A NEW CYBER REGULATOR ON THE BEAT: THE CFPB ISSUES ITS FIRST CYBERSECURITY ORDER AND FINE

Date: 8 March 2016

Government Enforcement Alert

By: Theodore L. Kornobis

On March 2, 2016, the Consumer Financial Protection Bureau ("CFPB") instituted its first data security enforcement action, in the form of a consent order against online payment platform Dwolla, Inc.[1] The CFPB joins several other regulators that have recently issued statements or instituted enforcement actions in this space, including the Securities and Exchange Commission ("SEC"), Commodity Futures Trading Commission ("CFTC"), the Financial Industry Regulatory Authority ("FINRA"), the National Futures Association ("NFA"), the Department of Justice ("DOJ"), state attorneys general, and the Federal Trade Commission ("FTC"), which has been active in this area for several years.

Dwolla runs an online payment network that allows users to transfer funds to other consumers or merchants. The CFPB alleged that Dwolla's marketing and other statements relating to the network violated the Consumer Financial Protection Act's unfair, deceptive, and abusive practices ("UDAAP") provisions,[2] because they included false representations regarding Dwolla's data security practices. Specifically, the CFPB found that Dwolla's representations that its data security practices were "safe," "secure," and "exceed[ed] industry standards," were deceptive in that the company's security practices at the time were in fact not "reasonable and appropriate measures to protect data obtained from consumers." Dwolla did not admit or deny any of the findings of fact in the order and has issued statements making clear that its current security systems are adequate.

As the CFPB's first foray into this area, the consent order is notable in several respects:

- **First**, this action was brought in the absence of any data breach or evidence of consumer harm. Thus, the consent decree is further evidence that regulators are turning their attention to cybersecurity proactively, in advance of any sign of trouble. Companies may therefore expect data protection issues to arise in the context of routine examinations by regulators as well as more targeted examinations or enforcement-related inquiries into entities in industries that are particularly likely to be handling sensitive customer data (e.g., FinTech). Indeed, the SEC and FINRA, for example, have announced that cybersecurity measures will be a focus in regular inspections of investment advisers and broker-dealers.

- **Second**, the CFPB is again acting to enforce new standards that it has not enunciated through guidance or its rulemaking authority. Although the alleged violations were based on the company making deceptive representations to customers (as opposed to "unfair" practices), the *Dwolla* consent order illustrates the CFPB's belief that there are certain baseline standards of "appropriate" and "reasonable" cybersecurity measures for the industry. Yet, the CFPB has not issued written guidance or regulations stating what

those "appropriate" and "reasonable" cybersecurity measures are. Nonetheless, the order faults Dwolla for, among other things, a failure to "adopt or implement reasonable and appropriate data-security policies and procedures," failure to implement a "written data-security plan," failing to conduct "adequate, regular risk assessments," and not providing "adequate training and guidance" to employees.

That a regulator is setting standards through enforcement activity is not new. In its enforcement action against Wyndham Worldwide Corporation,[3] the FTC pursued unfair and deceptive acts and practices ("UDAP") claims based on Wyndham's representations about its cybersecurity efforts. The FTC alleged that those representations were both "deceptive," in that they were inaccurate, and were "unfair," in that the company's actual cybersecurity practices were purportedly deficient. On appeal to the Third Circuit, Wyndham argued that it lacked fair notice as to the standard to which the FTC was holding it, asserting that there were no rules or statutes explaining what steps companies must take to safeguard customer data. The Third Circuit rejected Wyndham's arguments, holding that the company had sufficient notice that its activity could fall within the ambit of the Federal Trade Commission Act's UDAP statute,[4] which is similar to the Consumer Financial Protection Act's UDAAP provisions, although the court did not decide whether the conduct at issue actually constituted "unfair" acts or practices.[5] The court noted that agency guidance documents, enforcement actions, and settlements could provide adequate notice as to what cybersecurity measures are reasonable.

In the *Dwolla* consent order, the CFPB did not cite specific regulations, past consent decrees, or government-issued guidance as sources forming the basis for what it claims to be "reasonable and appropriate" measures, but it did cite to "industry standards" requiring encryption and standards issued by the Payment Card Industry (PCI) Security Standards Council. However, in significant part, the *Dwolla* consent order appears to build on the foundation laid in the *Wyndham* decision as another example of a regulator measuring companies' cybersecurity efforts based on an imprecisely articulated standard with respect to what is "adequate" and "reasonable."

- **Third**, the *Dwolla* consent order does provide a window into what types of measures the CFPB will be looking at in future cases. Among other things, the CFPB found that Dwolla was lacking: (1) a written data security plan, (2) employee training on data security, (3) regular risk assessments, (4) appropriate vetting of vendors who handle customer data to ensure they have sufficient data protection standards and policies, and (5) encryption of any sensitive data.[6]

Companies of all types, including those in emerging technology and FinTech, should be aware that federal regulators are looking at data security practices—even in the absence of an actual breach—and may use their enforcement powers to remedy cybersecurity measures that do not meet the regulators' view of "reasonable" or "adequate."

Notes:

[1] Consent Order, *In re Dwolla, Inc.*, File No. 2016-CFPB-0007 (Mar. 2, 2016).

[2] 12 U.S.C. § 5531(a).

[3] *See* Am. Compl., *FTC v. Wyndham Worldwide Corp.*, No. 12-1365 (D. Ariz. Aug. 9, 2012).

[4] 15 U.S.C. § 45(a) (making unlawful "unfair or deceptive acts or practices in or affecting commerce").

[5] *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[6] Some of these allegations as to insufficient data security measures are similar to those described in other regulator cybersecurity actions. *See, e.g.*, Complaint at ¶ 21, *In re Credit Karma, Inc.*, Dkt. No. C-4480 (FTC Aug. 13, 2014).

KEY CONTACTS

THEODORE L. KORNOBIS
PARTNER

WASHINGTON DC
+1.202.778.9180
TED.KORNOBIS@KLGATES.COM

STEPHEN G. TOPETZES
PARTNER

WASHINGTON DC
+1.202.778.9328
STEPHEN.TOPETZES@KLGATES.COM

