What’s trending in data privacy & security

We’re looking ahead on all fronts in privacy and data security. A NYC-based brokerage settles for $2 million, as the SEC continues to crack down on the privacy rights of investors. And the Department of Justice offers recommendations for those impacted by Gameover Zeus and Cryptolocker. Here’s a round-up of the latest news and what’s on the horizon.

Enforcement & Litigation

*Liquidnet, Inc. to pay SEC penalty of $2 million to settle charges related to failure to protect confidential information in “dark pool” trading system*

Liquidnet, Inc., a New York-based brokerage firm, has agreed to pay a $2 million penalty to settle charges against it by the SEC alleging that the firm permitted access to and used confidential trading information of its “dark pool” subscribers, despite its claims to those subscribers and its obligations under SEC Regulation ATS.

Liquidnet’s “dark pool” trading system allowed its members (or “subscribers”) to indicate their confidential trading intentions, which the alternative trading system (“ATS”) would use to look for “matches” with other members interested in buying and selling the same stock. Liquidnet assured its members in subscription agreements and marketing materials that it was protecting the confidentiality of their trading information and minimizing information leakage.

Section 301(b)(10) of Regulation ATS requires that an ATS establish safeguards and procedures to protect subscribers’ confidential trading information and adopt and implement adequate oversight to ensure that those safeguards and procedures are being followed.

The SEC claims that while Liquidnet assured its subscribers that the trading information was confidential, Liquidnet made the information available to employees that were not responsible for the operation of the ATS; used that confidential trading information to market its system to corporations, private equity and venture capital groups; and failed to disclose this conduct to its subscribers. According to the SEC, Liquidnet also failed to follow through with subscribers’ requests to opt out of an application that permitted executive users to track institutional demand by viewing trading information.
In addition to the penalty, the SEC issued a cease and desist against Liquidnet and censured the
group, indicating just how seriously the SEC takes obligations to protect confidential information.
The SEC's Order is available here.—Kate A.F. Martinez

Best Buy pays $4.5 million in class action settlement for its alleged violations of the TCPA

On June 10, 2014, Best Buy Co., Inc. (“Best Buy”) agreed to pay $4.5 million to settle a Telephone
Consumer Protection Act (TCPA) class action in which class members accused Best Buy of making
unsolicited automated telephone calls related to a customer rewards program.

The suit was filed in April 2010. Class members filed suit because they received telephone calls
related to their redemption of “Reward Zone” points—the class argued that these telephone calls
were not simply informational calls, but that they constituted telemarketing calls under the TCPA.
The class also alleged that Best Buy violated the Washington Automatic Dialing and Announcing
Act, which also prohibits telemarketing calls without prior consent from the consumer.

A Washington federal court approved the settlement agreement, which will be paid out as follows:
approximately $3.2 million of the settlement will be divided among 439,000 Washington State class
members and 42,000 class members from various other states; the additional funds will be
distributed for court-awarded fees and expenses. More and more TCPA class action settlements are
popping up. Businesses must be sure they are following TCPA requirements or they could end up
tangled in litigation.—Kathryn M. Sylvia

Data Breach

Illinois class action case against medical group dismissed

Although we commented last week that the highest court in West Virginia recently bucked the
trend by allowing a data breach class action case to proceed despite the failure of the plaintiffs to
allege actual injury, the Circuit Court in Lake County, Illinois, recently followed established case
law and dismissed a class action case against Advocate Health and Hospitals Corp. (“Advocate”) as
the plaintiffs failed to allege actual injuries related to a data breach.

The case involved the theft of four unencrypted laptops in July 2013 that contained the names,
addresses, dates of birth, medical diagnosis, health insurance information and Social Security
numbers of Advocate’s patients.

Advocate notified the patients following the breach, and a class action lawsuit was filed against it
alleging, among other things, negligence, violation of the Illinois Consumer Fraud and Deceptive
Business Practices Act, invasion of privacy and intentional infliction of emotional distress. The
Illinois Circuit Court dismissed the case as the plaintiffs were unable to allege or provide evidence
that the information contained in the laptops was actually accessed, used or sold. The court further
found that the plaintiffs did not satisfy the “injury in fact” requirement for standing to pursue the
claims, and that the mere risk of identity theft was insufficient to defeat a Motion to Dismiss.

This case is in line with the majority of data breach cases, which require plaintiffs to allege actual
injury in order to proceed. Nonetheless, as seen by the opinion of the West Virginia court, as more
state law claims are pursued, and more courts weigh in on the standing issue, the consistency in
this area of law will be in jeopardy. We will continue to monitor and report on these cases as they
develop.—Linn Foster Freedman
Social Media

**NH latest state to prohibit employers from requesting access to social media**

New Hampshire became the latest state to enact legislation to prohibit employers from requesting or requiring an employee or prospective employee from disclosing login information in order to access an electronic personal account or service.

In addition, the statute prohibits an employer from compelling an employee or applicant to add the employer to a list of contacts associated with an electronic mail account or personal account or require the employee to reduce privacy settings that would allow third parties to have access to the account.

Finally, the statute prohibits an employer from disciplining an employee for refusal to provide the information to the employer.

New Hampshire joins the following states who have enacted social media laws thus far: Louisiana, Oklahoma, Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Tennessee, Utah, Washington and Wisconsin.—**Linn Foster Freedman**

Cybersecurity

**Gameover Zeus and Cryptolocker assistance**

We reported last week about the [wide effects of Gameover Zeus and Cryptolocker](#) and heard from many of you asking for more information about remediation efforts. According to the Department of Justice, if you are a known victim, you should be contacted by your Internet Service Provider directly. In addition, a self-help tool is available [here](#).

With respect to Cryptolocker, if your computer was encrypted prior to the infection, there is no solution or tool to assist. You may need to engage a forensic firm to assist in retrieving your back-up data. Not very encouraging, but we hope this helps.—**Linn Foster Freedman**

For more information on the contents of this alert, please contact:

— Linn Foster Freedman, Privacy & Data Protection Group Leader, at lfreedman@nixonpeabody.com or 401-454-1108
— Kate A.F. Martinez at kmartinez@nixonpeabody.com or 585-263-1332
— Kathryn M. Sylvia at ksylvia@nixonpeabody.com or 401-454-1029