ALERTS

CFPB Targets Online Payment Platform in First Enforcement Action on Cybersecurity

March 9, 2016

The Consumer Financial Protection Bureau ("CFPB") broke new ground last week with its Consent Order against Dwolla Inc. ("Dwolla"), an online payment platform, for deceiving consumers about its information security practices.[1]

The Consent Order alleges that Dwolla made public statements regarding the efficacy of its data security system and failed to fulfill those promises. The enforcement action is especially striking because the CFPB imposed a $100,000 civil monetary penalty on Dwolla despite the lack of any evidence that the payment processor experienced a data breach or any kind of cybersecurity incident, and also because the CFPB imposed significant — and expensive — new compliance obligations beyond what other federal regulators have demanded in similar situations. Most notably, the Consent Order provided that Dwolla must perform regular risk assessments and retain an independent third party to perform an annual cybersecurity audit for the next five years.

In effect, the Consent Order warns entities subject to CFPB regulation to give particular attention to any representations they make on a website or in direct communications with consumers regarding information security. Entities seeking to evaluate the accuracy of any such representations or to improve their own information security practices should take note of the CFPB's allegations as well as the corrective action that the CFPB imposed on Dwolla.

The CFPB's Allegations

The Consent Order alleges that Dwolla made materially deceptive statements to consumers when Dwolla represented, among other things, that it: (1) complied with the Data Security Standard promulgated by the Payment Card Industry ("PCI") Security Standards Council; (2) "encrypted and stored securely" "100%" of consumers' information and "all sensitive information that exists on its servers," including both "data in transit and at rest"; and (3) "exceed[ed] industry standards" for information security.[2]

According to the CFPB, Dwolla's transactions, servers and data centers were not, in fact, PCI compliant; Dwolla did not "encrypt all sensitive consumer information in its possession"; and Dwolla "failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access."[3] To the contrary,"[i]n numerous instances, [Dwolla] stored, transmitted, or caused to be transmitted … without encrypting … : "first and last names"; "mailing addresses"; "Dwolla 4-digit PINS"; "Social Security numbers"; "[b]ank account information"; and "digital images of driver's licenses, Social Security cards and utility bills."[4]

The CFPB also criticized Dwolla for failing to take action or educate its employees after they performed poorly in a penetration test that simulated an email phishing attack — that is, an attack in which employees were sent deceptive emails designed to trick them into clicking on a suspicious link.[5] In fact, the CFPB noted with disapproval that, although the penetration test was conducted in 2012, "Dwolla did not conduct its first mandatory employee data-security training until mid-2014."[6]

Interestingly, however, one thing the CFPB did not claim was that Dwolla's failure to maintain adequate data security measures to protect consumer information was an "unfair" practice.[7] Rather, the CFPB based its action entirely on Dwolla's alleged failure to keep its promises regarding information security.

The Remedy

The Consent Order restrains and enjoins Dwolla from making misrepresentations, both expressly or by implication, regarding its data security practices, including its encryption practices or PCI compliance,

and requires Dwolla to pay a $100,000 civil penalty. The Consent Order also imposes many other requirements on Dwolla, including that the company:

- Develop and maintain a written, comprehensive data security plan;
- Designate a qualified person to coordinate and be accountable for the data security program;
- Conduct data security risk assessments twice annually, and adjust the data security program in light of those assessments;
- "Conduct regular, mandatory employee training on a) the Company's data-security policies and procedures; b) the safe handling of consumers' sensitive personal information; and c) secure software design, development and testing";
- Develop, implement and maintain an appropriate method of customer identity authentication at the registration phase and before effecting a funds transfer; and
- "[O]btain an annual data-security audit for the five-year term of the Consent Order from an independent, qualified third-party, using procedures and standards generally accepted in the profession."[8]

The Order also provides that the third-party data security auditor be "acceptable to the CFPB's Enforcement Director."[9]

Implications and Analysis

"Deceptive" Acts, Not "Unfair" Acts. In announcing the Consent Order, the CFPB stated that the action "builds off advances made by several other agencies."[10] The CFPB's decision to confine this enforcement action to "deceptive" acts and practices is therefore notable given that the Federal Trade Commission ("FTC") has taken a markedly different approach. For example, in its action against Wyndham Worldwide Corporation, a hotel company, the FTC alleged that inadequate security practices exposing the payment information of consumers were "unfair" in violation of Section 5 of the Federal Trade Commission Act.[11] In its action against Dwolla, the CFPB attacked Dwolla's deceptive statements, rather than its cybersecurity practices directly, and declined to claim that the failure to maintain an adequate cybersecurity program is an "unfair" practice. However, given the CFPB's desire to "build off" other agencies'

"advances," it is possible the CFPB may attempt to do so in future actions, pursuant to its power to enforce the Dodd-Frank Act's prohibition against "unfair" and "abusive" practices.[12]

The Birth of the Required Outside Audit on Cybersecurity. Other federal agencies, such as the FTC and the Securities Exchange Commission, have been more active in cybersecurity enforcement to date, but in some respects, the CFPB order, which will last five years unless it is extended due to a violation by Dwolla, is more aggressive than actions these other federal regulators have taken. In addition to requiring that Dwolla pay a significant civil money penalty ($100,000), adopt a written data security plan and implement a mandatory employee training program, all of which are steps that have been required or advised by other regulators in enforcement actions[13] or general industry guidance,[14] the CFPB's Consent Order also ordered Dwolla to undertake semi-annual risk assessments, to retain an independent third party to perform an annual cybersecurity audit for the next five years, and to submit documents to the CFPB for the review or non-objection of the enforcement director. These demands exceed the requirements of the PCI Data Security Standard,[15] as well as the requirements of any federal privacy regime.

The CFPB as Interpreter of PCI Standards. To be sure, it was Dwolla's misrepresentations, not its noncompliance with the PCI Data Security Standard per se, that the CFPB attacked. Examining compliance with the PCI Data Security Standard, however, is not a role that has been delegated to or traditionally occupied by the CFPB. Further, by determining that Dwolla's statements regarding PCI compliance were deceptive, the CFPB necessarily made itself an arbiter of PCI compliance. Entities regulated by the CFPB should take note that it is willing to interpret PCI standards when entities have promised to meet those standards.

The CFPB as Interpreter of Cybersecurity "GAAP." When the Consent Order demands that Dwolla "obtain an annual data-security audit" from a third party, it does so in a way that suggests the existence of a kind of cybersecurity GAAP. *See* Consent Order ¶ 52.c.x ("Respondent must … obtain an annual data-security audit from an independent, qualified third-party, *using procedures and standards generally accepted in the profession*.").

Practical Measures for Regulated Entities. The CFPB suggests what it believes the components of a "reasonable and appropriate" cybersecurity

program are through its criticism of Dwolla's cybersecurity practices, as well as the remedial measures that the Consent Order mandates. Entities seeking to evaluate or improve their own cybersecurity practices should strongly consider adopting components such as: (1) a written data security plan to govern the collection, maintenance or storage of consumers' personal information; (2) data security policies and procedures reasonable and appropriate for the organization; (3) regular risk assessments and other measures to identify reasonably foreseeable security risks; (4) regular outside cybersecurity audits; (5) prompt corrective action in response to adverse findings during risk assessments and audits; (6) employee training; (7) participation of the board of directors and appointment of a qualified person to be accountable for the program; (8) developments of procedures to select and retain qualified third-party service providers; (9) secure software design, development and testing; and (10) use of encryption technology to properly safeguard consumer information. These components are similar to the CFPB's existing requirements for a compliance management system.[16]

If you have any questions concerning this *Alert,* please contact your attorney at Schulte Roth & Zabel or one of the following attorneys: Donald J. Mosher, Michael L. Yaeger or Melissa G.R. Goldstein.

---

[1] *See In re Dwolla, Inc.*,CFPBNo. 2016-CFPB-007 (Mar. 2, 2016) ("Consent Order"). Dwolla's payment network "is used for retail purchases, peer to peer transactions, online businesses, and donations for charities/non-profits. It enables users to use phone, computer, social networks, and physical locations to send and receive cash. The company was founded in 2010 and is based in Des Moines, Iowa." Company Overview of Dwolla Corp. (last visited Mar. 6, 2016). Dwolla neither admitted nor denied the substance of the CFPB's allegations.

[2] Consent Order ¶ 20.

[3] *Id.* ¶¶ 23-29.

[4] *Id.* ¶ 38.

[5] *Id.* ¶¶ 34-36.

[6] *Id.* ¶ 36.

[7] *See* 12 U.S.C. § 5531, 5536.

[8] Consent Order ¶ 52.

[9] *Id.* ¶ 53, 57.

[10] Press Release, Consumer Financial Protection Bureau, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016).

[11] *See FTC v. Wyndham Worldwide Corporation, et al.*, No. 14-3514 (3d Cir. Aug. 24, 2015).

[12] *See* 12 U.S.C. § 5531 ("The Bureau may take any action…to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive act or practice.").

[13] *See In the Matter of R.T. Jones Capital Equities Management, Inc.*, Investment Advisers Act of 1940 Release No. 4204, Admin. Proc. File No. 3-16827 (SEC) (Sept. 22, 2015), at 2.

[14] *See* Securities and Exchange Commission, Division of Investment Management, *IM Guidance Update* (April 2015), No. 2015-02, "Cybersecurity Guidance" ("Guidance Update").

[15] Annual audits by an independent third party, bi-annual risk assessments and certain other corrective actions required by the CFPB's Consent Order against Dwolla are not necessarily required for PCI compliance. *See* PCI Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS) Version 2.0* (Oct. 28, 2010).

[16] Consumer Financial Protection Bureau, *CFPBSupervision and Examination Manual, Version 2*, *Compliance Management Review* (October 2012).

The contents of these materials may constitute attorney advertising under the regulations of various jurisdictions.

Related People

Donald Mosher

Partner

New York

Melissa Goldstein

Partner

Washington, DC

Practices

BANK REGULATORY

CYBERSECURITY AND DATA PRIVACY

LITIGATION

Attachments

Download Alert