Bloomberg BNA

BNA's Banking Report™

Reproduced with permission from BNA's Banking Report, Vol. 106, No. 23, 06/06/2016. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Data Security

The authors examine the Consumer Financial Protection Bureau's foray into data security enforcement by assessing how the bureau's data security authority compares with that of other federal regulators. The authors analyze the bureau's first data security enforcement and highlight open questions regarding the CFPB's data security agenda.

BNA INSIGHTS: The CFPB and Data Security Enforcement



BY MICHAEL GORDON, ELIJAH ALPER AND LEAH SCHLOSS

Michael Gordon is a Partner in the Washington office of WilmerHale and Chair of the firm's Consumer Financial Protection Bureau Practice. He joined WilmerHale after spending four years in senior positions at the CFPB, helping to design, build and set priorities for the Bureau since its inception.

Elijah Alper is Counsel in the Washington office of WilmerHale, where he advises financial institutions in supervisory and enforcement matters regarding traditional consumer finance and emerging technologies.

Leah Schloss is a Senior Associate in the Washington office of WilmerHale, where she advises clients on cybersecurity, government contracts, and export control investigative, regulatory and compliance issues.

The Consumer Financial Protection Bureau (CFPB) announced its intention to act as a data security regulator by releasing its first unfair, deceptive or abusive acts or practices (UDAAP) enforcement action for allegedly deceptive statements about data security practices after remaining largely silent on the topic for more than four years. The CFPB's March enforcement action, against a small payments company,[1] contains only a modest civil money penalty and does not require payments to customers. The language in the bureau's action suggests that it expects regulated companies to implement certain data security processes and that it may take further enforcement action in the area of data security.

Despite this enforcement threat, the bureau has provided virtually no guidance on the specific data security practices it expects companies to follow. Nor has it explained how it will determine whether data security measures are ''reasonable'' or ''industry standard.'' While other federal agencies have released extensive

[1] *In the Matter of Dwolla, Inc.*, File No. 2016-CFPB-0007 (Mar. 3, 2016).

COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0891-0634

rulemaking and guidance on data security, the bureau has not indicated whether it will act consistently with that prior guidance, or whether it will require its regulated institutions to adopt more stringent data security practices. The bureau's first data security enforcement action provides little guidance for regulated entities concerned about data security.

In this article, we examine the CFPB's foray into data security enforcement action by assessing how the bureau's data security authority compares with that of other federal regulators. We then analyze the bureau's first data security enforcement and highlight open questions regarding the CFPB's data security agenda.

Existing Federal Data Security Regulation Outside the CFPB

The CFPB has joined a crowded field of federal regulators policing data security through authority granted by several statutes and regulations. There is no universal federal law on data security, and jurisdiction is shared among regulators that oversee banks, nonbank financial services companies and nonfinancial companies.

Of all federal regulators, the Federal Trade Commission (FTC) has been the most active in data security to date. The FTC relies on two authorities to enforce data security compliance: (1) statutory authority to police unfair and deceptive acts or practices under Section 5 of the FTC Act, and (2) its authority to enforce its ''safeguards'' regulations promulgated under the Gramm-Leach-Bliley Act (GLBA). The federal banking agencies have similar authority over their regulated institutions.

FTC Section 5 Enforcement: The FTC has used its authority under Section 5 to bring more than 60 enforcement actions since 2002 against companies for engaging in allegedly ''unfair'' or ''deceptive'' data security practices.[2] The FTC has alleged that companies acted ''deceptively'' by making material and false statements about their data security practices that misled consumers,[3] and it has claimed that companies acted ''unfairly'' when allegedly lax data security practices caused (or were likely to cause) sensitive consumer information to be stolen through security breaches.[4] The FTC believes that such conduct is unfair under Section 5 of the FTC Act because consumers are reasonably likely to be harmed when their sensitive information is compromised, and consumers cannot avoid such injury.

The FTC's authority to enforce lax data security practices as ''unfair'' conduct is not fully resolved, especially where no data breach took place. In November 2015, the FTC's chief administrative law judge dismissed an FTC complaint against LabMD, holding that consumer harm that is merely *possible* due to alleged data security weaknesses — without any evidence to support that such harm is in fact *likely* — is insufficient to prove unfairness under Section 5 of the FTC Act.[5] The case is on administrative appeal to the full FTC, and oral argument was held March 8. The FTC did prevail earlier in 2015 on a challenge to its unfairness authority, when the Third Circuit Court of Appeals, in a case against Wyndham hotels, affirmed that the FTC's unfairness authority allows it to bring enforcement actions for lax data security.[6] However — unlike in *LabMD* — in the Third Circuit case, the FTC alleged an actual data breach resulting in a specific alleged loss to consumers.[7]

The FTC first released guidance in 2007 identifying what it considers reasonable data security standards for protecting personal information, and it updated this guidance in 2011.[8] Together with the FTC's extensive enforcement history,[9] the guidance provides companies with a detailed road map for complying with the FTC's data security expectations.

The Third Circuit pointed to this guidance, as well as the FTC's history of publishing complaints and consent decrees, in holding that Wyndham had fair notice that its specific cybersecurity practices might be interpreted by the FTC as ''unfair'' conduct under Section 5 of the FTC Act.[10]

FTC Safeguards Rule: In addition to its Section 5 authority, the FTC regulates data security through powers granted to it by the GLBA. That statute directed the FTC and federal banking agencies to establish ''appropriate standards'' for financial institutions to establish administrative, technical and physical safeguards relating to the security and confidentiality of customer information.[11]

The FTC's implementing regulations, commonly referred to as the ''Safeguards Rule,'' require those financial institutions subject to the FTC's GLBA jurisdiction to implement and maintain a comprehensive written

---

[2] Fed. Trade Comm'n, *Privacy & Data Security Update: 2015*, at 4 (December 2015). *See, e.g.*, *In re: HTC America, Inc.*, FTC Docket No. C-4406 (Jun. 25, 2013); *In re: CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009); *In re: Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (one of the first FTC orders requiring a ''comprehensive information security program'').

[3] *See, e.g.*, Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014).

[4] *See, e.g.*, *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR, Complaint at ¶¶ 47-49 (D.N.J., June 26, 2012).

[5] *In re: LabMD Inc.*, FTC Docket No. 9357, ALJ's Initial Decision (Nov. 13, 2015).

[6] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[7] *See, e.g.*, *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR, Complaint at ¶ 40 (D. Ariz., June 26, 2012).

[8] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (December 2007, updated November 2011). The guidance provides a security checklist built around five basic principles: organizations that keep personal information need to know what data they have, retain only the data they need, protect information that is kept, properly dispose of data that is no longer needed, and develop an incident response plan.

[9] In June 2015, the FTC released additional guidance based on ''lessons learned'' from its data security actions. Fed. Trade Comm'n, *Start with Security: A Guide for Business* (June 2015).

[10] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d at 256-259.

[11] 15 U.S.C. § 6801(b) (requiring safeguards ''(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer'').

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. BBR ISSN 0891-0634

data security program addressing a few basic prescribed security issues,[12] but the Safeguards Rule generally does not specify details about the types of data security measures the institutions must implement. The FTC has enforced the Safeguards Rule through more than 10 public actions (all against nonbanks) for alleged violations.[13]

Federal Banking Agencies: Separately, the federal banking agencies promulgated the Interagency Guidelines for Safeguarding Consumer Information.[14] Like the FTC's Safeguards Rule for nonbanks, the Interagency Guidelines implement the GLBA's data security provisions for institutions regulated by the federal banking regulators, but the Interagency Guidelines are generally more detailed and demanding.

For example, unlike the FTC Safeguards Rule, the Interagency Guidelines require involvement from bank directors and senior leadership, and they require banks to take an active role in overseeing data security practices of their service providers.

These Interagency Guidelines have been supplemented by various guidance documents and bulletins by the Federal Financial Institutions Examination Council (FFIEC).[15] Most significantly, the FFIEC Information Security Booklet, one of the booklets that comprise the FFIEC Information Technology Examination Handbook, includes detailed guidance on information security practices federal financial examiners expect financial institutions to implement.[16]

The CFPB's Potentially Powerful Data Security Authority

The Dodd-Frank Act did not explicitly direct the bureau to regulate data security, nor is there an obvious gap in federal data security oversight that only the bureau can fill. However, the bureau's UDAAP powers allow it to participate in data security supervision, rulemaking and enforcement.[17]

Like the FTC, the CFPB can assert that its UDAAP authority permits it to take enforcement action against companies for alleged data security practices or statements it finds unfair or deceptive, and the CFPB can also penalize companies for practices it deems abusive.

However, it is far from clear that Congress intended the bureau to use its UDAAP authority in this way. The Dodd-Frank Act granted the bureau authority over virtually every federal consumer financial law, including the GLBA's provisions regarding consumer privacy, but it expressly carved out the GLBA's data security provision that underlies the FTC's Safeguards Rule and the Interagency Guidelines.[18] Thus it appears that Congress intended the bureau's data security authority to be narrower than that reserved for the FTC and federal banking agencies, if Congress intended the bureau to be a data security regulator at all.

While the FTC's and CFPB's jurisdiction over unfair and deceptive acts and practices may cover similar conduct, there are key differences between the power each agency has to enforce these provisions:

- *Civil Money Penalties (CMPs)*: The bureau can assess civil penalties for any UDAAP violation, while the FTC can assess penalties only in limited circumstances, such as for violations of existing administrative orders.[19] CMP authority is particularly important in data security actions, where it might be difficult to estimate consumer harm for restitution purposes.
- *Supervisory Authority*: The bureau has examination authority over several of its regulated entities. Covered institutions include banks with more than $10 billion in assets (and their affiliates), mortgage companies, payday and private student lenders,[20] and ''larger participants'' in the consumer financial market, as defined by rulemaking.[21] This comprehensive power grants the bureau broad, on-site access to the books and records of the supervised institutions. Bureau supervisory staff can direct supervised institutions to change data security practices through the supervisory process, or they can refer suspected violations to the CFPB's enforcement division. By contrast, the FTC is generally limited to issuing civil investigative demands (CIDs) to investigate companies, and the CFPB has its own CID authority in addition to its supervisory powers.
- *Rulemaking Authority*: The bureau can write UDAAP regulations under standard administrative

[12] 16 C.F.R. Part 314.

[13] *See, e.g., United States v. PLS Fin. Services, Inc.*, No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012); *In re: ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011); *In re: Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Nov. 9, 2004).

[14] 12 C.F.R. pt. 30, app. B (as incorporated in Ofiice of the Comptroller of the Currency regulations). The federal banking agencies issued the Interagency Guidelines under their authority to establish safety and soundness guidance. Accordingly, a bank's failure to meet these guidelines permits the federal banking agencies to require a bank to submit a nonpublic compliance plan. Failure to submit an acceptable plan, or material failure to implement an accepted plan, can lead to a formal and public order to compel compliance. *See generally* 12 C.F.R. pt. 30 (OCC safety and soundness enforcement procedures).

[15] The CFPB is a member of the FFIEC, but, as explained below, the bureau lacks enforcement authority under the GLBA's data security provisions.

[16] Other booklets in the FFIEC Handbook, such as the booklets on outsourcing technology services and e-banking, also include information regarding financial regulators' data security expectations. FFEIC, *Outsourcing Technology Services* (June 2004); FFIEC, *E-Banking* (August 2003); *see also* Risk Management Guidance, OCC Bulletin 2013-29 (Oct. 30, 2013).

[17] Although the scope of the bureau's data security powers have never been tested, questions have been raised about the scope of the CFPB's jurisdiction in this area. *See, e.g.*, Jonathan G. Cedarbaum & Elijah Alper, *The Consumer Financial Protection Bureau as a Privacy & Data Security Regulator*, 17 FinTech Law Report (May/June 2014).

[18] *See* 12 U.S.C. § 5481(12)(J) (defining ''enumerated consumer laws'' and including only sections 502 through 509 of the GLBA).

[19] 15 U.S.C. § 45(l) (providing for penalties against a party ''who violates an order of the Commission after it has become final, and while such order is in effect''). *See, e.g., Fed. Trade Comm'n v. LifeLock, Inc., et al.*, No. 2:10-CV-10-00530-PHX-JJT (Dec. 17, 2015) (LifeLock agreed to pay $100 million to settle charges that it had violated the terms of 2010 federal court order).

[20] *See* 12 U.S.C. § 5514 (authority over certain nonbanks), 5515 (authority over large banks and their affiliates).

[21] To date, the bureau has issued rules identifying ''larger participants'' in the consumer reporting, debt collection, student loan servicing, international money transfers and auto finance markets. 80 Fed. Reg. 37496, 37497 (Jun. 30, 2015).

notice-and-comment procedures, while the FTC's Section 5 rulemaking authority is subject to significant procedural hurdles.[22] Before now, the bureau had given virtually no public guidance on data security.[23] While the bureau to date has preferred to define UDAAP practices through enforcement rather than prospective rulemaking,[24] it could bring much-needed transparency to its data security expectations by clarifying, through a notice-and-comment process, what data security practices and safeguards are required to avoid UDAAP violations.

- *Covered Persons*: The CFPB's UDAAP authority applies only to covered persons (and their service providers) to the extent they offer a ''consumer financial product or service.'' While most financial institution activities are included in the definition of ''consumer financial product,'' some activities (e.g., securities and the business of insurance) are expressly exempt, and other companies have argued that they are not covered by this term.[25] The FTC's Section 5 authority applies broadly to nonbanks regardless of whether they are subject to CFPB UDAAP jurisdiction.[26]

The CFPB's Uncertain Data Security Role Going Forward

The bureau has made a modest entrance into data security enforcement. Like the FTC, the bureau appears to be comfortable policing data security through its authority to address unfair and deceptive practices. But unlike the FTC, the bureau has not articulated which practices are ''reasonable'' or ''industry standard,'' even though it has now demonstrated a willingness to conduct enforcement for violations of its data security expectations. This leaves regulated entities in the difficult position of knowing that the bureau has data security expectations, but not knowing what those expectations are or what steps companies should take to avoid enforcement.

The bureau has several tools at its disposal should it choose to become more active on data security. It could use its unique UDAAP rulemaking authority to promulgate detailed regulations requiring specific data security measures. Unlike the FTC, the bureau could assert this UDAAP authority against banks to mandate data security protections that the federal banking regulators have not required. The CFPB might even assert that violations of the Safeguards Rule and Interagency Guidelines also constitute ''unfair'' or ''deceptive'' conduct, which could permit the bureau to take enforcement action for those violations.

The FTC's Safeguards Rule enforcement actions often allege that conduct violating the Safeguards Rule also violates Section 5 of the FTC Act,[27] and the CFPB has taken a similarly expansive view of UDAAP in other contexts, e.g., in applying violations of the Fair Debt Collection Practices Act to original creditors.[28] The bureau might decide to allege unfair conduct even where there is no data breach or evidence of consumer harm. It could claim that the LabMD decision holding otherwise applies to the FTC only, even though the standards both agencies use to define ''unfair'' conduct are essentially identical.

The bureau's latest action also brings to a head several questions about how, or whether, the CFPB will work with the other federal agencies enforcing data security practices. The bureau may be content with occasional enforcement actions that follow the FTC's existing Section 5 theories, or it may attempt to become the leading data security regulator for consumer financial products and services.

Bureau data security enforcement may renew calls for the CFPB to cooperate with the FTC, which has overlapping jurisdiction over unfair and deceptive practices. Thus far, the bureau has resisted calls for a formal, public division in enforcement authority with the FTC, despite reports that the two agencies seem to compete as much as they cooperate. Nor has either agency explained how certain cases end up with the bureau while substantially similar cases against similar companies are pursued by the FTC.[29] Because the CFPB has far greater civil money penalty authority, companies targeted by the bureau for data security issues might face greater punishment than a similarly situated company investigated by the FTC.

The bureau's single enforcement action to date provides few hints as to how often the agency will pursue data security regulation or enforcement. Absent further

---

[22] *See* 12 U.S.C. § 5531(b). The FTC's Section 5 rulemaking authority was restricted by the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, which required the FTC to show ''substantial evidence'' to promulgate regulations to prevent ''prevalent'' unfair or deceptive acts. *See* Pub. L. 93-637, 15 U.S.C. § 2301 et seq. (1975).

[23] In 2014, the CFPB published a blog post advising consumers on how to respond to a data breach. *See, e.g.*, Gail Hillebrand, ''Four Steps You Can Take If You Think Your Credit or Debit Card Data Was Hacked,'' Consumer Fin. Protection Bureau (Jan. 27, 2014).

[24] Richard Cordray, Director, Consumer Fin. Protection Bureau, Remarks at the Consumer Bankers Association (Mar. 9, 2016). (Bureau enforcement orders ''are also intended as guides to all participants in the marketplace to avoid similar violations and make an immediate effort to correct any such improper practices.'').

[25] *In re: J.G. Wentworth, LLC*, 20IS-MISC-J.G. Wentworth, LLC-0001, Petition to Set Aside Civil Investigative Demand (Oct. 2, 2015). Banks with less than $10 billion in assets and certain of their service providers are generally exempt from CFPB enforcement authority. *See* 12 U.S.C. 5516.

[26] 15 U.S.C. § 45(a)(1). Certain entities, such as common carriers and nonprofits, are wholly or partially exempt from FTC's Section 5 jurisdiction.

[27] *See e.g., United States v. PLS Fin. Services, Inc.*, No. 1:12-cv-08334, Complaint at ¶¶ 30-31 (N.D. Ill. Oct. 17, 2012); *In re: Premier Capital Lending*, FTC File No. 072-3004 Complaint at ¶¶ 19-21 (Dec. 10, 2008).

[28] *See* CFPB Bulletin 2013-07, *Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts* (July 10, 2013) (''Although the FDCPA's definition of 'debt collector' does not include some persons who collect consumer debt, all covered persons and service providers must refrain from committing UDAAPs in violation of the Dodd-Frank Act.'').

[29] Compare *Fed. Trade Comm'n v. T-Mobile USA, Inc.*, No. 2:14-cv-00967 (W.D. Wash., Jul. 1, 2014); *Fed. Trade Comm'n v. AT&T Mobility, LLC*, No. 1:14-mi-99999-UNA (N.D. Ga., Oct. 8, 2014) (alleging charging consumers for third-party subscription services they had not authorized were unfair or deceptive under Section 5 of the FTC Act), with *Consumer Fin. Protection Bureau v. Sprint Corp.*, No. 1:14-cv-09931 (S.D.N.Y., Dec. 17, 2014) (alleging similar conduct violated the Consumer Financial Protection Act).

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC. BBR ISSN 0891-0634

guidance from the bureau, it is too soon to tell whether the CFPB will merely supplement the data security oversight of the FTC and federal banking agencies, or whether it will break with those other regulators and pursue its own data security agenda.