October 8, 2015

DATA BREACH

Scottrade Announces Data Breach Affecting 4.6M Customers

Scottrade, a retail brokerage firm, announced late last week that it suffered an intrusion by cyber hackers who stole client contact information of 4.6 million customers. The intrusion occurred between late 2013 and early 2014 (coincidentally, the same time as the Target intrusion, the Excellus intrusion and others).

Although the hackers reportedly only stole customers' names and street addresses, and did not have access to Social Security numbers or other sensitive data, Scottrade will offer identity theft protection services to the 4.6 million customers affected by the data breach. Unfortunately, hackers use contact information for fishing expeditions and social engineering strategies.

Scottrade announced the data breach on Friday, October 2nd, and was hit with a proposed class action data breach suit the same day in California federal court. The suit alleges that Scottrade was negligent in failing to exercise reasonable security precautions, and that Scottrade had experienced previous incursions and had been warned that its security measures were inadequate, and failed to heed those warnings.

— Linn Foster Freedman

6,400 American Bankers Association Members' Usernames and Passwords Compromised

Late last week, the American Bankers Association disclosed that its computer systems had been compromised exposing thousands of members' personal information. The hacking occurred through its website's shopping cart tool, which is used to make purchases or to register for events. The hackers stole 6,400 usernames and passwords. The Association denies that any credit card information or financial information was compromised. The Association is urging its members to change their usernames and passwords for their ABA account.

— Linn Foster Freedman

Trump Hotel Collection Confirms Year-Long Data Breach

Trump Hotel Collection, the high-end hotel chain owned by the billionaire Republican presidential

nominee hopeful and real estate developer Donald Trump, has confirmed a data security breach involving malware that the company says was on its payment systems for just over a year. The company said that between May 19, 2014, and June 2, 2015, it believes there "may have been unauthorized malware access to some of the computers that host our front desk terminals and payment card terminals in our restaurants, gift shops and other point-of-sale purchase locations."

Stolen data could include credit and debit card information, including cardholders' full names, account numbers, expiration dates, and security codes. An initial investigation conducted by the chain has so far uncovered no evidence of misuse of customer data. However, it is offering affected customers 12 months of free identity-theft protection as a precautionary measure and has advised affected customers to check their financial statements for signs of suspicious activity.

This is not the first case of point-of-sale systems being targeted by hackers, and very likely won't be the last. Big name retailers like Home Depot and Target have been the victim of similar high-profile incidents in recent years.

— Kelly Frye Barnett

ENFORCEMENT + LITIGATION

EU Safe Harbor Program Declared Invalid by EU's Highest Court

The European Court of Justice (the EU's highest court) ruled on Tuesday, October 6, that the safe harbor pact between the EU and the U.S. should be declared invalid because it fails to provide adequate protection for EU citizens' data. The ruling follows Advocate General Yves Bot's opinion (covered here) two weeks ago that the safe harbor pact be struck down because U.S. officials, including the NSA, have unfettered access to EU citizens' data once it is transferred to the U.S.

The European Court of Justice declared that the program should be struck down because U.S. law enforcement officials' needs are put ahead of EU citizens' privacy rights. It stated "The United States safe harbor scheme thus enables interference, by United States public authorities, with the fundamental rights of persons, and the commission decision does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference."

So what does this mean for the 4,500 U.S. companies that have self-certified as safe harbor compliant since it came into existence in 2000?

According to the European Commission, it will continue to work toward a new framework for the transfer of EU citizens' data to the U.S. with the Department of Commerce, and the Commission expects companies to be able to use other privacy measures allowed by EU law. It will release "clear guidance" for data protection authorities in the EU in light of the ruling.

Companies may wish to continue to use appropriate data privacy and security measures for any data received from EU citizens and to keep a vigilant watch for guidance from the European Commission. We will be watching closely and will update you as guidance is issued.

But companies should also be aware that the Federal Trade Commission has publicly stated that despite the ruling, it will continue to monitor compliance by companies that have self-certified to the safe harbor program and move forward with enforcement actions. For the FTC, it is the status quo for now.

— Linn Foster Freedman

Twitter Ordered by Irish Court to Disclose Information about Author of Tweet

Twitter International Company (TIC) in Dublin, Ireland was reportedly ordered by a High Court to disclose data about the source of tweets about a whistleblower. The tweets, which included allegations of insurance fraud, are alleged to be defamatory.

The whistleblower provided the government with evidence that Irish hospital staff were accepting lavish gifts from a supplier. The whistleblower has brought a defamation action against the poster of the tweets, and asked the court to require Twitter to turn over information that would allow the whistleblower to identify the poster. The Court order TIC to turn over the poster's name. The Court also issued an injunction to prohibit the destruction of any evidence or records related to the tweets.

Twitter's policy is to not turn over information until required to do so by a court order. This is not the first time this year Twitter has made news for issues related to court orders to obtain access to user data. Earlier this year, San Francisco based Twitter changed its privacy policy for non-U.S. citizens. Non-U.S. citizen Twitter accounts are now held by Twitter International Company in Dublin, Ireland. This change was made to insulate non-U.S. citizens from the U.S. National Security Agency and other federal agency requests for their data. The accounts of U.S. citizens continue to be held by Twitter Inc. These changes also affect Periscope users as well.

See additional information here.

— Kathleen M. Porter

Judge Finds Genesis Healthcare Free of Any FCRA Violations

On October 1, 2015, U.S. District Judge Mark Kearney rules that Genesis Healthcare LLC (Genesis) did not violate the Fair Credit Reporting Act (FCRA) when it employed a third party to conduct a criminal history background check on a potential employee because Genesis provided notice to the employee that General Information Services Inc. (GIS) was going to conduct the inquiry. Genesis informed the potential employee that the inquiry uncovered one felony conviction for injuring a child BEFORE Genesis took any adverse action. Genesis even provided the potential employee with the opportunity to challenge the decision not to hire her based on the criminal history. Judge Kearney said, "All of the evidence confirms Ramos took advantage of the opportunity and Genesis evaluated her challenge, discussed it internally and only then reached a final decision."

However, while the court determined that Genesis did not violate the FCRA, and that GIS did not violate the FCRA by reporting a criminal conviction over 7 years old, the court determined that a jury will decide whether the background check was done properly and accurately by GIS. If the jury can conclude that the criminal history was a substantial factor in not hiring the plaintiff, GIS may be found negligent in not taking reasonable measures to ensure accuracy in its report to Genesis. We will keep you updated. For now, if you are running background checks on potential employees you should consider a refresher on what the FCRA requires.

— Kathryn M. Rattigan

HEALTH INFORMATION

VA OIG Reports Patient Data at Risk with Vendor

The Department of Veterans Affairs' Office of Inspector General recently issued a report, following a complaint that the VA Palo Alto Health Care System put veterans' health information at risk when it allowed personnel of a vendor to have access to VA patient information without appropriate background investigations or appropriate privacy and security awareness training. According to the report, "the Chief of Informatics…failed to ensure [vendor's] personnel met the appropriate background investigation requirements before granting access to VA patient information. The Chief of Informatics also failed to ensure [vendor] personnel completed VA's security and privacy awareness training." Finally, the report found that the ISOs failed to develop system security documentation and perform a system risk analysis prior to allowing the vendor to place its software on the VA servers.

Therefore, the OIG concluded that these actions "potentially jeopardized the confidentiality of veterans' PII, PHI, and other sensitive information.

— Linn Foster Freedman

HIPAA

OIG Report Spurs OCR to Announce Phase 2 Audits

On September 29, it was revealed that the HHS Office for Civil Rights (OCR) will commence Phase 2 of its HIPAA audit program in "early 2016." OCR's revelation regarding the Phase 2 audits, which had been the subject of significant industry speculation, came in response to two related reports on OCR's oversight and enforcement of HIPAA compliance by the HHS Office of Inspector General.

The OIG reports, available here and here, present a mixed-bag for OCR regarding fulfillment of its obligations under HIPAA to date. The OIG reports are based on a review of certain privacy cases and breaches reported to OCR between September, 2009 and March, 2011, and also interviews with OCR staff. The OIG reports contain a number of observations regarding OCR's HIPAA compliance practices, including:

- OCR's HIPAA Privacy Rule oversight is primarily reactive in response to complaints;
- OCR has not fully implemented the HIPAA audit program required under the HITECH Act;
- Cases where OCR identified HIPAA non-compliance most frequently involved hospitals and individual providers;
- OIG identified 23 covered entities within its sample that were investigated by OCR at least five times each; and
- OCR investigated all large breaches (breaches affecting at least 500 individuals) but did not document investigations into all small breaches (affecting less than 500 individuals) reviewed.

OIG then made certain recommendations for OCR to improve its policies and practices, including:

- OCR should fully implement an audit program;
- OCR should improve its documentation of corrective actions and small breaches;
- OCR should track previous breaches and investigations of covered entities; and
- OCR should develop a policy whereby OCR staff routinely check whether covered entities have

reported previous breaches.

Beyond announcing the Phase 2 audits, implementation of the OIG's remaining recommendations is likely to enhance OCR's enforcement activities by allowing OCR to more effectively leverage past non-compliance against entities facing allegations of HIPAA violations. OIG's findings suggest that certain covered entities are repeatedly violating HIPAA, and may have systemic compliance issues that merit heightened corrective action. Allowing OCR staff to track past corrective actions and routinely check previous breaches will enable OCR to increase penalties against entities identified as repeat offenders.

In addition to the OIG's conclusions, it is important that all entities subject to HIPAA recognize that OCR's Phase 2 audit announcement means that this is the final call for such entities to prepare for a HIPAA audit by assessing, and if necessary implementing, their HIPAA compliance policies and procedures.

— Conor O. Duffy

DRONES

Whopping $1.9 Million Fine Issued for Unauthorized Drone Use

The Federal Aviation Administration (FAA) issued a whopping $1.9 million fine against SkyPan International Inc. (Skypan), an aerial photography company, for carrying out 65 unauthorized drone flights from March 2012 to December 2014. SkyPan flew its drones over highly populated cities, such as New York City and Chicago, in "congested airspace" and allegedly "endangered the safety of [the] airspace" according to FAA officials. The drone flights did not have two-way radio capabilities, or altitude reporting equipment, which are both required under FAA drone regulations. Additionally, the FAA said that SkyPan did not have an airworthiness certificate or effective registration for its drones.

An FAA representative said, "Flying unmanned aircraft in violation of the federal aviation regulations is illegal and can be dangerous." However, SkyPan has the ability to respond to the FAA's violation notice by either paying this $1.9 million fine, submitting a response denying the allegations (which would likely lead to an even longer investigation), or referring the matter to the federal court system. SkyPan is required to make its move within 30 days.

— Kathryn M. Rattigan

CYBERSECURITY

AT&T Issues "What Every CEO Needs to Know about Cybersecurity"

We have reported before how CEOs, GCs and Boards are struggling with understanding and responding to cybersecurity risks within their organizations. Good for AT&T, which issued its report "What every CEO Needs to Know About Cybersecurity" Issue one: Decoding the Adversary," which "focuses on whether or not you and your board of directors are doing enough to protect against cyber threats."

The first issue "is intended to help strengthen your cybersecurity management and awareness. It provides insights into current threats, evolving technological and operational challenges, and offers suggestions to help you initiate improvements in your organization…"

This report is a definite read for all CEOs and boards.

— Linn Foster Freedman

---

1 Billion Android Phones Vulnerable to New Stagefright Bugs

Two new bugs, dubbed Stagefright 2.0, have impacted up to one billion Android phones since 2008. When the bugs are triggered, they allow attackers to use booby-trapped audio or video files to put malicious code on the phones. This can happen even when previewing the file.

Google has announced that it will release an update this week that will fix the bugs, although when users receive the fix will depend on the brand of the phone used.

— Linn Foster Freedman

Privacy Tip #4—What Do I Do When I Get a Letter Informing Me of a Data Breach?

We've all gotten them--the dreaded letter that informs us that our data has been compromised, including our Social Security number. Some have received so many of these "notifications" that they are de-sensitized, throw their hands in the air, and throw it in the trash. But doing this could put you at risk for identity theft.

In our experience with assisting companies with data breach response, approximately 10-15% of the people who receive the letter actually follow the instructions in the letter. That figure shows the general malaise of U.S. citizens when it comes to receiving breach notification letters.

So when we get one of those letters, what should we do? Read it, follow it and sign up for any services that are being offered. Whether you have been offered and are receiving credit monitoring for another breach, sign up for the service being provided in the new breach. Some products offered are for credit monitoring, which monitors your credit report, while others offer fraud resolution. Fraud resolution is different than credit monitoring, so you should avail yourself of each product that is offered. Sometimes you may have to sign up for the products online and keep reading the fine print to get to fraud resolution, but sign up for it if it is offered.

Get a copy of your credit report. You are entitled by law to get a free copy of your credit report every year through Annual Credit Report.com. DON'T GO TO FREE CREDIT REPORT.com. It is reportedly a scam.

Get your credit report, review it carefully, and make sure everything on it is accurate. If it isn't, federal law allows you to advise the credit reporting agencies that it is incorrect, and there is a process to follow. Although it is not an easy process, it is worthwhile to get any inaccurate information removed from your credit report.

In addition to credit monitoring, if you are the victim of a data breach, you can put a fraud alert or put a credit freeze on your credit accounts. Some state laws require companies to provide instructions on how to put a credit freeze on your account in the notification letter. There may be a small charge, which differs by state. When you put a fraud alert or a credit freeze on your account, you only have to tell one credit bureau, and that credit bureau is required to tell the other two. The advantage of a fraud alert or credit freeze is that no one can open an account without your actual authorization. So instead of waiting until a fraud might have occurred, which may be detected by credit monitoring, a fraud alert and credit freeze won't allow a new account (such as a credit card account or a utility account) to be opened without

additional measures to be taken. Hackers don't like to take additional measures, and will give up and go on to the next victim.

One caution about a security freeze. I don't recommend it if you are in the process of trying to get any type of credit, such as a credit card, a mortgage, a car loan or if you are refinancing your home. It is very difficult to even get credit for yourself if you have a credit freeze on your account. You have to jump through numerous hoops, so wait until your loan goes through before you put a freeze on your account. If you aren't getting any credit, it is one of the best ways to protect yourself from identity theft and fraud.

For more information, click here and here.

Also, some service providers offer free identity theft protection services for their members or customers, including employers, banks, automobile clubs and trade associations. Find out if you can get any services for free through these types of organizations and sign up for this benefit.

Identity theft continues to be the number one consumer complaint to the FTC, so protect yourself and sign up for any and all services when you receive that dreaded breach notification letter.

— 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.
