March 4, 2016

The CFPB Enters the Cybersecurity Arena with Its First Enforcement Action

Future Activity Against Banks and Other Companies Likely

On March 2, 2016, the Consumer Financial Protection Bureau ("CFPB" or the "Bureau") entered an enforcement order against online payment platform Dwolla, Inc. for deceiving consumers about its data security practices and the safety of its online payment system.[1] Under the terms of the consent order, Dwolla is required to, among other things: (1) stop misrepresenting its data security practices, (2) train employees and improve data security practices across a number of areas, and (3) pay a $100,000 civil penalty. Notably, although there was no allegation of a data breach or data leak, the CFPB imposed relatively intrusive remedial requirements given the size of the company, including requiring it to retain an independent expert to conduct data-security audits annually for five years.

As the CFPB acknowledged, this was its first data security enforcement action, and it likely marks the beginning of a line of CFPB supervisory and enforcement actions in the cybersecurity arena. The CFPB relied on its authority to enforce Dodd-Frank's prohibition against "unfair, deceptive, or abusive acts or practices" (its "UDAAP" authority)[2] in connection with consumer financial products and services, relying in this case on a deception theory. The agency's enforcement jurisdiction covers large banks and an array of non-bank companies that offer consumer financial products and services, including (based on prior CFPB actions) companies as diverse as wireless carriers, for-profit schools, and certain retailers.

Below, we review the key features of the Dwolla action, discuss potential future CFPB activity in this area, and outline some practical lessons for general counsel, working in coordination with IT, compliance, and business colleagues.

The Dwolla Enforcement Action

According to the CFPB consent order (in which Dwolla did not admit or deny liability), Dwolla provides consumers with a platform for making payments using the company's website and mobile applications. As of May 2015, it had more than 650,000 users and transferred as much as $5 million per day. For each account, Dwolla collects personal information including the consumer's name, address, date of birth,

[1] The CFPB press release announcing this action can be found here, and the consent order can be found here.

[2] *See* 12 U.S.C. §§ 5563, 5565.

telephone number, Social Security number, bank account and routing numbers, a password, and a unique 4-digit PIN. As a payment processor, Dwolla is a "covered person" under Title X of the Dodd-Frank Act.[3]

In finding that Dwolla engaged in deceptive acts, the CFPB noted the following representations (among others) made by Dwolla on its website and in personal communications with consumers:

- Dwolla's data security practices "exceed industry standards," or "surpass industry security standards";
- "100% of your info is encrypted and stored securely";
- Dwolla encrypts "all sensitive information that exists on its servers";
- Dwolla "encrypt[s] data in transit and at rest";
- "Dwolla's website, mobile applications, connection to financial institutions, back end, and even APIs use the latest encryption and secure connections"; and
- Dwolla is "PCI compliant."[4]

The CFPB found that Dwolla fell short of these claims in a number of ways, and that such claims were material to consumers because they were likely to affect a consumer's choice or conduct regarding whether to join Dwolla's network. Among other things, the CFPB found that Dwolla failed to:

- Adopt and implement data security policies and procedures reasonable and appropriate for the organization;
- Conduct 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;[5]
- Train employees who have access to or handle consumer information about security risks;[6]
- Use encryption technologies to properly safeguard sensitive consumer information;[7] and

[3] *See* 12 U.S.C. § 5481(6).

[4] The Payment Card Industry (PCI) Security Standards Council is an open global forum that issues the data security compliance standards for cardholder data adopted by some of the world's largest payment card networks.

[5] According to the consent order, Dwolla did not conduct its first comprehensive risk assessment until mid-2014.

[6] In December 2012, Dwolla allegedly failed to address the results of a phishing attack test. The test revealed that nearly half of the employees opened the email, and, of those, 62% clicked on the link.

- Test the security of the apps on Dwollalabs.com to ensure that consumers' sensitive information was protected before the apps' public release.

Notably, the consent order did not allege that there was a data breach or data leak or that any consumer was harmed (beyond purchasing the service in potential reliance on these claims).

The CFPB's consent order requires Dwolla to refrain from making misrepresentations, both expressly or impliedly, regarding its data security practices, and to pay a $100,000 civil penalty. The consent order, which lasts 5 years unless extended in the event of a violation, also requires that Dwolla take a long list of actions, including:

Data Security Policies and Procedures

- Develop and maintain a written, comprehensive data security plan that is reasonably designed to protect the confidentiality, integrity, and availability of sensitive consumer information;[8]
- Assess data security risks and the sufficiency of safeguards twice a year in areas relating to confidentiality, integrity of Dwolla's network, systems, or apps, and consumers' sensitive information;
- Develop and maintain an appropriate method of customer identity authentication;
- Develop and update, as required, security patches to fix any security vulnerabilities;

Personnel and Training

- Designate a qualified person to coordinate and be accountable for the data security program;
- Conduct regular, mandatory employee training on data security policies and procedures, handling consumers' information, and secure software design, development, and testing;

Audit, Compliance, Reporting & Recordkeeping

- Within 30 days, retain an independent person, with specialized experience in data security and acceptable to the CFPB's Enforcement Director, to conduct a data-security audit and issue an audit report within 180 days, and annually thereafter for the five-year term of the consent order;

---

[7] According to the consent order, Dwolla encouraged consumers to submit sensitive information, like Social Security numbers and scans of passports, by email in order to expedite the registration process.

[8] The plans must contain administrative, technical, and physical safeguards appropriate to Dwolla's size and complexity, the nature and scope of Dwolla's activities, and the sensitivity of the personal information collected about consumers.

- Within 30 days of receiving the audit report, the Board must develop a plan to correct deficiencies and implement any recommendations and submit the plan to the CFPB Enforcement Director, who may require revisions; and

- Create and retain records of policies, procedures, and compliance with the consent order for at least 5 years.

IMPLICATIONS

With this first CFPB enforcement action in the cybersecurity arena, the following are some areas to watch:

1. **The CFPB's cybersecurity activity may extend across the full range of its jurisdiction:** The Dwolla action signals the CFPB's willingness to take action on data security across the range of entities for which it has enforcement authority, including banks with more than $10B in assets and their affiliates, and the full range of non-bank consumer financial companies, such as mortgage lenders, credit card networks, payday lenders, debt collectors, student loan services, and auto finance companies. The CFPB has also taken enforcement action against wireless carriers, for-profit schools, and furniture and electronics retailers based on the financial products or services they offer, and presumably the CFPB believes that it could pursue data protection cases against those entities as well. While there are strong reasons that the banking regulators should have principal responsibility for cybersecurity with respect to banks, time will tell how active the CFPB decides to be in this area.

2. **For non-banks, the CFPB has stronger tools than the FTC:** While the Federal Trade Commission (FTC) has been active in pursuing cybersecurity enforcement cases, it does not have jurisdiction over banks. The FTC and CFPB share enforcement jurisdiction over almost all non-bank companies that provide consumer financial products and services (and FTC's jurisdiction sweeps more broadly to non-financial companies).[9] In the area of overlap, however, the CFPB has some notable advantages, including that it can pursue civil monetary penalties for UDAAP violations in court and administrative proceedings; it has the authority to send examiners into many of these companies, which entails an enhanced ability to identify data security issues; and it can potentially use its authority under the "abusive" prong of UDAAP in this area.

3. **The CFPB may incentivize more aggressive banking regulator activity in the cyber arena:** Not wanting to be outdone by the CFPB, federal banking regulators in recent years have stepped up their consumer protection activity, including by pursuing higher penalties. There is

[9] Because of their concurrent authority, the Dodd-Frank Act requires the CFPB and FTC to negotiate an agreement to coordinate their enforcement actions in connection with consumer financial products or services. 12 U.S.C. § 5514(c)(3). *See* Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission (Jan. 20, 2012), *available at* http://www.ftc.gov/os/2012/01/120123ftc-cfpb-mou.pdf; renewed March 12, 2015.

an appreciable chance that the CFPB's entry into the cybersecurity arena will prompt banking regulators to take a more assertive enforcement approach, including by using their own UDAAP authority and/or proceeding on safety and soundness grounds.

4. **The CFPB will likely also use "unfairness" theories to regulate cyber practices**: While the Dwolla order was based on a deception theory, the CFPB could borrow again from FTC's playbook by using an "unfairness" theory in future cases. The FTC has pursued an unfairness theory of enforcement when "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[10] Presumably, an unfairness theory will tend to be used when a company engages in allegedly faulty data protection practices, but its representations are not so aggressive as to make for a plausible deception case. The FTC's use of unfairness to target data protection lapses was upheld by the Third Circuit in the *Wyndham* case,[11] although, recently, the FTC suffered a loss on a similar theory in front of an administrative law judge in the *LabMD* matter.[12]

5. **The CFPB could use its UDAAP rulemaking authority to regulate cybersecurity practices across all banks and non-bank consumer financial companies:** While the CFPB's examination and enforcement authority is limited, on the bank side, to the largest banks and their affiliates, its rulemaking authority, including under UDAAP, extends across all banks, in addition to virtually all non-bank consumer financial companies. The CFPB could presumably issue a rule that regulates data protection practices involving consumer financial products and services under both deception and unfairness theories. But because such rulemaking endeavors require large investments and are more easily subject to challenge in court, it is probable that the CFPB will focus on supervisory and enforcement actions in the cyber space for the time being.

PRACTICAL LESSONS

The general counsel of a bank or non-bank subject to the CFPB's authority may wish to consider the following, working with IT, compliance, and business units:

1. **Review representations regarding data security:** The CFPB will likely target companies with strong claims about their data security practices. These representations can be made on

[10] 15 U.S.C. § 45(n).

[11] *F.T.C.* v. *Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[12] *In the Matter of LabMD*, Dkt. No. 9357 (Complaint filed Aug 29, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. There, the ALJ dismissed the FTC complaint, finding that the FTC's regulation of unfair trade practices requires a showing that consumer harm was "probable," not just "possible." Initial Decision (filed Nov. 13, 2015). That decision is being appealed to the FTC, and could further be reviewed in federal court.

websites, in promotional material, and orally by call center personnel. Companies should review these statements to ensure that they are accurate and supportable.

2. **Strengthen cybersecurity practices:** Companies have many incentives to strengthen their cybersecurity practices, but the risk of CFPB enforcement is now an additional reason. In addition to moderating representations about the strength of their data security practices, companies should also strengthen those practices to match and exceed the representations made. As noted, even if representations are not an issue, the CFPB, like the FTC and the banking regulators, can nonetheless target allegedly faulty data practices on an unfairness theory. Among other sources, companies should look to the remedial actions that the CFPB required of Dwolla for guidance on how to strengthen their systems. Other useful sources include the FTC's "Start with Security: A Guide for Business," which is a compendium of lessons from FTC cyber cases.[13]

3. **Pay particular attention to policies and procedures:** Especially if they are subject to the CFPB's examination authority, companies should ensure that there are documented policies and procedures regarding cybersecurity and data protection, that employees are appropriately trained, and that there is a process in place for testing these procedures and updating them periodically. Companies should also make sure that consumer complaints involving data security are addressed and incorporated into process improvements where appropriate.

4. **Watch for further guidance from the CFPB:** We expect that the CFPB will incorporate additional material on data protection into its supervision manual, its periodic summaries of supervisory actions, and other guidance documents.

For an overview of other regulatory and enforcement activity in the cybersecurity area, see our firm's memorandum, "Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks," available here.

[13] That FTC publication is available here.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jack Baughman
212-373-3021
jbaughman@paulweiss.com

H. Christopher Boehning
212-373-3061
cboehning@paulweiss.com

Jay Cohen
212-373-3163
jaycohen@paulweiss.com

Michael E. Gertzman
212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
212-373-3316
bkarp@paulweiss.com

Mark F. Mendelsohn
202-223-7377
mmendelsohn@paulweiss.com

Lorin L. Reisner
212-373-3250
lreisner@paulweiss.com

Elizabeth M. Sacksteder
212-373-3505
esacksteder@paulweiss.com

Justin D. Lerer
212-373-3766
jlerer@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Associates Will Durbin and Yenisey Rodriguez contributed to this client memorandum.