Engels Tejeda

Partner
801.799.5851
Salt Lake City
ejtejeda@hollandhart.com

Waiting May Cost You: Sanctions for Inadequate Cybersecurity Practices May Be Imposed Before a Cyber Attack

Insight — 8/1/2016

This year the Consumer Financial Protection Bureau, the Securities and Exchange Commission, and the Federal Trade Commission have published orders showing fines and settlements with companies they accused of having inadequate cybersecurity practices. These orders demonstrate a trend to motivate companies, in particular boards of directors, to strengthen, closely monitor, implement, and ensure adherence to strong cybersecurity practices.

The CFPB issued a $100,000 fine against an Iowa payment processor for making misrepresentations about its cybersecurity policies *In the Matter of Dwolla, Inc*. *See* Consent Order here. The misrepresentations included fairly typical disclosures made on company websites about cybersecurity, including that (1) transactions on the company's website were “safe” and secure;” (2) the company's website empowered “anyone with an internet connection to **safely** send money to friends or businesses;” (3) the company's data security practices “exceeded industry standards;” (4) the company encrypted information “utilizing the same standards required by the federal government;” (5) the company encrypted all consumer information, which was “securely encrypted and stored;” and (6) the company was “PCI compliant.” Although Dwolla did not suffer any reported cyber attacks (e.g., a data breach), the CFPB fined Dwolla because it found that these representations were false. Dwolla did not encrypt all of its customers' sensitive information, was not PCI compliant, and failed to “adopt and implement data-security policies and procedures reasonable and appropriate for the organization.” In addition to agreeing to pay the $100,000 fine, Dwolla's board of directors agreed to:

- Personally oversee the implementation of a cybersecurity program that included bi-annual cybersecurity “risk assessments;”
- Hold regular, mandatory cybersecurity training for all employees;
- Designate a qualified individual to oversee the company's cybersecurity program; and
- Manage outside vendors for compliance with the company's cybersecurity measures.

The SEC imposed a $100,000 fine on a broker-dealer *In the Matter of Craig Scott Capital, LLC (“CSC”), Craig S. Taddonio and Brent M. Porges*. *See* Cease and Desist Order here. The SEC determined that CSC failed

"to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records and information." The gist of CSC's wrongful conduct was the transfer of documents containing customer information, including instances where the company's co-founders and officers used their personal email accounts to transfer customer information. The SEC fined two officers $25,000 each, and censured them as well as the company. Notably, there were no allegations that the company suffered any cyber attacks, or that customer information had been otherwise compromised.

The FTC imposed a $250,000 fine on Henry Schein Practice Solution, Inc., a software company servicing dental practices. *See* Press Release here. The FTC alleged that Schein falsely claimed that its software "provided industry-standard encryption of sensitive patient information" in compliance with the Health Insurance Portability and Accountability Act (HIPAA). Although there were indications the software did not meet industry-standard encryption, there was no allegation of any cyber attacks leading to the loss or compromise of any patient data.

The key takeaways from these cases are:

1. **It is Open Season on Regulated Industries**: Companies operating in regulated industries, such as the financial and healthcare industries, should expect scrutiny of their cybersecurity practices even when they have not experienced a data breach. The risk of scrutiny is higher for companies that are required to make regular cybersecurity disclosures to government agencies.
2. **Walk Your Talk**: Companies should ensure not only that they have adequate cybersecurity practices that are compliant with industry or legal standards, but also that they are actually enforcing and practicing what they are advertising. Some companies recently sanctioned by government agencies had misrepresented that their policies were better than required.
3. **Regularly Assess Your Cyber Hygiene**: Companies should frequently conduct cybersecurity assessments, preferably by qualified outside professionals, and follow through with addressing vulnerabilities discovered during these assessments. Government agencies are relying on failures to address vulnerabilities identified in prior assessments, at least in part, to impose sanctions.

---

questions as to the application of the law to your activities, you should seek the advice of your legal counsel.