The Banking Law Journal

Established 1889

An A.S. Pratt® PUBLICATION MAY 2016

LexisNexis

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3000

ISBN: 978-0-7698-7878-2 (print)
ISBN: 978-0-7698-8020-4 (eBook)
ISSN: 0005-5506 (Print)
ISSN: 2381-3512 (Online)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Office
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
www.lexisnexis.com

MATTHEW BENDER

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.

For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer. Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258 (phone). Material for publication is welcomed— articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys.

authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL LexisNexis Matthew Bender, 630 Central Ave, New Providence, NJ 07974.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

CFPB Expands UDAAP Jurisdiction in First Foray into Data Security Enforcement

Christopher G. Cwalina, Anthony E. DiResta, Kaylee A. Cox, and Brian J. Goodrich*

In its recent consent order with online payment platform Dwolla Inc., the Consumer Financial Protection Bureau alleged that Dwolla made false representations to consumers relating to its data security practices. This is the first time the Bureau has engaged in a data security enforcement action, marking a significant expansion of its regulatory focus. The authors of this article discuss the consent order and what's next for the Bureau.

The Consumer Financial Protection Bureau ("CFPB") has entered into a consent order[1] with online payment platform Dwolla Inc., alleging that Dwolla made false representations to consumers relating to its data security practices. This marks the first time the CFPB has engaged in an enforcement action relating to data security, and the action presents a significant expansion of the CFPB's growing regulatory focus. Cybersecurity and privacy enforcement has traditionally been policed by the Federal Trade Commission ("FTC"), but the CFPB is the most recent to join other regulators who have been increasing their focus in this space.

REPRESENTATIONS MADE TO CONSUMERS

Dwolla collected and stored consumers' personal information in connection with its services as a platform for financial transactions. For each consumer account, Dwolla collected the consumer's personal information, including the consumer's name, address, date of birth, telephone number, Social Security number, bank account and routing numbers, password, and four-digit PIN.

From 2011 through 2014, Dwolla represented to its consumers that it protected consumer data from unauthorized access with safe and secure transactions. Dwolla touted its data security practices as not only reasonable, appropriate and capable of ensuring that all transactions would be secure, but

* Christopher G. Cwalina (chris.cwalina@hklaw.com) is a partner at Holland & Knight LLP and co-chair of the firm's Data Privacy and Security Team. Anthony E. DiResta (anthony.diresta@hklaw.com) is a partner at the firm and the co-chair of the Consumer Protection Defense and Compliance Team. Kaylee A. Cox (kaylee.cox@hklaw.com) is an associate at the firm and a member of the Data Privacy and Security Team. Brian J. Goodrich (brian.goodrich@hklaw.com) is an associate in the firm's Litigation and Dispute Resolution Practice.

[1] http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

also said that its data security practices *exceeded* industry standards. The company also made representations on its web site that its transactions were safer than credit cards and less of a liability for both consumers and merchants. Dwolla also claimed that its compliance policies and procedures were in line with accepted industry criteria.

CFPB ALLEGATIONS OF FALSE REPRESENTATIONS

The CFPB viewed Dwolla's data security practices as falling far short of the claims made to consumers. The CFPB initiated an enforcement action against the company, alleging that Dwolla's statements were false and deceptive acts or practices in violation of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"). The CFPB did not allege that Dwolla's systems were breached and instead focused on representations about Dwolla's security practices.

The CFPB alleged that Dwolla's data security practices and compliance efforts were inadequate, including, among others, that the company:

- did not adopt or implement reasonable and appropriate data security policies and procedures governing the collection, maintenance or storage of consumers' personal information;
- did not adopt or implement a written data security plan;
- failed to conduct adequate, regular risk assessments to identify reasonably foreseeable internal and external risks to consumers' personal information;
- provided little to no data security training to employees;
- failed to encrypt stored or transmitted consumer personal information on numerous occasions and encouraged consumers to submit sensitive information via e-mail in clear text;
- failed to test the security of the apps on its website prior to releasing the apps to the public; and
- did not conduct risk assessments or penetration tests on its web site.

CONSENT ORDER

Under the terms of the consent order, Dwolla must:

- cease making any misrepresentations about its data security practices;
- securely store and transmit all consumer data, including making changes to its current data security practices as necessary;

- establish, implement and maintain a written, comprehensive data security plan, which must designate a qualified person to coordinate and be accountable for the company's data security program, as well as conduct bi-annual risk assessments and audits, the results of which are to be used to adjust the plan as necessary;
- provide regular data security training to employees; and
- pay a $100,000 civil penalty.

CFPB EXPANDS JURISDICTION

The Dodd-Frank Act excludes from the definition of enumerated consumer laws placed under the CFPB's jurisdiction the key provisions of the Gramm-Leach-Bliley Act, the primary federal law regulating data security. The CFPB's consent order with Dwolla demonstrates that the CFPB has gotten around this limitation by self-defining its Unfair, Deceptive or Abusive Acts and Practices ("UDAAP") authority as encompassing data security matters. For entities subject to the CFPB's jurisdiction, this order indicates that data security practices and compliance policies may now be within the scope of the CFPB's review.

GUIDANCE FOR COMPANIES REGULATED BY THE CFPB

Going forward, companies subject to the CFPB's jurisdiction should ensure that their representations about data security practices are accurate and substantiated. Additionally, the terms of the consent order show that the CFPB expects management at the highest level to be involved in, and accountable for, companies' data security practices and compliance. This expectation of board-level oversight of companies' information security programs is consistent with that of other regulators, including the FTC, the U.S. Securities and Exchange Commission ("SEC"), state attorneys general, and others.

It is important to note that the CFPB frequently initiates new law enforcement initiatives by announcing an initial consent decree with a smaller company that does not have the resources to defend itself fully, thereby creating precedent to move forward (i.e., future CFPB data security actions are likely).

WHAT'S NEXT FOR THE CFPB?

The CFPB's inaugural foray into the realm of data privacy leaves two questions open that companies subject to the CFPB's jurisdiction should consider.

First, the CFPB's enforcement action against Dwolla was preemptive in

nature; the CFPB did not record any tangible harm to consumers. Accordingly, CFPB observers may be justified in wondering if Director Cordray will instruct his enforcement staff to apply the same preemptive approach to other areas of federal consumer protection law enforced by the CFPB. As such, companies should be sure to proactively assess sensitive areas of operations for compliance with federal consumer protection laws, and ensure that they have robust and up-to-date compliance procedures and policies.

Second, the CFPB has entered an already crowded regulatory area. The FTC, Federal Communications Commission and state attorneys general are active in the data security arena. Future CFPB enforcement actions may shed light on whether or not the CFPB intends to go it alone, or collaborate with the other active regulators in this field.