Published on *The National Law Review* https://natlawreview.com

Dwolla Fined $100,000 by CFPB in First Data Security Enforcement Action

Article By:

Christopher E. Hoyme

The Consumer Financial Protection Bureau ("CFPB") gave the fintech online payment sector a "wake up call" with an enforcement action against a Des Moines start up digital payment provider, Dwolla, Inc. ("Dwolla").

The CFPB alleged that Dwolla misrepresented how it was protecting consumers' data. Dwolla entered into a Consent Order to settle the CFPB charges and agreed to pay a $100,000 penalty and to change and improve its current security practices. The CFPB never alleged that Dwolla had breached any consumer data. According to the CFPB, Dwolla "failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access," while telling consumers that the information was "securely encrypted and stored." Dwolla, had over 650,000 customer accounts and was transferring as much as $5M a day in 2015.

In a nutshell, the CFPB alleged that Dwolla's representations regarding "securely encrypted and stored data," were inaccurate for a number of specific reasons including:

- Failing to implement appropriate data security policies and procedures until at least September 2012,
- Failing to implement a written data security plan until at least October 2013,
- Failing to conduct adequate risk assessments,
- Failing to use encryption technology to properly safeguard consumer information,
- Failing to provide adequate or mandatory employee training on data security, and
- Failing to practice secure software development for consumer facing applications

In addition to the fine, Dwolla agreed to take preventative steps to address security concerns including:

- Implementing a comprehensive data security plan,
- Conducting data security risk assessments twice annually,
- Designating a qualified individual to be accountable for data security issues,
- Implementing appropriate data security policies and procedures,
- Implementing an appropriate and precise method of customer identity authentication before any funds transfer,
- Adopting specific procedures for the selection and retention of service providers capable of maintaining security practices,
- Conducting regular and mandatory security data training, and
- Obtaining an annual data security audit from an independent, third party acceptable to CFPB's enforcement director.

The Consent Order will remain in effect for five (5) years.

This is the CFPB's first enforcement action directly related to data security and appears to expand the CFPB's jurisdiction into this arena. In the CFPB press release Director Richard Cordray stated, "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 informed consumers about their data security practices."

This virgin enforcement action by the CFPB appears to be a direct response to the growing concern about the lack of regulation for fintech digital payment firms. The enforcement action is also a welcome signal to traditional banks who have argued that the fintech sector has not received near the level of oversight or enforcement as they have. It appears regulators are attempting to find the right balance between acting too "heavy handed" and not squelching the technical advances that have made finance more convenient for consumers while still insuring an adequate level of consumer protection.

National Law Review, Volume VI, Number 68