CARLTON FIELDS

CFPB Enters First Enforcement Order Related to Data Security

March 04, 2016

On March 2, the Consumer Financial Protection Bureau (CFPB) brought its first enforcement order related to data security. The order, against online payment platform service provider Dwolla, Inc. (Dwolla), charges that Dwolla misrepresented its data security practices and the safety of its system to consumers, in violation of the Consumer Financial Protection Act (CFPA)'s prohibition against unfair, deceptive and abusive practices (UDAAP). The company has been ordered to pay a $100,000 penalty to the CFPB and to fix its security practices. Dwolla launched its online payment system and services in Iowa in December 2009 and nationally a year later. The company collects and stores consumers' sensitive personal information, while providing a platform for online financial transactions. As of May 2015, Dwolla had more than 650,000 users and had transferred as much as $5 million per day. For each account, Dwolla collects personal information including the consumer's name, address, date of birth, telephone number, Social Security number, bank account and routing numbers, a password, and a unique four-digit PIN. The CFPB found that from 2010 to 2014, Dwolla represented on its website and in communications with consumers, that its network and transactions were "safe" and "secure" and claimed its data security practices exceeded industry standards. However, the CFPB found Dwolla's data security practices fell far short of its claims. Among other issues, the CFPB found

Dwolla misrepresented:

- **That it employed "reasonable and appropriate measures to protect data obtained from consumers."** Dwolla did not: (1) adopt or implement data security policies and procedures governing the collection, maintenance, and storage of consumers' personal information until September 2012; (2) adopt a written data security plan until October 2013; or (3) conduct its first comprehensive risk assessment until mid-2014. Moreover, Dwolla operated a software development operation (Dwollalabs) that did not comply with the security practices Dwolla had implemented. It released applications through Dwollalabs without conducting risk assessments or penetration tests.
- **That "100%" of its consumers' information was "encrypted and stored securely."** In numerous instances, Dwolla did not encrypt sensitive consumer personal information such as: Social Security numbers, bank account information, first and last names, mailing addresses, Dwolla four-digit PINS, and digital images of driver's licenses, Social Security cards, and utility bills.
- **That its data security practices "exceed" or "surpass" industry security standards.** For more than one year and a half, Dwolla failed to address the results of a December 2012 penetration test. In that test, a phishing email attack was distributed to Dwolla's employees that contained a suspicious URL link. Nearly half of Dwolla's employees opened the email, and of those, 62 percent clicked on the URL link. Of those that clicked on the URL link, 25 percent further attempted to register on the phishing site and provided a username and password. Despite this knowledge, Dwolla did not conduct its first mandatory employee data security training until mid-2014.
- **That its transactions, servers and data centers were "safer than credit cards and "PCI compliant."** The Payment Card Industry (PCI) Security Standards Council is a global forum that issues data security compliance standards for cardholder data adopted by some of the world's largest payment card networks (e.g. American Express, MasterCard and Visa). Contrary to its claims, Dwolla's transactions, servers and data centers were not PCI compliant.

In other words, Dwolla failed to: (a) adopt and implement data security policies and procedures reasonable and appropriate for the organization; (b) use appropriate measures to identify reasonably foreseeable security risks; (c) ensure that employees who have access to or handle customer information received adequate training and guidance about security risks; (d) use encryption technologies to properly safeguard sensitive consumer information; and (e) practice secure software development. The CFPB determined Dwolla's false representations regarding its data security practices were material because they were likely to affect a consumer's choice to become a member of the network. In addition to the civil penalty, pursuant to its authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB ordered Dwolla to:

- Stop misrepresenting its data security practices;
- Enact a written, comprehensive data security plan;

- Adopt and implement reasonable and appropriate data security measures to protect consumers' personal information;
- Designate a qualified person to coordinate and be accountable for its data security program;
- Conduct data security risk assessments twice annually and adjust the data security program in light of the results of the risk assessments ;
- Conduct regular, mandatory employee training on data security; the safe-handling of consumers' private information; and secure software design, development and testing;
- Develop, implement and update security patches to fix any security vulnerabilities identified in any web or mobile application;
- Develop, implement, and maintain an appropriate method of consumer identity authentication at the registration phase and before effecting a funds transfer;
- Develop, implement and maintain reasonable procedures for the selection and retention of service providers capable of maintaining security practices consistent with the consent order;
- Within 10 days, identify a qualified, independent person (acceptable to the Enforcement Director) to conduct an annual data security audit.

Dwolla consented to the issuance of the order without admitting or denying the CFPB's findings of fact or conclusions of law. In announcing the consent order, CFPB Director Richard Cordray said, "With data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." The $100,000 penalty paid by Dwolla will be deposited in the CFPB's Civil Penalty Fund.

Related Practices

Consumer Finance
Cybersecurity and Privacy