Consumer Financial Protection Bureau

Press Release

CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices

MAR 02, 2016

Payment Processor Deceived Consumers About the Data Security Risks of Using Its Online System

WASHINGTON, D.C. – The Consumer Financial Protection Bureau today took action against online payment platform Dwolla for deceiving consumers about its data security practices and the safety of its online payment system. The CFPB ordered Dwolla to pay a $100,000 penalty and fix its security practices.

"Consumers entrust digital payment companies with significant amounts of sensitive personal information," said CFPB Director Richard Cordray. "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."

Dwolla, Inc., based in Des Moines, Iowa, operates an online payment system. Since December 2009, Dwolla has collected and stored consumers' sensitive personal information and provided a platform for financial transactions. As of May 2015, it 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 4-digit PIN.

From December 2010 until 2014, Dwolla claimed to protect consumer data from unauthorized access with "safe" and "secure" transactions. On its website and in communications with consumers, Dwolla claimed its data security practices exceeded industry standards and were Payment Card Industry Data Security

Standard compliant. They claimed also that they encrypted all sensitive personal information and that its mobile applications were safe and secure.

But rather than setting "a new precedent for the payments industry" as asserted, Dwolla's data security practices in fact fell far short of its claims. Such deception about security and security practices is illegal. Specifically, the CFPB found, among other issues, that Dwolla misrepresented its data-security practices by:

- **Falsely claiming its data security practices "exceed" or "surpass" industry security standards:** Contrary to its claims, Dwolla failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access.
- **Falsely claiming its "information is securely encrypted and stored":** Dwolla did not encrypt some sensitive consumer personal information, and released applications to the public before testing whether they were secure.

Enforcement Action

Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB is authorized to take action against institutions engaged in unfair, deceptive or abusive acts or practices, or that otherwise violate federal consumer financial laws. This is the Bureau's first data security action, and builds off advances made by several other agencies. Under the terms of the order, Dwolla is required to:

- **Stop misrepresenting its data security practices:** Dwolla must stop deceiving consumers about the security of its online payment system and enact comprehensive data security measures and policies, including a program of risk assessments and audits.
- **Train employees properly and fix security flaws:** Dwolla must train employees on the company's data security policies and procedures, and on how to protect consumers' sensitive personal information. Dwolla must also fix any security weaknesses found in its web and mobile applications, and securely store and transmit consumer data.
- **Pay a $100,000 civil money penalty:** Dwolla must pay a $100,000 penalty to the CFPB's Civil Penalty Fund.

The CFPB's order is found at:
http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf

###