August 18, 2016

DATA BREACH

Visa Issues Security Alert Warning of Oracle MICROS POS Compromise

We reported last week that Oracle's MICROS point-of-sale devices had been compromised. On the heels of the compromise, Visa sent out a security alert last Friday to merchants warning companies that use Oracle's MICROS point-of-sale devices to check their machines for malicious software or unusual activity and to change passwords on the devices.

The Visa alert indicates that, although Oracle is investigating the situation, "Visa is issuing this alert to provide indicators of compromise (IOCs) associated with cybercrime threats known to have previously targeted Oracle systems." The IOCs include a list of suspect Internet addresses, domain names, and other digital clues that connect the attacker with the victim. The IOCs can help MICROS customers track whether their point-of-sale system has been compromised by checking to see if there has been any communication between their system and the IOCs. Oracle MICROS customers may wish to check the IOCs with their company's traffic to see if there is any communication, which may indicate a compromise.

— Linn Foster Freedman

3.3 Million Health Records Breached by Business Associate Newkirk

Newkirk Products Inc., which provides ID cards and management services for health care organizations, including multiple Blue Cross Blue Shield organizations, has announced that it has discovered that its computer system was compromised starting on May 21, 2016, although the intrusion was not discovered until July 6, 2016.

Newkirk has started to notify the 3.3 million individuals affected and is offering two years of identity theft monitoring and resolution services.

The compromised data includes name, address, date of birth, health plan type, member ID number, group ID number, premium invoice information, primary care provider, Medicaid ID number (usually a SSN), and names of dependents enrolled on members' health plans, although Newkirk states that no Social Security numbers, health insurance details and financial information were exposed.

According to reports, the compromise included approximately 790,000 Blue Cross Blue Shield of Kansas City members.

This represents the third largest data breach involving health information in 2016.

— Linn Foster Freedman

Ransomware and Malware Continue to Plague Health Care Organizations

We continue to warn health care organizations about the real and serious risks associated with ransomware and malware, but organizations don't adequately prepare for possible consequences and are getting hit hard.

Just this past week, several health care organizations have publicly announced that they have been victims of ransomware and malware. The organizations include a dermatology practice that was the victim of a ransomware attack on its network that encrypted 13,237 patient records, a California-based medical billing service company that paid a ransom to get its billing records back, a prosthetic and a Mississippi-based general medical practice orthotic practice that was the victim of a hacking that exposed 23,000 patient records, and a hacking incident exposed 10,401 records.

Health care organizations are being targeted with ransomware and malware attacks, and this risk does not appear to be dissipating any time soon. Healthcare entities may wish to put this risk high on their radar screen to protect patient data from compromise and continue to focus on data security and employee education and training.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

FCC and Federal Debt Collectors, More Restrictions under TCPA

In July we wrote about the exemption for robocalls made by the federal government (or its contractors) from the restrictions of the Telephone Consumer Protection Act (TCPA). Now, the Federal Communications Commission (FCC) added another caveat to the TCPA, advising that, while federally backed debt collection calls to consumers at risk of delinquency are exempt from the TCPA, these debt collectors cannot call or text consumers using automated dialing technology more than three times per month and must limit the calls to 60 seconds or less. Debt collectors are also prohibited from robocalling or texting the debtor's family or friends.

FCC Chairman Tom Wheeler, said, "The commission is establishing strong, pro-consumer limits on robocalls to collect federal debt. These protections are particularly important following a January Supreme Court ruling that federal government entities conducting official business are not subject to robocall limits unless Congress says otherwise. Our decision implements Congress' directive and responds to thousands of comments from consumers expressing frustration with robocalls and urging clear, strong limits on debt-collection calls."

To read the full report and order, click here.

— Kathryn M. Rattigan

Final Order against Practice Fusion Approved by FTC

On August 16, 2016, the Federal Trade Commission (FTC) approved the final order resolving its privacy complaints against Practice Fusion. The complaint [view related post] alleged that Practice Fusion "misled consumers by soliciting reviews for doctors in connection with an online healthcare satisfaction survey, without disclosing adequately that these reviews would be publicly posted on the Internet." The FTC further alleged that patients' sensitive personal and medical information was publicly disclosed, which violated the FTC Act.

The order requires Practice Fusion to obtain consumers' explicit consent before making any consumers' information publicly available and to refrain from making deceptive statements about how it protects the privacy or confidentiality of consumers' information.

— Linn Foster Freedman

CYBERSECURITY

HEI Hotels & Resorts Investigating Malware Intrusion

HEI Hotels & Resorts (HEI), which includes Hyatt, Sheraton, Marriott, and Westin hotels have notified individuals who purchased food and beverages at 20 locations in 10 states and the District of Columbia that their credit card information may have been compromised due to a malware intrusion.

The intrusion occurred between early 2015 and June 2016 and included card holders' names, card numbers, expiration dates, and verification codes.

HEI warns customers to review their credit card statements for unusual activity or discrepancies. A list of the properties affected can be accessed here.

— Linn Foster Freedman

DIGITAL ASSETS

California Passes Digital Assets Law

Following in the footsteps of numerous other states, California became the newest state to pass a digital assets bill, which allows individuals to access social media accounts, music accounts, gaming accounts or other digital accounts on behalf of a deceased individual.

The California Revised Uniform Fiduciary Access to Digital Assets Act provides guidelines for how companies can share deceased individuals' emails, IMs, and other digital records following death.

The law allows an individual to "use an online tool to direct the custodian to disclose to a designated recipient or not disclose some or all of the user's digital assets" Significantly, if the online tool contradicts the individual's will, then the instructions in the online tool prevails. Otherwise, a user may provide instructions in his or her will.

Further, the law provides that an individual's instructions override the custodian's (like Facebook or LinkedIn) terms of service.

The law provides the social media company permission to grant full or partial access to the designated recipient if it receives a written request, a certified copy of the death certificate, and a certified copy of the letter of appointment of the representative, along with authenticating information about the deceased user.

The passage of this bill is another gentle reminder for all individuals to think about their digital assets and how they want the assets to be accessed or distributed after their death.

— Linn Foster Freedman

INFORMATION GOVERNANCE

SaaS Adoption Continues to Rise Despite Security Concerns

Software as a Service (SaaS) adoption has continued to climb with each passing year. Major contributors to this have been ease of deployment, improved productivity, and lower cost of ownership. Furthermore, organizations have begun to reason that SaaS applications can be more secure than their premises-based counterparts. Despite these facts, a recent survey of 176 IT security leaders conducted by the Cloud Security Alliance and Bitglass revealed that visibility and control remain hot topics in organizations around the globe. Interestingly, the survey found that more than half do not have adequate visibility and have experienced a security incident due to a lack of controls.

The full report can be downloaded here. Highlights of the survey include the following:

- 62 percent have written policies discouraging use of unsanctioned applications, few have technical controls in place.
- 38 percent outright block unsanctioned applications, while just 29 percent use a proxy or firewall to redirect users.
- 16 percent reported they do not use any SaaS applications.
- 59 percent reported cloud security incidents related to unwanted external sharing.
- 47 percent reported incidents involving access from unauthorized devices.
- 28 percent have access to users logins and 29 percent have audit logs.
- Less than half (48 percent) know where and when sensitive data is being downloaded from the cloud.
- 55 percent of security professionals believe that cloud application vendors should not be forced to cooperate with government by providing access to encrypted data.
- 15 percent believe that cloud vendors should be forced to build backdoor access for government agencies.

Doing business in the cloud sure is a balancing act of convenience and data protection. It will be interesting to see how organizations and cloud vendors continue to innovate in the months and years ahead.

— James Merrifield

DRONES

A.I. Company Flock Develops Risk Analysis Program for Drone Flights

Flock, an artificial intelligence company based in London, announced its development of a risk analysis program for commercial drones that will monitor real-time weather information, the location of buildings, and the most congested areas of people and vehicles to safely and effectively use drones (away from crowds) such as aerial photography drones and package delivery drones. Flock's program uses technology to choose routes that are less congested or to fly in those areas only when it will be less crowded (i.e., not during rush hour). Flock also hopes that its program will be a valuable tool for insurance companies to help quantify risks of individual drone flights.

Flock's CEO, Ed Leon Klinger, said, "The machine learning element of our technology is what allows us to predict when and where certain areas of cities will become particularly hazardous for drones."

Flock plans to test its program in London and Singapore and then possibly conduct some test flights in the U.S. and Japan as well.

— Kathryn M. Rattigan

SOCIAL MEDIA

Aer Lingus Warns Customers about Social Media Scam

Social media users should beware of online scams purporting to offer free Aer Lingus flights.

One scam asks users to fill out a questionnaire for a chance to win Aer Lingus tickets in celebration of its 80th anniversary. Once they have completed the questionnaire, users are told they have won two free tickets to anywhere in the world and are taken to a bogus Aer Lingus website where they are asked to share the promotion with 15 friends and text €2 to a number to claim tickets.

Recently, the national airline took to Twitter and Facebook to warn its followers not to fall for the scam. Its Facebook post, complete with a photo of the phony post, reads: "We're aware of an online scam offering free Aer Lingus tickets. This is NOT an official Aer Lingus promotion. For your own information security, please don't click on any posts in your Newsfeed similar to this one."

Another similar scam involves a phony competition run by a sham Facebook page called Aer Lingus Ireland. The post asks users to like the post, leave a comment on the post saying what city they are from, and share the post with their friends for a chance to win flights to Paris, London, or New York and €10,000 spending money. The post has since been removed but not before it managed to fool tens of thousands of Facebook users.

— Kelly Frye Barnett

PRIVACY TIP #48

Watch Your Amazon Prime Now Account for Hacked Purchases

Those of you with Amazon Prime Now accounts love the convenience of getting goods delivered to your home *right now*, well at least within hours, until Amazon drones become commonplace.

But beware of recent reports that fraudsters are hacking into customers' Prime Now accounts, buying expensive items, waiting outside your home while you are at work (since these fraudsters don't have a job) and grabbing packages when they are delivered to your home and before you get home.

Many times this fraud occurs without the individual becoming aware of it until days or months later when they see they have been charged for an expensive item they did not purchase.

One way criminals are using Amazon Prime Now is to activate accounts in individuals' names using stolen credit cards and other information to open accounts without the individuals' knowledge.

Another way they victimize individuals is to send an email to the customer where they pretend to be from Amazon, asking for access to the customer's Amazon account so they can provide assistance or review or make changes to the account. They then take over the account.

Amazon warns customers not to respond to false or phishing emails and to never allow anyone other than themselves to make any changes to their Amazon account.

My tip for today is to watch your Amazon account closely—just like your bank, credit card, and debit card accounts to make sure you are not unwittingly the victim of fraud.

— 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 relevant areas. The following are several upcoming speaking engagements:

- 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.