Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

December 3, 2015

DATA BREACH

VTech Discloses Cyberattack Exposing Five Million Parents' and Kids' Personal Information

VTech, an electronic toymaker, disclosed on November 30, 2015, that it experienced a cyberattack on its Learning Lodge app store portal on November 14, 2015, that accessed and stole the personal information of 5 million customers, some of whom were children.

The portal, used by customers to download apps, e-books, and learning games, included customers' names, email addresses, encrypted passwords, password security questions, IP addresses, mailing addresses, gender, dates of birth, and downloaded histories of parents and their children.

According to VTech, the attack did not expose any financial information, and the company confirmed that it does not store any credit card data on the website. It has notified every account holder of the intrusion.

— Linn Foster Freedman

Hilton Hotels Acknowledges Payment Card Breach

Hilton Worldwide has issued a statement that it has "identified and taken action to eradicate unauthorized malware that targeted payment card information in some point-of-sale systems."

The information exposed included cardholder names, payment card numbers, security codes, and expiration dates from November 18 to December 5, 2014, or April 21 to July 27, 2015.

Interestingly, Hilton did not indicate how many cardholders were affected and are not offering any type of mitigation, even though security codes of the payment cards were exposed.

Hilton suggests that customers "review and monitor their payment card statements" if they used a credit card at any Hilton property during that time frame. I for one, always closely monitor my credit card statements. Unfortunately, in this case it does not appear that new cards will be issued to cardholders even though security codes were compromised.

— Linn Foster Freedman

Target Settles Data Breach Class Action with Financial Institutions for $39 Million

We previously reported that Target Corp.'s (Target) settlement with MasterCard was rejected, but now Target has agreed to pay $39 million to settle the class action filed against it on behalf of the financial institutions affected by Target's 2013 data breach. Target will pay $20.5 million directly to class members, consisting of all U.S. financial institutions that issued payment cards that were identified as at risk due to the 2013 data breach, and $19.1 million to fund MasterCard's Account Data Compromise program. Target has also agreed to give up its right to challenge MasterCard's assessment of breach liability. Counsel for the financial institutions said, "This settlement is a strong and important result for those financial institutions that sustained losses as a result of the Target data breach, providing compensation well beyond what the card brand networks offered." This settlement is another example (in addition to the $67 million settlement with Visa stemming from the same data breach) where financial institutions have not had to bear the burden of a data breach in which they had no hand.

— Kathryn M. Rattigan

HIPAA

Lahey Hospital Agrees to Pay a Whopping $850,000 to OCR for Stolen Laptop

Just before Thanksgiving, the Office for Civil Rights (OCR) announced that Lahey Hospital and Medical Center (Lahey) has agreed to pay $850,000 in fines and penalties to the OCR and enter into a Resolution Agreement following the self-disclosure that a laptop containing CT scans was stolen from Lahey in October 2011.

Surprisingly, the fine is inconsistent with other fines levied by the OCR for similar issues over the past several years, and it is hard to understand why it is so out of whack.

According to the Resolution Agreement, the case stemmed from the theft of an unencrypted laptop from an "unlocked treatment room off of the inner corridor of Lahey's Radiology Department." The laptop contained the names, birthdates, and imaging information of 599 patients from a CT scanner.

The OCR alleged, and Lahey did not admit, that this violated six separate provisions in HIPAA, including failing to conduct a risk assessment, failing to implement reasonable and appropriate physical safeguards of a workstation, failing to implement policies and procedures governing the receipt and removal of hardware and electronic media, failing to assign a unique user name to identify and track user identities on workstations, failing to implement a mechanism to record and examine activity on the workstation, and the impermissible disclosure of the PHI of 599 individuals.

Lahey has agreed to implement a Corrective Action Plan, including conducting and implementing a security management process, implementing policies and procedures, training employees, and checking in with the OCR periodically regarding implementation.

— Linn Foster Freedman

Triple-S Settles HIPAA Violations for $3.5M

Triple-S Management Corp., an insurance holding company based in San Juan, Puerto Rico, has agreed

to settle an investigation of HIPAA violations by the Office for Civil Rights (OCR) for $3.5 million. According to the OCR press release dated November 30, Triple-S, formerly known as American Health Medicare Inc., will pay the fine and "adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program…"

OCR started an investigation "after receiving multiple breach notifications…involving unsecured protected health information." The investigation "indicated widespread non-compliance throughout the various subsidiaries of Triple-S, including…impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement; use or disclosure of more PHI than was necessary to carry out mailings; failing to conduct an accurate and thorough risk analysis…and failure to implement…security measures…"

A series of self-reports revealed seven different data breaches leading up to the investigation. The breaches ranged from failing to terminate access rights of previous employees; their vendor mailing brochures to members that included health claim numbers on the outside of the envelope; an employee of a business associate downloading member information, including Social Security numbers, onto a CD and taking it home and then downloading it onto his new employer's system, mailing the wrong medical ID cards to the wrong members, and putting the wrong member's letter into another member's envelope.

In addition to the fine, Triple-S has agreed to enter into a Resolution Agreement, which is typical of settlements with the OCR, including conducting a risk assessment and developing a risk management plan, implementing and distributing policies and procedures, and training employees annually.

The OCR fines are always a teaching moment for covered entities and business associates. One of the lessons in this case is to evaluate whether business associate agreements are in place with each entity that has access to PHI of the organization.

— Linn Foster Freedman

BOARD GOVERNANCE

Look for an Increase in Shareholders' Suits in 2016

A new study released by NYSE Governance Services and security firm Veracode, "Cybersecurity and Corporate Liability: The Board's View," is a must read for directors and officers. Veracode was quite accommodating when I asked for a copy.

The report is based upon a survey of 276 directors and officers of publically traded companies "to draw parallels between businesses' cyber risk management practices and their efforts to address cybersecurity liability matters."

The results are sometimes surprising—such as "89% of surveyed directors and officers believe that a company that does not make reasonable efforts to secure its data should be held liable by regulators." So they believe that they should be held accountable, but what are considered "reasonable efforts"? The points made in the report about what is reasonable are spot on. And who determines what is "reasonable"?

It is also interesting to note the impact the Wyndham Worldwide shareholders derivative suit had on the directors and officers surveyed and the final conclusion that there will be an increase in shareholders' lawsuits against officers and directors for cybersecurity liability. Based upon how the litigation environment has changed over the past two years, this conclusion is one to take into the boardroom. If you are board member, check out the survey report—it is well worth the time.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

LabMD Sues FTC Lawyers and FTC Appeals Decision

We previously reported that LabMD had a big victory in the case filed against it by the Federal Trade Commission (FTC). There was speculation as to whether or not the FTC would appeal the decision.

The FTC did in fact exercise its administrative right and filed an appeal of the decision to three commissioners of the FTC. Filing an appeal to the commission is the next step in the administrative proceeding. We will keep you advised of the proceeding as it progresses.

The other big news in the case is that just one week after its big win, LabMD filed suit against three of the FTC lawyers handling the case, saying the lawyers "supported their actions with lies, thievery and testimony from a private company, Tiversa, whose business model was based on convincing companies to pay them to 'recover' files that, in trust, they hacked from computers all over the world." The complaint further states that the FTC lawyers knew or should have known that they were using fraudulent data, misled the commissioners to pursue a vindictive case, and were responsible for constitutional violations. The saga continues and we will follow it closely.

— Linn Foster Freedman

Big Win for Car Manufacturers, Dismissal of Data Breach Suit

A California federal court dismissed a proposed class action against Toyota Motor Corp. (Toyota), Ford Motor Co. (Ford), and General Motors, LLC (GM) this week after a class of drivers alleged that the car companies failed to protect the drivers' vehicles from hackers. The court dismissed the action because the drivers failed to establish any actual injury and because the potential risk of being hacked at some point in the future was not enough to show "injury in fact." U.S. District Judge William H. Orrick said, "It is difficult for me to conclude whether plaintiffs' vehicles might be hacked at some point in the future, especially in light of the fact that plaintiffs do not allege that anybody outside of a controlled environment has ever been hacked. Plaintiffs have alleged only that their cars are susceptible to hacking but have failed to plead that they consequently face a credible risk of hacking."

The drivers also claimed that Toyota, Ford, and GM violated their privacy rights under California law, but again, the court determined that the plaintiffs did not have standing because tracking and dissemination of information about the drivers and their vehicle use "is not categorically the type of sensitive and confidential information that [California state] constitution aims to protect." Additionally, the court determined that it did not have jurisdiction over Ford because the models owned by the driver plaintiffs were manufactured in Kentucky and Mexico, and sold in Oregon and Washington.

This action stems from the announcement back in July of this year of several vehicle recalls for their hacking vulnerabilities and the National Highway Traffic Safety Administration's start of an investigation into the effectiveness of the vehicle software updates.

— Kathryn M. Rattigan

The "Going Dark" Problem

"Going Dark" refers to law enforcement's lack of technical ability to intercept and access communications and information. In response, the Department of Justice (DOJ) is using a law from the 1700s, the All Writs Act, which grants courts the power to issue "necessary or appropriate" writs to force cellphone manufacturers to assist it in extracting this information.

Two federal courts in New York and California have ordered the phone manufacturers (Apple and an unnamed manufacturer) to provide law enforcement with "reasonable technical assistance." The New York court left it up to the manufacturer to request a hearing to limit any actions it determines are unreasonably burdensome. The California court ordered Apple to bypass the cellphone user's passcode, extract data from the cellphone, and copy it to a storage medium. It did not require Apple to attempt to decrypt or otherwise enable law enforcement's attempts to access any encrypted data.

By contrast, another New York court held that Apple cannot be automatically conscripted in government investigations because it is "a private-sector company that is free to choose to promote its customers' interest in privacy over the competing interest of law enforcement." The court requested that Apple advise whether it is capable of unlocking the device and whether doing so would be unreasonably burdensome. Apple responded that, generally, for devices running a version of iOS 7, it can extract certain user-generated active files, but it cannot extract email, calendar entries, or any third-party app data. It noted, though, that, aside from the technical burden to unlock the device, Apple may suffer other burdens, including reputation harm and requirements that its employees testify in the instance of criminal prosecution. The case is still pending.

Apple has warned that law enforcement requests soon will be impossible to perform because Apple lacks the technical ability to unlock devices running iOS 8 or higher.

— Kathleen E. Dion

DATA PRIVACY

New Data Protection Regulation to Impact Cloud Providers

The GDPR (General Data Protection Regulation) outlines a series of amendments to the data protection and data privacy requirements applicable to all companies with European customers, regardless of where the company's headquarters reside.

Some of the proposed amendments include:

- penalties of up to €100 million or 2.5 percent of annual worldwide turnover, whichever is greater
- increased territorial scope
- tighter requirements for obtaining valid consent to the processing of personal data
- enhanced restrictions on profiling and targeted advertising
- new data breach reporting obligations
- direct legal compliance obligations for "data processors"
- extended data protection rights for individuals, including the "right to be forgotten" clause
- processing companies—such as third-party vendors or technology service providers—subject to regulation and privacy compliance.

All indicators point toward a 2017 deadline for sign-off. We'll have to wait and see which amendments are officially adopted. It sure proves to be an exciting ride. No doubt, cloud providers (if they haven't done so already) will begin planning for these changes immediately so they don't fall further behind the eight ball.

— James Merrifield

PRIVACY TIP #12

Credit Card Safety during the Holidays (Use Cash!)

'Tis the season of shopping. CyberMonday has just passed, and news flashes indicate that the total amount consumers purchased online on Monday will exceed $3 billion. Wow. All with credit cards.

We all use our credit cards more during the holidays than any other time of year. As a result, it is a prime time for scammers and fraudsters to steal credit card information. Remember the Target breach? It happened between Thanksgiving and Christmas.

Here are some tips to consider this holiday season (and all year long):

- Use cash whenever possible. Cash is still king, and your identity can't be stolen when using cash.
- Limit the number of credit cards that you apply for. It is very tempting when the clerk at the checkout line asks you if you want to save 15 percent on your purchase by applying for the store credit card. Some say yes on the spot because, well, saving 15 percent on your purchase could be significant. But as soon as you say "yes," the clerk slides a credit card application form for you to fill out. And guess what? It asks for your Social Security number because they will want to do a credit check. So you are giving your full Social Security number to a stranger on a piece of paper that you don't know where it is being sent, who is seeing it, or how it is being secured. The same is true for walking-by salesmen trying to get you to apply for an airline credit card in airports. Be smart about these offers and know that you have to give your personal information to strangers to get the deal.
- Limit the number of credit cards that you use. Do you really need a credit card in every store? Do you really want every store to hold (and potentially breach) your personal information, including your Social Security number? Pick a card that you will use primarily and keep track of your purchases so it is easier to follow the statement and determine whether or not there are any unauthorized charges on your statement.
- Closely monitor your credit card statements every month and make sure there are no unauthorized charges.
- Limit the number of credit cards you keep in your wallet. If your wallet is lost or stolen, you will have to remember every card you had in your wallet to cancel the account. The more you have, the more of a hassle it is to cancel the accounts.
- If you lose your credit card, cancel the account immediately.
- Only use one credit card for online shopping. If the credit card is compromised during an online purchase, you will know exactly which credit card it is so you can close that account quickly.
- While shopping, don't let others use your credit card or borrow your credit card and put your credit card back into your wallet or purse after each purchase. It is easy to lose if you put it in your pocket or jacket or leave it on the counter. There have actually been reports of fraudsters standing near checkout lines and writing down credit card numbers.
- When you no longer need them, shred your credit card receipts.

Safe shopping and hope these help!

— 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

---