Financial Fraud Law Report

AN A.S. PRATT & SONS PUBLICATION JULY/AUGUST 2013

The FINANCIAL FRAUD LAW REPORT is published 10 times per year by Matthew Bender & Company, Inc.
POSTMASTER: Send address changes to the *Financial Fraud Law Report*, LexisNexis Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974. *ISBN: 978-0-76987-816-4*

Five Cybersecurity Mistakes Companies Make that Could Result in Their Prosecution

MICHELLE A. REED AND ELIZABETH D. SCOTT

Five common cybersecurity mistakes may lead to heightened regulatory scrutiny/prosecution. The authors provide strategies that may help companies successfully avoid these potential pitfalls.

Over the last two years, more than 40 million confidential records have been exposed from countless data breaches. These types of cyber attacks are no longer limited to the financial and health care sectors: hackers and other foes now target companies' intellectual property and the nation's critical infrastructure.[1] These and other cyber threats have gained significant public and political attention and have been characterized as one of the nation's most serious national security challenges.[2] In light of the increasing threat cyber attacks pose to the country's national and economic security, lawmakers have called for heightened regulatory scrutiny with respect to the disclosures companies are making regarding cybersecurity risks, material cyber incidents, and the steps taken to manage cyber threats.[3] State and federal regulators, including the Securities and Exchange Commission and the Federal Trade Commission, have responded affirmatively to these

Michelle A. Reed is a partner and Elizabeth D. Scott is counsel in the Dallas office of Akin Gump Strauss Hauer & Feld LLP, focusing on representing public companies and their officers and directors in securities and privacy litigation, internal investigations, and regulatory investigations and enforcement proceedings. The authors can be reached at mreed@akingump.com and edscott@akingump.com, respectively.

Published by Matthew Bender & Company, Inc. in the July/August 2013 issue of *Financial Fraud Law Report*.

requests, issuing guidance concerning cybersecurity disclosure requirements and conducting targeted reviews to ensure compliance with such guidance.

This increased regulatory attention to cybersecurity risks continues to grow, and in May 2013, the new SEC Chairman, Mary Jo White, announced that she had initiated a review of the current SEC cybersecurity disclosure guidance with an eye toward future SEC action in this area.[4] In this environment of enhanced focus on cybersecurity risks and their disclosure, regulatory exposure from data breaches and other cyber attacks is significant, and companies subject to such incidents are likely to become the immediate subject of scrutiny by state attorneys general and federal agencies. Five common cybersecurity mistakes may lead to heightened regulatory scrutiny/prosecution, and the following strategies may help companies successfully avoid these potential pitfalls.

FAILURE TO ADEQUATELY DISCLOSE CYBERSECURITY RISKS AND CYBER INCIDENTS IN SEC FILINGS PURSUANT TO ITEM 503(c) OF REGULATION S-K

Failing to adequately disclose cybersecurity risks and cyber incidents in public filings with the SEC exposes companies to increased scrutiny from the SEC. Item 503(c) of Regulation S-K of the Securities and Exchange Act of 1934 requires disclosure of companies' most significant risk factors.[5] Due to the expanding reliance on digital technologies and the growing threat of cyber attack, cybersecurity risks have become an increasingly significant risk factor for many companies.

Recognizing this fact and responding to lawmaker requests for greater regulatory oversight, in October 2011, the SEC Division of Corporation Finance ("Corp Fin") issued guidance concerning cybersecurity disclosure obligations.[6] Corp Fin advised public companies to consider including cybersecurity threats and cyber incidents as a risk factor disclosure pursuant to Item 503(c) and to make other cybersecurity disclosures as necessary (e.g., including cybersecurity-related disclosures in the MD&A, Description of Business, Legal Proceedings, Financial Statements, and Disclosure Controls and Procedures portions of their public filings).

Corp Fin has initiated a review of public company cybersecurity disclosures to ensure compliance with this guidance and proper disclosure under

Item 503(c).[7] As part of this review, Corp Fin issued comment letters to approximately 50 companies addressing various shortcomings with respect to the disclosure of cybersecurity risks and cyber incidents.[8] Although these comment letters relate to companies of varying size and industry, they reveal a few common expectations regarding the nature and specificity of a company's required cybersecurity disclosures and the disclosure failures most likely to lead to heightened regulatory scrutiny.

First, companies must assess and disclose their cybersecurity risks. In a number of its recent comment letters, Corp Fin identified companies' failures to include any cybersecurity risk disclosure and requested that such a disclosure be included in future filings. Companies in industries that are frequently subject to cyber attack are especially likely to catch Corp Fin's eye for failing to include a cybersecurity risk factor disclosure, as are companies that have been subject to recent news articles or public statements concerning cybersecurity risks.

Second, disclosures must include sufficient detail concerning the nature and extent of companies' cybersecurity risks and their efforts to remediate such risks. In repeated comment letters, Corp Fin has requested that companies do more than merely list cyber attack as one of many potential hazards a company may face. Rather, Corp Fin has requested that companies include a detailed, separate discussion concerning the risks cyber attacks and other cyber incidents pose to their businesses, operations, and reputations.

Third and most significantly, Corp Fin has requested that companies disclose if they have been subject to prior cyber attacks or other incidents, *even if such incidents were not material to their business or operations*. In the vast majority of the comment letters issued with respect to its cybersecurity guidance, Corp Fin has requested additional information concerning whether the company at issue has previously experienced cyber attacks or other cyber incidents, and has requested that the company disclose any such prior attacks or incidents to provide a proper context for the company's cybersecurity risk disclosure. Corp Fin has requested disclosure even if the company does not consider the prior attacks material to its business or results of operations, though it has suggested that the company may mitigate the impact of such disclosure by explaining that the prior attacks or incidents did not significantly impact the company's performance or operations.

FAILURE TO ESTABLISH AND FOLLOW A COMPANY-WIDE CYBERSECURITY RISK MANAGEMENT AND DATA PROTECTION PROGRAM

Companies make a critical mistake if they lack company-wide cybersecurity risk-management and data-protection programs. Although there is no overarching privacy/cybersecurity regulator, the FTC has interjected itself as the principal federal regulator under the Federal Trade Commission Act's prohibition of "unfair or deceptive acts or practices in or affecting commerce." An "unfair or deceptive" act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[9] State regulators almost uniformly have similar authority to protect consumers against unfair or deceptive trade practices.

Accordingly, there is a complex web of affirmative requirements for company-wide cybersecurity risk management programs. Some regulations, such as the Health Insurance Portability and Accountability Act ("HIPPA") for the health sector and the Gramm-Leach-Bliley Act ("GLBA") for the financial sector, are well known. However countless others impact the way data should be handled.[10] Even state laws require affirmative protection. For example, Massachusetts's state security law, Mass. 201 CMR 17, requires businesses holding "personal information" to:

(1) designate an individual who is responsible for information security;

(2) anticipate risks to personal information and take appropriate steps to mitigate such risks;

(3) develop security program rules;

(4) impose penalties for violations of the program rules;

(5) prevent access to personal information by former employees;

(6) contractually obligate third-party service providers to maintain similar procedures;

(7) restrict physical access to records containing personal information;

(8) monitor the effectiveness of the security program;

(9) review the program at least annually and whenever business changes could impact security; and

(10) document responses to incidents.

Similarly, the SEC and CFTC adopted "red flag" rules that became effective May 20, 2013, with compliance required by November 20, 2013.[11] Like the FTC's long-standing red flag rules, the SEC/CFTC rules require a wide variety of companies to adopt Identity Theft Protection Programs that identify warning signals that should alert companies to the risk of identity theft and mitigate any identity thefts that ultimately occur. The red flags program must be *approved by a company's board of directors* or a committee *designated by the board*.

Both state and federal regulators have brought actions against companies that have failed to adequately implement these types of data protection requirements. For example, in 2012, the FTC charged EPN, Inc. with failure to have an appropriate security plan, failure to train employees, and failure to scan its networks to identify peer-to-peer applications. A few areas of data protection failure are especially likely to draw attention: inadequate security, employee negligence, failure to train employees, failure to adhere to privacy policies, retroactive privacy policy changes, deceptive data collection, and inadequate disclosure of data collection practices.

The primary take away is that companies need to identify their legal requirements for data protection and then map their internal processes to determine whether they are currently in compliance. Further protective measures, such as tracking digital information that leaves the company and evaluating who is logging into the network, can be essential to preventing data loss. Although many regulations only address personally identifiable information, PIT (which includes information ranging from social security numbers to zip codes, depending on the regulation), companies should apply safeguards to all information of value, including their own intellectual property.

FAILURE TO ADOPT AND IMPLEMENT A COMPREHENSIVE CYBER BREACH RESPONSE PLAN

Companies that fail to adopt and implement a comprehensive cyberbreach response plan should expect attention from the FTC. The FTC has brought 40-plus actions against companies for data breach, across a wide variety of industries. For example, the FTC sued Wyndham Hotels for alleged data security failures that allowed hackers to breach its systems three times. Wyndham has fought this lawsuit in the U.S. District Court in New Jersey, arguing that it had reasonable security practices. The court's decision is expected any day and will likely impact the security policies of companies throughout the country. The causes of the breaches the FTC has prosecuted, like those at the Wyndham Hotels, have ranged from cyber attacks to negligent employees. In nearly every case, the FTC has imposed a standard penalty: "implement a comprehensive information security program and . . . obtain independent, third-party security audits every year for twenty years." Thus, a single incident of breach may result in at least 20-years of enhanced FTC scrutiny.

To avoid such prosecution, companies should adopt and implement a comprehensive cyber-breach response plan. The plan should be vetted by the board or its designated subcommittee and should be tested regularly. There should be a single point of contact for coordinating the company's response to the cyber incident, and outside counsel should be retained immediately to provide legal advice and the protection of work product privilege. With a previously established cyber-breach response team that includes stakeholders from the IT, legal, and finance departments and senior executives designated by the board, the company should be prepared to contain the breach, coordinate with law enforcement, and develop a communication strategy to minimize any public relations damages resulting from the breach.

FAILURE TO PROVIDE PROPER NOTIFICATION OF A MATERIAL CYBER BREACH OR OTHER INCIDENT PURSUANT TO STATE LAW AND OTHER REGULATIONS

Failing to provide proper notification of a cyberbreach is a mistake that could be costly. Nearly every state in the union has some form of data breach

notification statute, but the statutes vary widely. Some states require notice simply upon "reasonable belief" that PII has been *accessed* while other states require notice only when companies have found *risk of misuse or harm* with respect to such data. Although the vast majority of these statutes do not provide a private right of action (i.e., do not allow private citizens to sue based on the particular statute), all are enforceable by a state official, typically the state attorney general.

Such enforcement actions can be costly to companies. For example, 42 state attorneys general entered into a $12.25 million settlement with The TJX Companies, Inc. as a result of a massive data breach that exposed over 90 million transaction records. Similarly, Choice Point entered into a $15 million settlement with the FTC and a further settlement with 44 state attorneys general requiring the company to make multi-million dollar operational changes to its business.

Companies should carefully consider when notification is necessary, who must be notified, and what the contents of the notification must be – and they have very little time to make this evaluation, since some statutes require notification within 24 hours. Additionally, implementing preventive measures, such as credit monitoring for affected consumers, result in a six-fold lower risk of being sued in federal court.[12]

FAILURE TO MONITOR AND DISCLOSE CYBERSECURITY RISKS AND INCIDENTS ASSOCIATED WITH SIGNIFICANT THIRD-PARTY SERVICE PROVIDERS AND BUSINESS PARTNERS

In addition to monitoring and disclosing its own cybersecurity risks and incidents, a company must also monitor and disclose the cybersecurity risks and incidents associated with its significant third-party service providers and business partners, and may be subject to enhanced regulatory scrutiny for failing to monitor and disclose such risks. Companies increasingly rely on third parties for critical aspects of their businesses, including those involving key data and electronic infrastructure. Companies also frequently depend on third parties for the encryption and authentication technologies used to securely store and transmit confidential information. As such, the cybersecurity risks and incidents associated with a company's third-party service

providers and business partners may significantly impact its operations and the safety of its data. In light of this risk, regulators, including the SEC, have requested that disclosures be made with respect to the cybersecurity risks and incidents of a company's significant third-party service providers and business partners and the potential impacts of such risks on the company itself. Similarly, the FTC has prosecuted companies for failure to adequately safeguard data accessed by third parties. For example, in *In the Matter of MySpace, LLC*, in 2012, the FTC prosecuted MySpace for "constructive sharing"—the sharing of PII with third parties that can be used by third parties to access PII.

Thus, to avoid regulatory scrutiny with respect to the actions and inactions of third parties, companies should carefully monitor and disclose the cybersecurity risks and incidents associated with their third-party service providers. They should also incorporate and address such risks as part of their comprehensive cybersecurity risk management and data protection programs, and these risk management plans should be reduced to contract with all third-parties that handle company data.

NOTES

[1] According to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, the number of cyberthreats to critical U.S. infrastructure by mid-2013 has already exceeded the total number of incidents in 2012. Alexei Alexis, *DHS Report Shows "Troubling" Cybersecurity Trend, Carper Says*, BLOOMBERG BNA FEDERAL CONTRACTS REPORT, July 9, 2013.

[2] *See, e.g.*, Proclamation No. 13636, 78 Fed. Reg. 11739, 2013 WL 596302, at *11739 (Feb. 12, 2013).

[3] *See, e.g.*, Letter from Senator John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp., to Mary Jo White, Chairman, SEC (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=File.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51 (last visited June 30, 2013).

[4] Letter from Mary Jo White, Chairman, SEC, to Senator John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp. (May 1, 2013), *available at* http://www.commerce.senate.gov/public/?a=File.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf (last visited June 30, 2013).

[5] 17 C.F.R. § 229.503(c).

[6] Securities & Exchange Commission, CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last visited Aug. 7, 2013).

[7] Letter from Mary Jo White, Chairman, SEC, *supra* note 4, at 1.

[8] *Id.*

[9] 15 U.S.C. § 45(n).

[10] Some examples include the Cable Communications Policy Act, CAN-SPAM Act, Children's Online Privacy Protection Act, Computer Fraud and Abuse Act, Drivers Privacy Protection Act, Employee Polygraph Protection Act, Fair Credit Reporting Act, Family Education Rights and Privacy Act, Foreign Intelligence Surveillance Act, Stored Communications Act, Telephone Consumer Protection Act, Video Privacy Protection Act, and countless others.

[11] 17 C.F.R. pts. 162, 248.

[12] Romanosky, Sasha, et al., *Empirical Analysis of Data Breach Litigation*, June 1, 2012, *available at* http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf (last visited Aug. 6, 2013).