CFPB Brings First Ever Data Security Enforcement Action: Review and Analysis

March 9, 2016

On March 2, 2016, the CFPB announced that it had settled an enforcement action with Dwolla, Inc., an online payment platform, for making allegedly deceptive statements regarding its data security practices and the safety of its online payment system. Dwolla agreed to pay a $100,000 civil penalty and to undertake measures to improve its data security.

Key Takeaways

- **The CFPB Formally Enters the Data Security Enforcement Space.** The CFPB now joins the cacophony of regulatory agencies—including the FTC, the SEC, the FCC, and State Attorneys General—that have brought enforcement proceedings against companies related to their data security practices. The CFPB's interest in penalizing companies for allegedly deceptive data security representations suggests future enforcement activity in this area, particularly given that the CFPB brought this action without an alleged data breach. Companies subject to CFPB jurisdiction should consider themselves on notice to adopt the data security standards that the CFPB is likely to expect from the financial services industry, as further discussed below. The CFPB has asserted itself as a data security enforcement agency even though Title X of the Dodd-Frank Act expressly withholds authority from the CFPB to enforce the financial institutions safeguards rules under the Gramm-Leach-Bliley Act, unlike other financial sector regulators including the Federal Reserve System, the FDIC and the OCC.
- **The CFPB Duplicates an FTC Enforcement Theory.** Rather than relying on any direct regulatory authority over Dwolla's data security practices, the CFPB invoked its general authority to penalize regulated entities engaging in any unfair, deceptive, or abusive act or practice ("UDAAP"). The FTC has previously asserted claims under a similar theory in dozens of data security-related enforcement actions. Here, the CFPB's theory of liability was limited to the "deceptive" prong of its UDAAP authority, based on Dwolla's alleged misrepresentations to consumers. It remains to be seen whether the CFPB will also follow the FTC by invoking its UDAAP authority to penalize companies for employing "unreasonable" data security practices, even in the absence of any deceptive representations to consumers, by characterizing these practices as "unfair." The CFPB could prove to be a more formidable agency than the FTC in this space, given the CFPB's fining authority (which the FTC generally lacks) and the CFPB's more substantial consumer protection resources. While Dwolla's civil monetary penalty was modest, perhaps influenced by a lack of demonstrable consumer harm, future actions may involve a different order of magnitude.
- **The Consent Order Provides a Roadmap for Reasonable Data Security Practices.** Although the CFPB's enforcement theory was based on allegedly deceiving consumers, and not unreasonable data security practices *per se*, the Consent Order still provides useful guidance on best practices for companies. Based on the Consent Order, companies regulated by the CFPB should be prepared to demonstrate compliance with the CFPB's implicit guidance in each of the following areas:
    - **Data Security Policies and Procedures:** Companies should adopt and implement a written data security plan to govern the collection, maintenance and storage of consumers'

personal information. The plan and accompanying procedures should be appropriate for and commensurate with the company's size, sophistication and risk profile.

- **Risk Assessments:** Companies should conduct thorough, regular risk assessments to identify reasonably foreseeable risks to consumers' personal information and to assess the effectiveness of safeguards in place to control those risks. To the extent that risk assessments reveal vulnerabilities, those vulnerabilities should be addressed promptly.
- **Employee Training:** Companies should hold regular, mandatory employee training sessions on data security practices and test employees on their responses to hacking attempts. Poor testing results should prompt further training efforts.
- **Encryption**: Companies—or at least payment system companies—should encrypt sensitive personal data in storage and transmittal.
- **Testing Software:** Companies should run tests on any consumer-facing software applications to ensure that the applications adequately protect consumer data.

The Facts

Dwolla is an Iowa-based company that provides an online payment system and mobile payment network. Consumers can open a Dwolla account by submitting their name, address, date of birth, telephone number and Social Security number. After opening an account, consumers can link a bank account to their Dwolla account by submitting a bank account number and routing number. Consumers can then use their Dwolla account to transfer funds to another Dwolla account holder or a merchant. As of May 2015, Dwolla had approximately 653,000 members and had transferred as much as $5,000,000 per day.

According to the Consent Order, between January 2011 and March 2014, Dwolla made various representations to its consumers about the measures it took to ensure the security of consumers' sensitive personal information. Specifically, Dwolla represented to consumers that its network and transactions were safe and secure, that it employed reasonable and appropriate measures to protect consumer data, that it encrypted all sensitive information it possessed, that its data security practices surpassed industry standards, and that its transactions, servers and data centers were in compliance with the Payment Card Industry ("PCI") standards.

Notwithstanding these representations, Dwolla failed to employ reasonable and appropriate measures to protect consumer data from unauthorized access or comply with PCI standards. Dwolla did not implement data security policies and procedures governing the collection, maintenance or storage of consumers' personal information. Moreover, Dwolla failed to conduct regular risk assessments to identify risks and assess safeguards. Until December 2012, Dwolla employees did not receive training on handling and protecting consumers' personal information, and Dwolla did not conduct its first mandatory training for employees until mid-2014. In December 2012, a third-party auditor tested Dwolla's systems and found that employees were vulnerable to email phishing attacks, but Dwolla failed to address the auditor's findings in its employee training program.

To use Dwolla's services, consumers were required to provide sensitive personal information, but in many instances, information including names, addresses, Social Security numbers and bank account details was not encrypted, and was often solicited via email in clear text, leaving it susceptible to unauthorized access. In addition, Dwolla developed applications for consumers using an alternative software development operation known as "Dwollalabs" that was led by a software developer without data security training. The applications that Dwollalabs developed, which stored sensitive personal information, were made available to the public via Dwollalabs' website without prior security testing.

The CFPB did not allege that a data breach occurred or that any third party had improperly obtained any consumer's sensitive personal information.

CFPB Consent Order

The CFPB found that Dwolla committed deceptive acts and practices as a result of its alleged misrepresentations to consumers regarding its data security practices, in violation of Sections 1031(a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§5531(a), 5536(a)(1).

The Consent Order enjoined Dwolla from misrepresenting its data security practices, required Dwolla to implement improved and appropriate data security measures, and required Dwolla to develop policies and procedures to govern its data security practices. Dwolla was further required under the Consent Order to conduct regular risk assessments and independent audits, conduct mandatory employee training, and develop patches to cure existing security vulnerabilities. The Consent Order also imposed a civil money penalty of $100,000.

Dwolla consented to CFPB's Order without admitting or denying any of the findings of fact or conclusions of law.

Click on the following links to find the CFPB's **press release** and **Consent Order**.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Greg D. Andres	**212 450 4724**	**greg.andres@davispolk.com**
John L. Douglas	**202 962 7126**	**john.douglas@davispolk.com**
Joseph Kniaz	**202 962 7036**	**joseph.kniaz@davispolk.com**
Jon Leibowitz	**202 962 7050**	**jon.leibowitz@davispolk.com**
Neil H. MacBride	**202 962 7030**	**neil.macbride@davispolk.com**
Margaret E. Tahyar	**212 450 4379**	**margaret.tahyar@davispolk.com**