of this decision is that by overturning the ALJ's decision the FTC will "ensure" that LabMD "reasonably protects the security and confidentiality of the personal consumer information in its possession by requiring LabMD to establish a comprehensive information security program." LabMD is no longer in business. According to its CEO, LabMD went out of business because it attempted to fight the FTC. It continues to fight the FTC with pro bono lawyers. So how does the FTC's Final Order requiring "periodic independent, third-party assessments" regarding the data security program of a defunct business accomplish anything except to make a point?

The point of the FTC's decision in the LabMD case, and reiterated by the Wyndham Worldwide case, is that the FTC is a very powerful entity to be reckoned with and that established power creates a treacherous future for other businesses who come under the FTC's hammer. In this case, there was no evidence of access to or misuse or compromise of any information. The FTC responded by stating that the FTC "need not wait for consumers to suffer known harm at the hands of identity thieves" to take action. And now the FTC will continue to exercise its authority in this matter until the courts or Congress tells them otherwise.

LabMD has 60 days from the FTC's service of the Final Order to file a petition for review with a U.S. Court of Appeals. Knowing the CEO, Michael Daugherty, he will continue the fight to the bitter end.

*— Linn Foster Freedman and Kathryn M. Rattigan*

---

**FTC Approves Final Order against ASUS**

We previously reported that the Federal Trade Commission (FTC) had entered into a proposed settlement with ASUSTek Computer, Inc., in February 2016. The allegations against ASUS were that it failed to take reasonable steps to secure the software on its routers, despite representations made to consumers about its top security practices. The FTC alleged that the representations made to consumers were misleading.

On July 28, 2016, the FTC, by a vote of 3-0 and following a public comment period, approved the settlement.

The settlement requires ASUS to "establish and maintain a comprehensive security program subject to independent audits over the next 20 years. In addition, ASUS must notify consumers about software updates or other steps they can take to protect themselves from security flaws, including through an option to register for direct security notices."

Finally, the order prohibits ASUS from "misleading consumers about the security of the company's products, including whether a product is using up-to-date software."

This case illustrates how important the language is in privacy policies or statements on company websites and representations made in any consumer-facing publications. The FTC is all about transparency and consistency between representations made on a company website or other materials and actual data security measures taken with consumers' information. It is a reminder to take frequent looks at website policies and tweak them to conform to actual practices.

*— Linn Foster Freedman*

**Pokemon App Developer Sued for Failed Privacy Protections**

Niantic Inc. (Niantic), developer of the mobile game Pokemon GO, was sued in a Florida court on July 27, 2016. The named plaintiff, David Beckman, filed the complaint against Niantic, claiming the game's terms of service and privacy policy offer no protection to users and allows Niantic to change the terms at will.

The complaint alleges the terms of service are an illusory contract that allows the developer broad rights to collect user data without offering any protection to users. In addition, the complaint also claims the terms are deceptive, unfair, and in violation of state contract laws and the Florida Deceptive and Unfair Trade Practices Act.

This lawsuit comes after the report of a bug that allowed the game total access into some users' Google accounts and an inquiry by Senator Al Franken into the app's data collection. Recently, the Electronic Privacy Information Center urged the Federal Trade Commission to investigate Niantic and Pokémon GO after concerns that user data may be at risk from potential hackers.

Niantic has not responded to the complaint.

*— Leonel Gonzalez and Linn Foster Freedman*

---

**California Federal Judge Certifies Class in S2Verify FCRA Class Action, Using Spokeo Concreteness Test**

Last week, the decision in the *Spokeo* case influenced a California court's decision to certify a class in a Fair Credit Reporting Act (FCRA) case. The class of applicants, who claim that S2Verify, a background check company, unlawfully included criminal information in their reports, includes approximately 4,500 individuals who were subject to S2Verify reports from June 2013 to February 2014 and whose reports included criminal charges, arrests, or indictments over seven years old that did not result in a conviction. Lead plaintiff, Regmon L. Hawkins, claims that his background check included past drug arrests that were older than seven years, which is prohibited by the FCRA.

California federal judge William Alsup said in this order that this FCRA class action met the numerosity, commonality, typicality, and adequacy requirements for granting class certification. The order specifically said that this case should proceed based on the "concreteness" test that the Supreme Court set forth in Spokeo. Judge Alsup's order read, "The [*Spokeo*] court acknowledged, however, that 'intangible' injuries can be concrete and that the 'risk of harm' can satisfy the requirement of concreteness in some cases." S2Verify argued against certification and questioned Hawkins' ability to serve as a class representative since this is his third lawsuit against a consumer reporting agency with the same legal counsel representing him. However, despite S2Verify's arguments, Judge Alsup said, "S2Verify [ ] sent restricted information about plaintiff into the world and as such caused injury to plaintiff's privacy interest."

*— Kathryn M. Rattigan*

---

**HEALTH INFORMATION**

**JCAHO Delays Decision Allowing Physicians to Text Orders**

We previously reported that the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)

lifted its ban on allowing health care providers to use texts for physician orders.

JCAHO recently reversed its decision and reinstated the ban, stating that more guidance is needed "to ensure a safe implementation involving the secure texting of orders for those organizations desiring to employ technology supporting this practice." In order to continue the evaluation of whether or not the ban will remain in effect, JCAHO is collaborating with the Centers for Medicare and Medicaid Services (CMS) to issue additional guidance on the use of secure texting for physician orders in the form of frequently asked questions (FAQs) designed to supplement the initial guidance issued in May 2016. JCAHO and CMS hope to issue the FAQs in September 2016.

*— Linn Foster Freedman*

---

**PRIVACY TIP #46**

**Protect Your Home Computer from Ramsomware**

Even though we have reported numerous accounts of ransomware attacks against businesses, according to a recent survey, individuals continue to be the primary target by hackers employing ransomware.

Individual home computers are easy targets for hackers because individuals usually do not invest as much in data security measures as businesses do.

The ransomware surfaces with messages that compromising information or pictures will be released to family, friends, and social media contacts, or personal information, including names, addresses, phone numbers, and credit card information, will be released and sold unless the individual pays the attacker between $250 and $1200 in Bitcoin in a short amount of time.

Real messages received say the following:

"Unfortunately, your data was leaked in a recent corporate hack and I now have your information. I have also used your user profile to find your social media accounts. Using this I can now message all of your friends and family members."

"If you would like to prevent me from sharing this information with your friends and family members (and perhaps even your employers too) then you need to send the specific Bitcoin payment to the following address..."

The Internet Crime Complaint Center (IC3) gives consumers seven ways to combat personal ransomware attacks:

**1.** Do not open emails or attachments from unknown individuals.

**2.** Monitor bank account statements regularly and credit reports at least once a year.

**3.** Do not communicate with the subject.

**4.** Do not store sensitive or embarrassing photos online or on mobile devices.

**5.** Use strong passwords and do not use the same password for multiple websites.

**6.** Never provide personal information of any kind via email. Question any emails requesting personal

information.

**7.** Set security settings for social media accounts at the highest protection levels.

I would add that you need to educate others in your household, including your children to the risks associated with ransomware and malware so they are aware of the tips. Don't unwittingly compromise your personal computer.

It is clear that ransomware is not going away, so hopefully these tips will help protect you and your family in the future.

*— Linn Foster Freedman*

---

**UPCOMING EVENTS**

**Authors' Events**

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars and participate on panels that discuss developments in the area. The following, are several upcoming speaking engagements:

- August 10 – NSPA Regional Meeting in Washington, D.C. (Linn F. Freedman)
- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. 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.