CFPB action sends warning signal to financial institutions

In March 2016, the US Consumer Financial Protection Bureau ('CFPB') brought its very first enforcement action related to data security against online payment system operator Dwolla, Inc. David A. Stein and Caleb Skeath, Of Counsel and Associate at Covington & Burling assess the impact of the action and its significance regarding the CFPB's enforcement remit.

When the US Congress established the CFPB in the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ('the Dodd-Frank Act'), it did not transfer jurisdiction over data security issues to the CFPB. Instead, it kept responsibility for data security regulation, guidance, and enforcement with the US regulators historically responsible for data security issues: the US Federal Trade Commission ('FTC') for non-banks, and the US federal bank regulatory agencies - the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency - for banking institutions and their holding companies. By bringing a data security enforcement action, the CFPB has blurred the line between consumer financial protection regulation and data security regulation.

The CFPB's jurisdiction

Even though the Dodd-Frank Act did not explicitly grant the CFPB jurisdiction over data security issues, Sections 1031(a) and 1036(a)(1) grant the CFPB the authority to prohibit deceptive acts or practices in connection with the offering of, or any transaction, with a consumer for a consumer financial product or service. Providing payment products and services to a consumer, which is Dwolla's business, constitutes a consumer financial product or service. The CFPB used these broad enforcement powers to enter into a consent order with Dwolla on 2 March 2016. In the consent order, the CFPB alleged that Dwolla deceived consumers about its data security practices and the safety of its online payment system.

Under US law, an act or practice is deceptive when:

1. The act or practice misleads or is likely to mislead the consumer;
2. The consumer's interpretation is reasonable under the circumstances; and
3. The misleading act or practice is material.

As explained in CFPB Bulletin 2013-07, the CFPB considers the totality of the circumstances in determining whether an act or practice has actually misled or is likely to mislead a consumer. Deceptive acts or practices can take the form of a representation or omission. To determine if the consumer's interpretation of the information was reasonable under the circumstances, the CFPB considers the communication from the perspective of a reasonable member of the target audience. Material information is information likely to affect a consumer's choice of, or conduct regarding, the product or service.

Dwolla

The CFPB alleged that, between January 2011 and March 2014, Dwolla made a number of false and misleading representations on its website and in direct communications with consumers. Firstly, the CFPB alleged that Dwolla represented that it employed 'reasonable and appropriate measures to protect data obtained from consumers from unauthorised access.'

Secondly, the CFPB alleged that Dwolla made a number of representations indicating that its data security practices met or exceeded industry standards. These representations included statements that the company 'sets a new precedent for the industry for safety and security,' stores consumer information 'in a bank-level hosting and security environment,' and encrypts data 'utilising the same standards required by the Federal Government.'

Thirdly, the CFPB alleged that Dwolla made a number of representations regarding its use of encryption and other data security measures. These representations included statements that '[a]ll information is securely encrypted and stored,' that the company encrypts 'all sensitive information that exists on its servers and data in transit and at rest,' and that Dwolla complied with the data security standards established by the Payment Card Industry ('PCI') Security Standards Council, a global forum that issues data security compliance standards for cardholder data adopted by some of the world's largest payment card networks.

The CFPB found these and similar representations were deceptive because Dwolla did not:

- Have data security practices that surpassed or exceeded industry standards;
- Encrypt all sensitive consumer information in its possession at rest;
- Conduct transactions or maintain servers and data centres in a manner that was PCI compliant;
- Adopt or implement reasonable and appropriate data security policies and procedures until at least September 2012;
- Adopt or implement a written data security plan to govern the collection, maintenance, or storage

of personal information until at least October 2013;
- Conduct adequate, regular risk assessments to identify reasonably foreseeable internal and external risks to consumers' personal information, or to assess the safeguards in place to control those risks;
- Use encryption technologies to properly safeguard sensitive consumer information, including names, addresses, Social Security Numbers, bank account information, digital images of driver's licenses, Social Security cards and utility bills, and Dwolla-issued PINs;
- Follow secure software development and testing practices for consumer-facing applications developed at an affiliated website, Dwollalabs; or
- Provide adequate or mandatory employee training on data security.

Consent order

Through the consent order, the CFPB ordered Dwolla to pay a $100,000 civil money penalty, although the CFPB made no finding of any data breach or other compromise of consumer data as a result of Dwolla's actions. The CFPB also ordered Dwolla to take substantial measures to fix its security practices, including:
- Establishing a written, comprehensive data security plan;
- Implementing reasonable and appropriate data security policies and procedures;
- Conducting data security risk assessments twice annually and evaluating and adjusting the data security programme in light of the results of the risk assessments;
- Designating a qualified person to coordinate and be accountable for the data security programme;
- Implementing and updating security patches to fix security vulnerabilities, as required;
- Developing and implementing an appropriate method of customer identity authentication at the registration and before effecting a funds transfer;
- Adopting reasonable procedures for the selection and retention of service providers capable of maintaining security practices consistent with the consent order;
- Conducting regular, mandatory employee data security training;
- Obtaining an annual data security audit from an independent and qualified third party, deemed acceptable by the CFPB's Enforcement Director; and
- Developing a compliance plan to address audit findings and recommendations, and providing the compliance plan and the audit report to the CFPB for non-objection by the Enforcement Director.

This is the first time the CFPB has brought a public enforcement action against a financial technology company engaged principally in developing payments innovations

The consent order, will remain in effect for a period of five years from the order's effective date.

The remediation ordered by the CFPB is significantly more prescriptive and burdensome than remediation imposed by other US regulators, particularly the FTC, in data security enforcement actions. By contrast, the CFPB consent order requires Dwolla to take very specific steps, such as implementing specific authentication measures and security patches, and includes a civil monetary penalty.

Conclusion

In the press release accompanying the consent order, CFPB Director Richard Cordray stated, "Consumers entrust digital payment companies with significant amounts of sensitive personal information [...] It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." Director Cordray's statement signals that the CFPB does not view the Dwolla action as an isolated case and that the CFPB may bring in the future additional enforcement actions involving data security.

In addition to blurring the line between data security and consumer financial protection regulation, this action also represents the first time the CFPB has brought a public enforcement action against a financial technology company engaged principally in developing payments innovations. Previously, the CFPB had, for the most part, taken a hands-off approach to financial technology payments firms. Combined with Director Cordray's remarks, this consent order should serve as a cautionary note to companies developing financial payments technology that they may find themselves in the CFPB's crosshairs if they do not pay close attention to representations they make regarding data security issues.

Finally, we note that Dwolla is a participating provider of digital wallet services through Pay.gov, the US Treasury Department's electronic payment portal for individuals, businesses, and states to make non-tax payments to the federal government. Even operating as a preferred provider of services to the US government did not protect Dwolla from the CFPB's enforcement. As a result of this action, the US Treasury and other US federal and state agencies may scrutinise emerging payment providers more closely for data security compliance both before accepting them as partners or service providers and after on-boarding them.

David A. Stein Of Counsel
Caleb Skeath Associate
Covington & Burling, Washington, D.C.
dstein@cov.com
cskeath@cov.com