Client Alert: Another Federal Regulator Steps Up Data Security Enforcement: CFPB Fines Online Payment Processor Dwolla for Lax Data Security

Related Professionals

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

Litigation and Appeals

CLIENT ALERT | 3.4.2016

On March 2nd, the Consumer Financial Protection Bureau (CFPB) announced a $100,000 penalty and settlement with online payment processor Dwolla, Inc. (Dwolla) for weak data security practices. Although Dwolla had not suffered a data breach, the CFPB found that Dwolla falsely advertised that customers' personal information was "safe" and "secure."[i] This is the CFPB's first action against a company for data security practices.

The action by the CFPB is consistent with and indicative of the overall regulatory focus on cybersecurity controls for all financial institutions.

False Statements

Dwolla, based in Des Moines, Iowa, is an online payment processor that collects and stores consumers' personal information in order to process financial transactions. The CFPB focused on statements made from January 2011 until March 2014 by Dwolla regarding its data security practices, claiming that these statements were false representations and therefore deceptive acts and practices in violation of Sections 1031 (a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010, 12 U.S.C. §§ 5531(a), 5536(a)(1).[ii] These false representations included:

- Claiming its network and transactions were "safe" and "secure;"
- Claiming its data security practices "exceed" or "surpass" industry security standards;
- Claiming "information is securely encrypted and stored;" and
- Stating it was "PCI compliant."[iii]

The CFPB found that Dwolla "failed to employ reasonable and appropriate" measures to protect consumer data from unauthorized access, that its data security practices did not surpass or exceed industry standards, that not all consumer data was encrypted at rest, and that its transactions, servers and data centers were not PCI compliant.[iv]

Data Security Mandates

In addition to the $100,000 penalty, the Order requires Dwolla to implement several data security measures, including that Dwolla would:

- Establish and maintain a comprehensive data security plan designed to protect consumer personal information that includes administrative, technical and physical safeguards;
- Adopt and implement reasonable data security policies and procedures;
- Conduct data-security risk assessments twice a year;
- Fix its security flaws and train employees about data security;
- Develop and maintain additional customer identity authentication at registration and before transferring funds;
- Obtain annual data-security audits from an independent third party; and
- Stop misrepresenting its data security practices.[v]

Board Requirements

The Order also places compliance responsibilities squarely on the Board of Director's shoulders. The Order requires Dwolla's Board of Directors to review all documentation demonstrating compliance with the Order's data security mandates and all other submissions required under the Consent Order prior to submission to the CFPB, and specifically states that the Board has "ultimate responsibility for proper and sound management" of Dwolla and for complying with the Order.[vi]

Crowded Space

The CFPB joins an already crowded field of data security regulators, including notably all of the federal financial institutions regulatory agencies. In addition to the Federal Trade Commission's long history of regulating data security representations and practices, the Federal Communications Commission levied nearly $26 million in fines related to data security practices last year,[vii] and the SEC recently fined an investment adviser $75,000 in connection with its practices that came to light from a data breach.[viii] The message from the regulators is clear: Companies must take their data security obligations seriously.

Contact Heather Enlow-Novitsky or your Vorys lawyer if you have questions about how to best stay ahead of the emerging regulatory framework over data security.

---

[i] Consent Order ¶ 15, In re Dwolla, Inc., File No. 2016-CFPB-007 (Feb. 27. 2016), available at http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

[ii] *Id.* at ¶ 51.

[iii] *Id.* at ¶¶ 16 - 20

[iv] *Id*. at ¶¶ 23- 26.

[v] *Id.* at ¶ 52

[vi] *Id.* at ¶¶ 60-61.

[vii] FCC Press Release: "AT&T to Pay $25M to Settle Investigation Into Three Data Breaches," https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0; FCC Press Release: "Cox Communications to Pay $595,000 to settle data breach investigation," https://www.fcc.gov/document/cox-communications-pay-595000-settle-data-breach-investigation-0.

[viii] Order, R.T. Jones Capital Equities Mgmt. Inc., No. 3-16827 (Sec. and Exch. Comm'n Sept. 22, 2015)