

CFPB Brings First Enforcement Action for False and Misleading Statements on Data Security

By Kit Addleman | March 14, 2016

RELATED PRACTICES Privacy and Cybersecurity, Litigation

The Consumer Financial Protection Bureau (“**CFPB**”) recently announced a settlement with Dwolla, Inc., an online payment processor, for allegedly deceptive statements Dwolla made to consumers regarding the company’s data security practices. In the settlement, Dwolla agreed to pay a \$100,000 penalty and take specific actions to improve its data security. Notably, the enforcement action was not precipitated by a data breach but was predicated solely on the company’s statements regarding the safety of its systems. The Dwolla settlement marks the first enforcement action by the CFPB in the data security space and provides a cautionary lesson for those under CFPB authority.

As described in the CFPB’s consent order, Dwolla operates an online payment network with more than 650,000 members who transfer up to \$5 million per day. Users can register as a member on Dwolla’s website by providing a name, address, date of birth, telephone number, and social security number. Once registered, Dwolla members can link a personal bank account to their Dwolla accounts, which allows them to transfer funds through Dwolla to other members or merchants registered on the network.

The consent order resolving the CFPB’s action against Dwolla states that, from January 2011 to March 2014, Dwolla made the following representations to consumers regarding data security:

- The Dwolla network and Dwolla transactions were “safe” and “secure.”
- Dwolla transactions were “safer [than credit cards] and less of a liability for both consumers and merchants.”
- All information stored by Dwolla was “securely encrypted” and stored “in a bank-level hosting and security environment.”
- Dwolla was “PCI compliant” (referring to the data security compliance standards adopted in the payment card industry).

The CFPB alleged that these representations were inaccurate and made the following findings in the consent order:

- Dwolla failed to adopt or implement “reasonable and appropriate data-security policies and procedures” governing the storage of consumers’ personal information until September 2012 and did not adopt written policies and procedures until October 2013.
- Dwolla failed to conduct “adequate” and “regular” risk assessments until mid-2014.
- Dwolla failed to provide appropriate data security training to its employees.
- Dwolla stored and transmitted unencrypted personal information belonging to consumers and encouraged consumers to send sensitive personal information via email to expedite the registration process.

The CFPB found that Dwolla's allegedly false representations to consumers regarding its data security practices constituted "deceptive acts and practices" under Section 1036(a)(1) of the Consumer Financial Protection Act. To settle the charges, Dwolla agreed to pay a \$100,000 penalty and to take a number of actions to enhance its data security practices including:

- Establishing a written and comprehensive data security plan to protect consumer data;
- Designating an employee to coordinate the company's data security program; and
- Conducting regular risk assessments, employee training, and data security audits.

In light of this action, companies that provide consumer financial products and services, as well as service providers to those companies, would be well-advised to carefully examine their own data security practices and the public disclosures surrounding data security. In light of the enhanced focus on data security by a variety of federal regulators (including the FTC and the FCC, which just released proposed data security rules for Internet service providers), any business entity handling consumer data should maintain written data security policies and procedures that, at a minimum, satisfy the requirements established by the Dwolla consent order. Doing so may not only help companies to prevent, mitigate and detect data breach incidents but may also help them avoid unwanted regulatory scrutiny.

For additional information on CFPB enforcement matters or government enforcement actions involving data security disclosures, please contact one of the Haynes Boone lawyers listed below.