Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Post-WannaCry—US-CERT Warns of Samba Security Flaw

US-CERT issued a warning late last week that there is a newly discovered flaw, CVE-2017-7494, in Samba that can be exploited via mass attacks. Samba provides Windows-based file and print services for Unix and Linux systems. According to US-CERT, "all versions of Samba from 3.5.0 onwards are vulnerable to a remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to lead and execute it." Basically, this means that if an intruder is successful in gaining access to a device, it can take over the device by acquiring root-level access permissions. *Read more*

Pacemakers at Risk for Remote Tampering

A new study by WhiteScope concludes that pacemakers from four manufacturers contain security weaknesses that expose them to remote tampering. Pacemakers run on radio frequency, and health care providers can adjust them to assist patients with heart abnormalities so they won't have to undergo surgery. However, according to the study, the programmers adjusting the pacemakers are not required to authenticate themselves when accessing the pacemaker, so anyone can reprogram the implanted device. *Read more*

ENFORCEMENT + LITIGATION

TCPA Class Action Tossed Out After Hospital Provides Records Indicating Consent

Central Florida Regional Hospital was released from a proposed class action last week for its alleged violations of the Telephone Consumer Protection Act (TCPA). The hospital's debt collector, Transworld Systems, allegedly made autodialed calls to collect overdue hospital debts without prior patient consent. *Read more*

June 1, 2017

FEATURED AUTHORS:

Kathleen E. Dion
Linn Foster Freedman
Kathleen M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Privacy
Drones
Enforcement + Litigation
Privacy Tip
Wearable Technology

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Illinois Court Rules that College Foundation Documents Subject to FOIA

On May 9, 2017, the Illinois Appellate Court held that the College of DuPage Foundation, a fundraising organization for the public College of DuPage, is subject to the state's open records law. In doing so, the Court rejected the foundation's argument that it was a charitable organization with no public role and instead found that the foundation was performing a government function for the college. *Read more*

DATA PRIVACY

Twitter Updates its Privacy Policy

Twitter recently announced updates to its privacy policy. The updates are effective on June 18, 2017. The updates enable Twitter to collect more user data, including about a user's visits from Twitter to websites based on embedded tweets. By using the social media platform on or after that date, Twitter users will be deemed to have agreed to these updates. *Read more*

DRONES

Air Traffic Control Systems for Drones Tested in Nevada

As more drones take to the skies in Nevada, home to one of only six of the country's Federal Aviation Administration (FAA) Unmanned Autonomous Systems (UAS) Designated Test Sites, officials are trying to figure out how to keep them all from crashing into each other. While the FAA and the National Aeronautics and Space Administration (NASA) certainly envision a future where UAS (or drones) perform all sorts of jobs and functions for society, the FAA, NASA, and the industry as a whole need to figure out how to do this safety in the national airspace. *Read more*

Trump's Proposed Track and Destroy Drone Legislation

President Trump's administration is asking Congress to grant the federal government power to track, hack, and destroy any type of drone flying over domestic soil. The draft legislation includes new exceptions to laws governing surveillance, computer privacy, and aircraft protection. It stems from the government's growing concern for the widespread use of drones after several have flown over sporting events in restricted airspace and one even crashed into the

White House lawn. The draft legislation would authorize the government to summarily track, seize control, and use force to destroy any drone it determines could pose a security threat to an area or airspace designation with special protections (for example, critical infrastructure, political conventions, etc.). *Read more*

WEARABLE TECHNOLOGY

New Study Shows Inaccuracies of Wearable Fitness Trackers for Calories Burned

Researchers at Stanford University have released a study that evaluated seven wearable fitness trackers and how they measured heart rate and calories burned. Most of them measured heart rate pretty accurately, but all seven had error rates of 20 percent or higher in measuring the calories burned by the user. *Read more*

PRIVACY TIP #90

Payment Card Breaches—Both Sides of the Story

We hear daily about another payment card breach at a retail store, restaurant chain, or hotel line. The response to a payment card breach differs from company to company. I get a lot of questions about payment card breaches and why some companies provide credit monitoring and others don't, why some companies provide individual notification and others post it on their website and issue a press release, and why the burden seems to fall on consumers to watch their credit card bills for fraud and deal with it when the breach wasn't their fault.

Here is my attempt to explain both sides of the story.

For the Company

From the company's perspective, often the company has been advised of a data breach by a third party, not from its internal IT department. The FBI, a security researcher, or a credit card processor may give the company the heads up that a dump of credit card numbers on the dark web has one thing in common: a charge to their company.

When this happens, the company usually doesn't have the name or address of the consumer—only the credit card number and security code that was lifted from its point of sale system because it does not house the data. Tthe credit card processor and/or bank that issued the card does. So it isn't that easy for the company to find out who the individual was behind the credit card charge as the data isn't in its possession. It is only given information on how many credit card

transactions from its company were compromised.

Under 48 state laws, the company is usually required to provide notice to the consumers of the compromise if it includes the credit or debit card number and the security code. If the company cannot obtain the credit card owner's name and address, it usually provides notice on its website and issues a press release.

When the company is able to find out the names and addresses of the credit card users, it sends an individual letter to those consumers that notifies them about the breach.

Sometimes companies offer credit monitoring for payment card breaches, a service offered to mitigate the consumer's potential damages. However, credit monitoring is not really helpful unless the information compromised can be used to open a new account (like a Social Security number). Usually in payment card breaches, Social Security numbers are not included. Basically, an individual can't use a credit card number and security code to open a new account, so credit monitoring is of limited benefit for a payment card breach.

Fraud resolution services may be offered, which are designed to assist consumers who become victims of fraud (such as someone using the credit card after it is stolen to buy merchandise). Using the credit or debit card to buy something is a very real threat, and fraud resolution can assist the consumer in the event the card is used fraudulently.

Finally, the individuals involved in the data breach may be issued new credit and/or debit cards, which inactivates the compromised card so it can't be used for any purchases.

Following a payment card breach, the only true way to determine whether the individual is the victim of fraud is when illegitimate charges show up on the credit card account. Luckily, credit card companies limit the amount owed by the consumer to $50, although, in most instances, even this amount is waived. Consumer fraud victims can work with their credit card company's fraud department to resolve the situation but usually are not responsible for any of the charges.

For the Consumer

I will write this in the first person as this happened to me in the last month.

As a lawyer, I frequent Brooks Brothers for spiffy suits and businesswear. As an informed data privacy and security lawyer, I am up-to-date on all of the latest payment card data breaches, so, naturally, I found out about Brooks Brothers' payment card breach.

I pretty much use one credit card. Because I had purchased items from Brooks Brothers during the time of the data breach, I was pretty sure that my credit card had been compromised. I always watch my

credit card statement closely, but this was even more reason to do so. Brooks Brothers announced the data breach on its website (which I have never visited) and issued a press release (which is how I found out about it, as it was part of a daily listserv that I subscribe to in my field). I did not receive a letter from Brooks Brothers about the breach, and I have not confirmed whether they sent out individual notices or not. I do not believe I would have even known about it if I was not in this field.

I travel quite a bit and stay in hotel chains, including Intercontinental Hotel Group (IHG) properties. Several days after I found out about the Brooks Brothers breach, I received a letter from IHG advising that my credit card had been compromised. The letter was dated a month earlier and told me to watch my credit card statement and to contact the credit card company if there is any fraudulent activity.

Because this was the second notice I received in one month, I called my credit card company, told them about the situation, and asked them to stop any activity on the compromised card and issue me a new one. They did, and I received the new card two days later. I have no worry or angst that the credit card number is being used, as it is no longer active. I still look closely at my credit card statement, but my mind is at ease that I reduced the risk of fraud.

I am in this business and knew I was at risk of fraud, not just because of one data breach, but because I had two on the same card. I am not in the habit of going on websites of companies that I do business with to see if they have had a data breach. Who does that? No one.

The purpose of notifying consumers is to make them aware of the compromise so they can protect themselves from fraud. If companies don't have sufficient contact information to notify consumers individually, telling consumers they are unable to provide individual notification because of that fact is important for them to know and shows them the difficulties the company is going through in trying to notify them. Most consumers don't know that the companies may not have their contact information, and they don't know how credit or debit cards are processed.

Although it has its limitations, communicating with consumers on the website is the most logical way to disseminate information. But, not all affected consumers will find out about the incident if notification is only through the website.

To protect themselves after receiving a breach notification letter, consumers may wish to follow the letter's instructions. Companies have spent a lot of time and money to get that letter to you, and the purpose of the information it contains is to help you.

Companies and consumers alike are adversely affected by data breaches. For companies, it is a crisis to the operations and brand of the company and can lead to a loss of customer trust. For consumers, being at risk of or a victim of fraud is disruptive and frightening. Clear communication and cooperation is needed on both sides to get through the difficulties inherent in every data breach.