PUBLICATION

CFPB Issues Fines and Penalties Against Financial Institutions for Misleading Marketing Materials

March 07, 2016

The Consumer Financial Protection Bureau (CFPB) recently issued a first of its kind Consent Order against an online payment platform for misrepresenting the security measures used to protect consumer's data. Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the CFPB may take action against financial institutions for deceptive acts. While the fines imposed may not put a dent in a company's overall bottom line, the conduct and reporting obligations are substantial. The CFPB's recent action should make all financial institutions take notice, as an actual data breach may not be required before government agencies take action.

On March 2, 2016, the CFPB announced a $100,000 fine against an online payment platform, Dwolla, Inc., for "deceptive acts and practices relating to false representations regarding [Dwolla's] data-security practices." The CFPB determined that Dwolla's security practices did not "exceed industry standards" as advertised, nor did it store data "in a bank-level hosting and security environment." According to the CFPB, Dwolla "did not adopt or implement reasonable and appropriate data-security policies and procedures governing the collection, maintenance, or storage of consumers' personal information," nor did it adopt or implement a written data-security plan. Regular risk assessments were not conducted and Dwolla's employees received insufficient data-security training. Dwolla also operated a software development operation that failed to comply with Dwolla's own documented security practices.

As a result, Dwolla must now comply with a host of detailed conduct requirements regarding the adoption and implementation of its data-security measures. It must retain an independent auditor to perform an initial audit within six months, conduct annual risk assessments to validate the performance assessments Dwolla must conduct, and review Dwolla's overall compliance with the Consent Order. Compliance reports must also be submitted to CFPB and copies of Dwolla's compliance-related records must be maintained for at least five years. Further, the Board of Directors must review all submissions required by the Consent Order. As for its reporting requirements, Dwolla must inform CFPB of any developments that could affect compliance with the Consent Order and provide progress reports after 90 days and one year. Additional compliance reports are due 30 days after request is made by the CFPB.

The CFPB action is strikingly similar to recent actions taken by the Federal Trade Commission (FTC). The FTC also recently announced that it entered into a consent agreement with Henry Schein Practice Solutions, a leading dental office management software provider, to resolve allegations that Schein's marketing claims regarding security practices to dentists violated § 5 of the FTC Act. The FTC took issue with Schein's claims that its software provided industry-standard encryption of sensitive patient information. The FTC also accused Schein of misleading dental practices into believing that it met regulatory requirements for protecting patients' information. According to the agreement and consent order, Schein must pay a $250,000 fine and is prohibited from misrepresenting its level of encryption, its ability to satisfy customers' privacy or security-related regulatory obligations, or the extent of the security protections implemented. Schein must also disclose to customers that its software does not meet the industry recommended standard for encryption. The consent order, if made final by FTC after public comment, remains in effect for 20 years.

The Takeaway. Financial institutions have long been attuned to their obligations with regard to data-security under the Gramm Leach Bliley Act (GLB). These recent actions remind financial institutions of the CFPB's jurisdiction over GLB since Dodd-Frank; specifically, that their data-security practices and related marketing claims are subject to scrutiny by the CFPB. Although the FTC does not have specific consumer protection jurisdiction over financial institutions, its long history of enforcement over companies in the data-security arena may serve as a guide to the CFPB or serve as a basis for its own action.

The CFPB has the jurisdiction to regulate financial institutions' data-security practices and has demonstrated its willingness to do so. Although the fines imposed are not shocking in terms of their face value, the obligations imposed in the consent order, and the negative publicity associated with such settlements, demands attention. The CFPB is now proactively taking measures to protect the public from data breaches, before any actual harm may be suffered by the end consumer. Given the CFPB's focus on protecting consumers, it is not surprising that marketing materials are proving to be a target-rich environment.

Compliance and information security officers need to be sure that they have appropriate and robust policies and procedures in place, including regular audit procedures, to ensure that they can substantiate claims made regarding the strength of their data-security measures. Most importantly, these obligations are continual and should be routinely validated as part of an ongoing information security program. Financial institutions should also be leery of simply relying on data-security representations made by third-party vendors without some measure of objective diligence that supports the vendors' claims. At a minimum, financial institutions should consider obtaining strong contractual indemnification from the vendors if their claims turn out to be misrepresented.

If you have questions regarding data-security issues facing financial institutions, please contact the author of this alert, your regular Baker Donelson attorney, or any members of the Firm's Privacy and Information Security Team or Financial Services Team.