Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How 3 Agencies Prosecute Lax Cybersecurity

Law360, New York (March 2, 2016, 10:42 AM ET) --


Thomas Rohback


Patricia Carreiro

Following a data breach, hacked companies not only face lawsuits by private plaintiffs, but also enforcement actions by state and federal regulators. For example, following the Target Corp. breach, Target was not only sued by consumers, financial institutions, and shareholders, it also faced a Federal Trade Commission investigation. Similarly, following its breach, DSW Inc. faced parallel actions from consumers and the FTC; and Wyndham Worldwide Corp. was sued by both the FTC and its shareholders.

This article discusses three federal regulators who have used their enforcement authority to prosecute lax cybersecurity: the FTC, the U.S. Securities and Exchange Commission and the U.S. Department of Health and Human Services.

Federal Trade Commission

Section 5 of the FTC Act authorizes the FTC to prosecute "unfair or deceptive acts or practices in or affecting commerce." Functioning under the theory that lax cybersecurity is an unfair trade practice and misrepresenting cybersecurity is a deceptive trade practice, the FTC has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data is an unfair practice.

For example, in one recently settled case against GMR Transcription Services Inc., the FTC alleged that GMR's inadequate cybersecurity protocols, including its failure to properly oversee its service providers, were "deceptive and unfair information security practices that exposed the personal information of thousands of consumers online." Press Release, Fed. Trade Comm'n, FTC Approves Final Order In Case Against GMR Transcription Services (Aug. 21, 2014).

FTC data security settlements generally involve some combination of the following: a requirement that the company implement new cybersecurity practices, monetary penalties, redress for injured consumers, and biennial cybersecurity audits for 20 years.

For example, following a data breach at BJ's Wholesale Club Inc., the FTC prosecuted BJ's poor cybersecurity practices, including its failure to encrypt consumer personally identifiable information,

securely store PII, only store PII as long as necessary, and use readily available security measures to prevent and detect hacks, as an unfair business practice. BJ's Wholesale Club Inc., No. C-4148 (Fed. Trade Comm'n Sept. 20, 2005). The parties settled and BJ's agreed to implement new cybersecurity protocols and obtain biennial cybersecurity audits for the next 20 years. Similarly, when three credit report reselling companies settled FTC allegations that they did not take reasonable efforts to protect consumer PII, they were required to strengthen their cybersecurity practices and subject themselves to biennial cybersecurity audits for 20 years.

While most companies have simply settled FTC allegations regarding their lax cybersecurity practices, some have pushed back. Following three separate hacks at Wyndham between 2008 and 2010, the FTC brought a complaint against Wyndham, alleging that the hotel engaged in deceptive and unfair practices by failing to maintain "reasonable and appropriate" cybersecurity and misleading customers regarding its cybersecurity practices. Rather than settle the charges, Wyndham challenged the FTC's authority to regulate cybersecurity as an unfair or deceptive trade practice. The Third Circuit found such authority within the broad language of Section 5 of the FTC Act. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015). While the FTC's required showing of harm has not been conclusively settled, one administrative judge has required the FTC to show either actual or likely harm. Press Release, Fed. Trade Comm'n, Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD Inc. (Nov. 19, 2015).

Securities and Exchange Commission

Unlike the FTC, the Securities and Exchange Commission is not required to show harm and has brought a number of data privacy or cybersecurity enforcement actions under Rule 30(a) of Regulation S-P ("the Safeguard Rule"), requiring companies to have written and reasonable policies and procedures for safeguarding customer PII.

In LPL Financial Corp., No. 3-13181 (Sec. and Exch. Comm'n Sept. 11, 2008), the FTC sued respondent LPL Financial Corp. after an unauthorized person(s) logged into LPL's representatives' accounts and submitted unauthorized trade requests. While LPL blocked the majority of these trades, reversed the others, and compensated customers for any losses, the SEC prosecuted it for failing "to adopt written policies and procedures reasonably designed to protect its customer information." The settlement censured LPL, required it to undertake a number of steps to improve its security, and ordered it to pay a fine of $275,000.

The SEC settled a similar action against another respondent the following year in Commonwealth Equity Services LLP, No. 3-13631 (Sec. and Exch. Comm'n Sept. 29, 2009). In that case, respondent Commonwealth Equity Services LLP was sued by the SEC after one of Commonwealth's employees had his credentials stolen by a hacker using a malware/keystroke virus. The hacker used the access credentials to place unauthorized stock purchase orders, in the process gathering customers' PII. Although Commonwealth canceled the purchases and absorbed the resulting losses, the SEC nonetheless prosecuted Commonwealth for failing to have adequate written policies and procedures to protect its customers' PII. Commonwealth was censured and fined $100,000. Then, for years, the SEC did not bring any cybersecurity enforcement actions.[1]

The SEC's pause in enforcement actions, however, came to an end in 2015, when the SEC sued investment advisor R.T. Jones Capital Equities Management Inc. Order, R.T. Jones Capital Equities Mgmt. Inc., No. 3-16827 (Sec. and Exch. Comm'n Sept. 22, 2015). R.T. Jones stored customer PII on a third-party-hosted server which was hacked, exposing its customers' PII. By all accounts R.T. Jones took more than adequate post-breach action to investigate and provide notice of the breach, even hiring three different cybersecurity firms to confirm and investigate the hack. Nonetheless, the SEC censured R.T. Jones and fined it $75,000 for failing to have appropriate written cybersecurity policies, specifically noting R.T. Jones' failure to conduct periodic risk assessments, implement a firewall, encrypt PII and

maintain a cyber response plan.

Department of Health and Human Services

When it comes to federal enforcement of cybersecurity and cybersecurity breach notification for compromises of protected health information, the Department of Health and Human Services, pursuant to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, has taken the lead. As of Dec. 30, 2015, HHS has resolved 119,964 HIPAA complaints, roughly 66 percent of which required the health care entity to take corrective action. Numbers at a Glance, U.S. Dep't of Health & Human Services (Dec. 30, 2015). Private practices were the most common entities required to take corrective action, followed by general hospitals, outpatient facilities, pharmacies and health plans (in that order). Id. Some of the most common compliance issues prosecuted by HHS involve the impermissible disclosure of PHI and the lack of safeguards to protect PHI. Enforcement Highlights, U.S. Dep't of Health & Human Services (Dec. 30, 2015).

While most HHS enforcement actions merely require covered entities to take corrective measures, HHS has settled 26 separate cases in which it imposed civil fines totaling $27,974,400, and referred 566 cases to the U.S. Department of Justice for criminal prosecution. Id. Notable civil fines include a $4.8 million fine of New York Presbyterian Hospital and Columbia University Medical Center for their lax cybersecurity protocols, a $1,725,220 fine of Concentra Health Services following the theft of one of its laptops containing unencrypted PHI, and a $1.7 million fine of Anthem (then WellPoint) following its security weaknesses making patients' PHI available via internet search. HHS is now launching an industry-wide audit campaign, which could mean even more HIPAA enforcement actions ahead.

Cases involving the lack of safeguards to protect PHI often draw HHS and the FTC together. For example, HHS and the FTC joined together to prosecute both CVS Pharmacy Inc. and Rite-Aid Corp. for their poor efforts to protect consumer information after they were found to have disposed of tubes containing patients' information in the trash. CVS settled the claims with both regulators, agreeing to (among other things) pay HHS $2.25 million, implement new privacy protections, obtain biennial audits for the next 20 years, and avoid future misrepresentations regarding consumers' privacy. Press Release, Fed. Trade Comm'n, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009). Rite Aid settled similar claims with both regulators for $1 million, new privacy protections, biennial audits for 20 years, and avoiding future misrepresentations. Press Release, FTC Approves Final Order Settling Charges that Rite Aid Failed to Protect Medical and Financial Privacy of Customers and Employees (Nov. 22, 2010).

The FTC and HHS continued their cooperation, prosecuting Henry Schein Practice Solutions Inc., a dental software company, for using a vendor with insufficient cybersecurity practices while at the same time advertising its software's protection of patient privacy. Press Release, Fed. Trade Comm'n, Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data (Jan. 5, 2016).

Despite HIPAA's 566 referrals to the Department of Justice, criminal HIPAA prosecutions are extremely rare and generally involve individuals who abuse patients' PHI for financial gain. For example, a phlebotomist who stole a patient's PHI and used it to obtain credit cards in that patient's name, taking cash advances and making fraudulent purchases of over $9,000; a clinic employee who sold over a thousand Medicare patients' PHI; and a hospital employee who stole patients' social security numbers and used them to file false tax returns.

The risk of compromised medical information, however, goes far beyond mere financial loss and impacts patient safety. The Ponemon Institute's 2013 study reveals that due to medical identity theft, 14 percent of victims received delayed treatment; 15 percent were misdiagnosed, 13 percent received the wrong

treatment, and 11 percent were prescribed the wrong drug. Looking to protect PHI, some hospitals push large amounts of new software out to their system. Unfortunately, some of these software updates overwhelm the decade-old hardware at some hospitals, causing outages.

Ransomware could have similarly catastrophic results on patient safety and has already begun to hit hospitals. If a system crash or freeze happens at the wrong moment, lives could be at risk.[2] Even if a particular glitch does not crash a system, the dangers of a menacing hacker in a hospital's system are obvious. Consider, for example, the repercussions of a hacker altering patients' health records data, including denying providers access to, or altering a patients' record of, their blood type, allergies, and other information that could cause serious mistreatment. Accordingly, hospitals that proceed with outdated machinery or inadequate cybersecurity are opening themselves up to serious liability exposure.

The risk of physical injury from a hack, however, is not limited to health care. Hacked cars, planes and utilities are a few examples of hacks that could cause serious physical injuries. It is only a matter of time until companies find themselves facing personal injury liability for cybersecurity breaches.

—By Thomas Rohback and Patricia Carreiro, Axinn Veltrop & Harkrider LLP

Thomas Rohback is a partner in Axinn's New York and Connecticut offices. During one year, he tried three federal court jury cases in a three-month period and obtained a directed verdict in each case. Patricia Carreiro is an associate in the firm's Connecticut office.

[1] During the SEC's enforcement gap, the Financial Industry Regulatory Authority ("FINRA") continued using the SEC's Safeguard Rule, as well as the NASD Conduct and FINRA Rules, to enforce consumers' data privacy rights. For example, FINRA censured and fined Valores Finamex International, Inc. $27,500 for, among other things, failing to establish required customer privacy safeguards, D.A. Davidson & Co. $375,000 for failing to adequately protect its customers' PII, and Sterne Agee & Leach Inc. $225,000 after it lost a laptop containing the unencypted PII of over 350,000 of its customers. Letter of Acceptance, Waiver and Consent, Valores Finamex Int'l, Inc., No. 2009016196001 (Fin. Indus. Regulatory Auth. Feb. 18. 2010); Letter of Acceptance, Waiver and Consent, D.A. Davidson & Co, No. 20080152998 (Fin. Indus. Regulatory Auth. Apr. 9, 2010); Letter of Acceptance, Waiver & Consent, Sterne, Agee & Leach, Inc., No. 2014041619501 (Fin. Indus. Regulatory Auth. May 22, 2015).

[2] This is particularly true as areas such as interventional radiology continue to expand. An interventional radiologist is entirely dependent on technology. If that technology shuts down in the midst of a delicate procedure or as a bleed begins, that radiologist is helpless to save his patient.