WINSTON & STRAWN LLP

BLOG

U.S. Consumer Financial Protection Bureau Announces Its First Privacy Settlement

MARCH 15, 2016

The U.S. Consumer Financial Protection Bureau (CFPB) – which enforces privacy for those entities covered under the Consumer Financial Protection Act of 2010 – recently announced its first consent order. The order was entered into with Dwolla, Inc., a digital payment platform that permits real-time bank transfers (and collects sensitive personal information like social security numbers as part of the provision of its services).

According to the CFPB, Dwolla falsely represented its data security practices in violation of Sections 1031(a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§ 5531(a), 5536(a)(1), and that those false statements were material because people would rely on them when making decisions to use Dwolla's services. According to the consent order, Dwolla represented to consumers that its network and transactions were "safe" and "secure," including claims that its data security practices met or exceeded industry standard; all information was securely encrypted and stored; and its transactions, servers, and data centers were compliant with PCI Security Standards Council standards. However, the consent order noted that Dwolla's security measures were not "reasonable or appropriate" (it had no written data security plan); Dwolla did not conduct regular risk assessments; the company did not train employees on security; failed to encrypt sensitive data even though industry standards said such information should be encrypted; and did not enforce compliance of its own security policies on its software development branch.

The consent order requires payment of a civil money penalty of $100,000 to the CFPB. The order also requires Dwolla to stop misrepresenting its data security practices; adopt and implement reasonable and appropriate data-security measures; enact a written data security plan; designate a qualified person to be accountable for the data-security program; conduct risk assessments twice a year; and conduct regular, mandatory employee training on its data security policies and procedures; develop an appropriate method of customer identity authentication at the registration phase; and obtain an annual data security audit from an independent third party. The order outlines, interestingly, the role the Dwolla Board should play, namely making sure that the company is managed properly and soundly, complies with the Consent Order, and "Federal consumer financial law."

TIP: This first case from the CFPB demonstrates that the agency, like the FTC, is focusing on false representations about data security practices. Companies making statements about their security measures should thus ensure that they have substantiation to back up their statements. This case also suggests that the

CFPB believes that companies should live up to industry standards when developing their data protection practices.

2 Min Read

Related Locations

Chicago

Related Topics

Financial Privacy

Data Breach

Related Capabilities

Privacy & Data Security

Financial Services

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.