# EXPERT COMMENTARY

## CFPB Issues First Data Security Action

by Melissa J. Krasnow
Partner, Dorsey & Whitney LLP

**March 2016**

**The Consumer Financial Protection Bureau (CFPB) issued its first data security enforcement action against online payment platform Dwolla, a Delaware corporation. Of particular note, the consent order describes requirements for Dwolla's board of directors in addition to data security measures that Dwolla must take.**

The Consent Order can be found here: In the Matter of Dwolla, Inc., File No 2016-CFPB-0007.

### CFPB Findings about Dwolla's Deceptive Representations

Dwolla had directly or indirectly represented to consumers on its website or in direct communications with consumers that it employed reasonable and appropriate measures to protect data obtained from consumers from unauthorized access, and that its data security practices met or exceeded industry standards. Dwolla also made representations regarding its encryption and data security measures including, without limitation, that it was "PCI compliant."

The Consumer Financial Protection Bureau (CFPB) found that Dwolla's representations regarding its data security practices were (a) likely to mislead a reasonable consumer into believing that Dwolla had incorporated reasonable and appropriate data security practices when it had not and (b) material because they were likely to affect a consumer's choice or conduct regarding whether to become a member of Dwolla's network. Further, Dwolla's practices constituted deceptive acts or practices in violation of the Consumer Financial Protection Act of 2010.

### Data Security Measures That Dwolla Must Take

In addition to paying a civil money penalty of $100,000 to the CFPB, the CFPB consent order requires that Dwolla not misrepresent, expressly or by implication, the data security practices it implements, including regarding data storage or encryption practices, PCI compliance, or adherence to any relevant data-security standard or best practices. Dwolla also must take measures to improve the safety and security of its operations and



Learn How To Get Access Get Answers Get Ahead with IRMI
IRMI.com
©2016 IRMI®

the consumer information that is stored on, or transmitted through, its network(s), as follows.

- Establish, implement, and maintain a written, comprehensive data security plan (a) that is reasonably designed to protect the confidentiality, integrity, and availability of sensitive consumer information and (b) that must contain administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of Dwolla's activities, and the sensitivity of the personal information collected about consumers.

- Adopt and implement reasonable and appropriate data security policies and procedures.

- Designate a qualified person to coordinate and be accountable for the data security program.

- Conduct data security risk assessments twice annually of each area of relevant operation (a) to identify internal and external risks (1) to the security, confidentiality, and integrity of Dwolla's network, systems, or apps and (2) to its stored consumers' sensitive consumer information; and (b) to assess the sufficiency of any safeguards in place to control these risks.

- Evaluate and adjust the data security program in light of the results of the risk assessments and monitoring required by the consent order.

- Conduct regular, mandatory employee training on Dwolla's data security policies and procedures; the safe handling of consumers' sensitive personal information; and secure software design, development, and testing.

- Develop, implement, and update, as required, security patches to fix any security vulnerabilities identified in any web or mobile application.

- Develop, implement, and maintain an appropriate method of customer 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, and require service providers by contract to implement and maintain appropriate safeguards.

- Obtain an annual data security audit from an independent, qualified third party, using procedures and standards generally accepted in the profession.

## Annual Data Security Audit

Dwolla must retain one or more qualified, independent person(s) with specialized experience in data security who is acceptable to the CFPB to conduct an annual data security audit of its data security practices (a) to validate the effectiveness of periodic risk assessments in identifying any internal or external risks to the security, confidentiality, and integrity of the sensitive consumer information and (b) to verify that Dwolla has implemented reasonable and appropriate risk mitigation activities to sufficiently safeguard against any identified risks.

The data security audit must include a review of Dwolla's compliance with the data security measures required by the CFPB consent order. The qualified person(s) must prepare a written report detailing the findings of the audit and provide the audit report to Dwolla's Board of Directors.



Get Access Get Answers Get Ahead with IRMI
IRMI.com
©2016 IRMI®

## Board Requirements

According to the CFPB, "… [Dwolla's] Board will have the ultimate responsibility for proper and sound management of [Dwolla] and for ensuring that it complies with Federal consumer financial law and this consent order." After receiving the audit report, Dwolla's Board must develop a compliance plan to correct any deficiencies identified, implement any recommendations or explain in writing why a particular recommendation is not being implemented, and submit the audit report and the compliance plan to the CFPB. Dwolla's Board must make any revisions to the compliance plan directed by the CFPB and resubmit the compliance plan to the CFPB.

In addition, Dwolla's Board must review all submissions (including plans, reports, programs, policies, and procedures) required by the consent order before submission to the CFPB. Dwolla's Board must do the following.

- Authorize whatever actions are necessary for Dwolla to fully comply with the consent order.
- Require timely reporting by management to the Board on the status of compliance obligations.
- Require timely and appropriate corrective action to remedy any material noncompliance with any failures to comply with board directives.

The consent order also describes certain reporting, order distribution and acknowledgement, recordkeeping, notice, and compliance-monitoring requirements.

As part of the reporting requirements, Dwolla must submit to the CFPB on an annual basis an accurate, written compliance progress report that has been approved by the Board that, at a minimum, describes in detail the manner and form in which Dwolla has complied with the consent order and attach a copy of each order acknowledgement.

* * *

**Melissa J. Krasnow**
Partner, Dorsey & Whitney LLP
50 South Sixth Street, Suite 1500
Minneapolis, MN 55402
Phone: (612) 492–6106
Fax: (612) 340–2868
krasnow.melissa@dorsey.com
www.dorsey.com

Melissa Krasnow writes on cyber and privacy risk and insurance issues for IRMI.com.

Ms. Krasnow is a partner in the Minneapolis office of Dorsey & Whitney LLP, whose practice encompasses domestic and cross-border privacy matters and transactions, including:

- Commercial and technology transactions (e.g., outsourcing) and mergers and acquisitions
- Data breaches and crisis situations, including preparation (e.g., tabletop exercises)
- Advice to boards of directors and senior executives (e.g., privacy and security)
- State, federal, and international privacy, advertising and marketing, securities, corporate governance and compliance, and regulated industry laws (e.g., financial services) and standards (e.g., PCI DSS)
- Privacy, security, mobile, text message, social media, corporate and technology policies, programs, and agreements
- Cyberliability insurance policy and SEC disclosure review

She serves as cyberliability insurance panel counsel with a leading international insurance organization and their insureds.

Ms. Krasnow serves as an Advisory Board member for the Bloomberg BNA Privacy & Security Law Report and the International Association of Privacy Professionals.



Get Access Get Answers Get Ahead with IRMI
IRMI.com
©2016 IRMI®

She also is a Certified Information Privacy Professional/US (CIPP/US) and a board leadership fellow of the National Association of Corporate Directors.

Ms. Krasnow holds a bachelor of arts degree in Chinese studies and political science from Wellesley College and a juris doctor from Northwestern University School of Law. She also attended the University of British Columbia.

Opinions expressed in Expert Commentary articles are those of the author and are not necessarily held by the author's employer or IRMI. Expert Commentary articles and other IRMI Online content do not purport to provide legal, accounting, or other professional advice or opinion. If such advice is needed, consult with your attorney, accountant, or other qualified adviser.



©2016 IRMI®