Attorney Advertising

Robinson+Cole

Data Privacy + Security

June 11, 2015

Data Privacy + Security Insider

ENFORCEMENT + LITIGATION

NY Dept. of Financial Services Releases Final Bitcoin License Regulations

The New York Department of Financial Services (NYDFS) made history last summer when it proposed Bitcoin regulations (reportedly the first in the nation) including the requirement that financial firms handling virtual currencies or Bitcoins in New York or for New York residents to obtain a license from NYDFS.

On June 3, 2015, the NYDFS adopted the final regulations, entitled "Virtual Currencies." The final Regulations prohibit any person or entity from conducting any Virtual Currency Business Activity without a license. Persons or entities chartered under New York Banking Law and approved by the Superintendent to engage in Virtual Currency Business Activity and merchants and consumers that utilize Virtual Currency solely for the purchase or sale of goods or for investment purposes are exempted from the licensure requirement.

The regulations have gone through two iterations with months of comments, roundtables and conferences sponsored by NYDFS. Primarily adopting the second version of the proposed Regulations, they are designed to regulate the "conduct of business involving Virtual Currency." They require that cybersecurity policies be put in place by companies obtaining a Virtual Currency license, including identifying a Chief Information Security Officer and Compliance Officer, that detailed books and records be put in place of all customers so they can no longer be anonymous, that detailed records be kept of each Virtual Currency transaction, and to suspend accounts of any users they feel may be engaging in fraudulent activity. In addition, written compliance policies, must be developed and adopted, including "policies with respect to anti-fraud, anti-money laundering, cyber security, privacy and information security," and such policies "must be reviewed and approved by the Licensee's board of directors or equivalent governing body."

The Regulations provide details on how to obtain a license and the initial application fee is $5,000 and is non-refundable. Although NYDFS is intent on regulating the new technology of Virtual Currencies, the Regulations do not provide for the payment of the application fee with Bitcoins and we suspect that NYDFS' technology system might not be able to handle a Bitcoin transaction.

Importantly, companies engaged in Virtual Currency Business Activity must apply for a license by July 20, 2015 or will be deemed to be "conducting unlicensed Virtual Currency Business Activity," and subject to regulatory enforcement by NYDFS. This gives Virtual Currency businesses a very short time frame to shore up policies and procedures and other requirements in order to obtain a license and comply with the Regulations.

- Linn Foster Freedman

U.S.A. Freedom Act Passed into law

On June 4, 2015, President Obama and his administration signed into law the U.S.A. Freedom Act, which "reform[s] the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes." So what does this mean? It means that finally, after the unleash of the Snowden Report back in 2012, the Federal Government is amending the Foreign Intelligence Surveillance Act (FISA) of 1978 and limiting the National Security Administration's (NSA) ability to collect bulk data from U.S. citizens. The Act requires telephone companies to continue to collect and store telephone records and data in the same way that they do now, but now, instead of simply supplying that same information to the NSA, the telephone companies would only be required to turn over the information in response to a request that has been previously approved by the Foreign Intelligence Surveillance Court (FISC). Some skeptics believe this may not be enough to stop the bulk data collection. The passage of this Act also restored three sections of the Patriot Act, which sunset last week, allowing the Federal Government to continue certain surveillance efforts for national security purposes. Senator Patrick Leahy of Vermont, said "It's historical. It's the first major overhaul of government surveillance in decades." While the legislation has been passed, and politicians seem hopeful, only time will tell whether something like this can truly restore the American public's trust in the Federal Government.

- Kathryn M. Sylvia

Zappos Proposed Data Breach Class Action Litigation Dismissed

Continuing the growing trend of dismissing data breach cases when there is no evidence of actual harm, the United States District Court for the District of Nevada last week dismissed a class action case filed against Zappos related to a 2012 hacking incident. Following the hacking incident, Zappos provided notice of the data breach to over 24 million customers that their names, emails addresses, addresses, telephone numbers, last four digits of their credit card numbers and account numbers and passwords were compromised.

The judge dismissed the proposed class action lawsuit as the plaintiffs failed to allege an adequate injury in order to claim appropriate standing to sue Zappo's under Article III. There were no allegations of actual identity theft or fraud against any of the customers in the Complaint, and therefore, the judge found that the plaintiffs did not have standing to sue, ruling consistently with the majority of Courts that have addressed the issue to date. The fact that none of the plaintiffs suffered any harm since the breach occurred in 2012 was further support of the dismissal. Although there are still a few outlying cases that hold to the contrary, this area of the law is becoming more settled in the wake of numerous data breaches.

- Kathryn M. Sylvia

DATA BREACH

Heartland Payment Systems Suffers Another Data Breach

Heartland Payment Systems suffered one of the largest breaches in history in 2008, when over 100 million credit and debit cards issued by hundreds of financial service companies were stolen from their payroll payment processor. That breach reportedly cost the company over $100 million in costs, fines and penalties.

Heartland has notified approximately 2,200 individuals that their personal information was stolen when an intruder broke into the physical office of one of Heartland's offices located in Santa Ana, CA and took off with 11 computers, 4 of which contained personally identifiable information, which may include Social Security numbers and bank account information. Reports indicate that although the computers were password protected, unfortunately, they were not encrypted. A basic security concept is to mitigate losses, learn from previous incidents, and implement processes so incidents won't happen again. In

reviewing risks, take into consideration physical, technical and administrative safeguards of both paper and electronic records. A physical burglary can happen, and it is no different than losing a laptop or being the victim of a cyber-hacking incident.

- Linn Foster Freedman

SOCIAL MEDIA
California Introduces 'Opt-In' Digital Assets Bill

On June 8, 2015, it was reported that the California legislature is considering a new bill, A.B. 691, which would set forth the procedure for handling a deceased individual's digital assets, including their social media accounts. Under this bill, a deceased individual's digital assets and communications may only be disclosed to an estate executor IF the deceased individual 'opted-in' to that choice through his or her online service provider or his or her will. This is a new twist on digital assets legislation. Back in 2014, the National Conference of Commissioners on Uniform State Laws created a model law that would allow executors and trustees to access a deceased's individual's digital assets unless the individual specifically prohibited it. Assemblyman, Ian C. Calderon said, "There have been several attempts nationally to create a model for other states to use in order to address [the issue of digital assets], but California has the opportunity with the passage of A.B. 591 to take the reins and to be the champion for the tech industry." We will follow the bill's journey and keep you updated.

- Kathryn M. Sylvia

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and 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 and Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---