The Consumer Financial Protection Bureau

Bethany Rupert[1]

I. INTRODUCTION

In July 2010, Congress passed and President Obama signed the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act). Title X of the Dodd-Frank Act created the Consumer Financial Protection Bureau (the Bureau or the CFPB).[2] The Bureau's purpose is to "implement and . . . enforce Federal consumer financial law consistently" and to ensure both "that all consumers have access to markets for consumer financial products and services" and "that markets for consumer financial products and services are fair, transparent, and competitive."[3] The creation of the CFPB consolidated most federal consumer financial protection authority in one place, although the CFPB's authority still overlaps to some degree with that of the Federal Trade Commission and other federal banking agencies.

Since its creation, the Bureau has focused primarily on providing guidance on and enforcing the laws and rules governing the development, marketing, and maintenance of consumer financial products and services. The CFPB also has authority to regulate the privacy and cybersecurity of consumer financial information. The Bureau, however, has taken only a limited number of steps to regulate privacy and cybersecurity, even though the Dodd-Frank Act granted it extensive authority in those areas.

This paper provides an overview of the CFPB's sources of authority to regulate privacy and cybersecurity, the tools the CFPB has to encourage and require compliance with privacy and cybersecurity regulations and statutes, the CFPB's initial enforcement steps as a regulator of privacy and cybersecurity, and the CFPB's first cybersecurity enforcement action.

II. STATUTES AND REGULATIONS ENFORCED BY THE CFPB

The CFPB's authority to penalize acts or omissions in the cybersecurity and privacy spaces partly stems from its authority to issue and enforce regulations that implement the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Electronic Fund

[1] King & Spalding would like to recognize former associate Brett Schlossberg for his contributions to previous drafts of this white paper.

[2] *See* 12 U.S.C. § 5491(a) (2014).

[3] *See* 12 U.S.C. § 5511(a) (2014).

Transfer Act (EFTA). Title X of the Dodd-Frank Act — also known as the Consumer Financial Protection Act of 2010[4] — transferred much of the rulemaking and enforcement authority under these statutes, including the privacy provisions, to the CFPB.[5] Therefore, the CFPB may enforce these statutes and even issue new regulations covering a wide range of financial institutions, including banks, mortgage servicers, credit rating agencies, and other nonbank financial companies.[6]

A. Unfair, Deceptive, or Abusive Acts or Practices

Under the Consumer Financial Protection Act, the CFPB has the authority to penalize certain entities that commit an "unfair, deceptive, or abusive act or practice . . . in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service."[7] That authority is known as the CFPB's "UDAAP" authority. Unlike other statutory sources of the CFPB's authority (described below), prior to the Dodd-Frank Act, UDAAP authority did not exist. Rather, the Dodd-Frank Act created UDAAP authority and granted it to the CFPB.[8] The CFPB may define UDAAP through its rulemaking authority, just as it would any other regulation.[9] Although the CFPB's transferred authority over enumerated consumer laws applies to any person covered by those laws, its UDAAP authority is limited to consumer financial products and services.[10] Therefore, a "covered person" for the purposes of UDAAP is a person or institution that offers or provides a consumer financial product or service, including extensions of credit, mortgages, money transmissions or exchanges, payment processors, credit reporting, and debt collection.[11] Additionally, a "covered person" also includes any "related person" — a person who has managerial responsibility or is "materially involved" in the management of a person within the CFPB's jurisdiction, including independent contractors.[12]

Under its UDAAP authority, the CFPB may declare certain acts or practices by covered persons "abusive," and may use this power to enforce certain privacy and data security standards. The CFPB may declare an act abusive if the act occurs in connection with a consumer financial product or service, and if it (1) materially interferes with the ability of a consumer to understand a term or condition of a product or service; or (2) takes unreasonable advantage of a consumer's lack of understanding of the costs or risks of the product or service, a consumer's inability to protect his or her interests in selecting the product or service, or a

---

[4] Sections 1053 and 1055 of the Consumer Financial Protection Act of 2010 correspond to 12 U.S.C. §§ 5563 and 5565, respectively.

[5] *See* 12 U.S.C. § 5581(b)–(c) (2014).

[6] *See, e.g.,* 15 U.S.C. § 1681s (2014) (describing FTC and CFPB authority over credit rating agencies); 12 U.S.C. § 5564 (2014) (authorizing the CFPB to commence civil actions against "any" person who violates a federal consumer financial law).

[7] *See* 12 U.S.C. § 5531 (2014).

[8] Alper, Elijah and Cedarbaum, Jonathan G., *The Consumer Financial Protection Bureau As a Privacy & Data Security Regulator*, FINTECH LAW (May/June 2014), *available at* file:///C:/Users/113403/Downloads/fintech-law-report-IP-strategies-competitive-marketplace-2014%20(3).pdf, at 6.

[9] *See* 12 U.S.C. § 5531(b) (2014).

[10] *See* 12 U.S.C. § 5531(a) (2014).

[11] *See* 12 U.S.C. § 5481(6) (2014).

[12] *See* 12 U.S.C. § 5481(25) (2014).

consumer's reasonable reliance on a covered person to act in the interests of the consumer.[13] Although the CFPB has issued little guidance on how it will interpret the "abusive" standard, some commentators have suggested that the Bureau could interpret the standard to cover privacy or cybersecurity failings.[14] Furthermore, others have noted that CFPB enforcement in the area of privacy and cybersecurity is even more likely if the CFPB follows its historical practice of adopting the broad understanding of the FTC's "deceptive" and "unfairness" authority.[15] According to then-CFPB Senior Counsel Pavneet Singh in November 2014, the CFPB's priorities "are . . . based on what . . . [the Bureau] find[s]" when it examines violations of and enforces consumer financial protection laws.[16] If the CFPB finds cybersecurity practices that it deems abusive, the Bureau may, through federal district court proceedings or its administrative procedures, "order any appropriate legal or equitable relief, including, among other remedies, rescission of contracts, restitution, disgorgement, and civil monetary penalties," or it may "issue cease-and-desist orders or obtain consent orders in settlement of" its proceedings.[17]

Although the FTC has similar authority to the CFPB to address "deceptive and abusive" practices, the authority of the two agencies does not always overlap. If the CFPB chooses to exercise its UDAAP authority to enforce privacy and cybersecurity requirements, some commentators have hypothesized that the Bureau likely will concentrate that authority on institutions "exempted from the FTC jurisdiction, such as banks and credit unions . . . , or on concerns that are unique to covered persons, such as how credit bureaus safeguard consumer credit report information, or concerns that are unique to consumer financial products, such as data sharing between creditors, debt collectors, and debt buyers."[18] Also, if the CFPB becomes a more active regulator in these areas, it will have access to more powerful investigatory and enforcement tools than the FTC.

i. The Gramm-Leach-Bliley Act and Regulation P

Using its statutory authority, the CFPB has issued certain regulations to enforce data privacy and cybersecurity. For instance, the CFPB issued Regulation P under the Gramm-Leach-Bliley Act. Regulation P requires financial institutions to provide annual notices to

---

[13] According to an article written by two U.S. litigators in 2012, "with this reliance component, the CFPB has singlehandedly transformed the relationship between financial institutions and consumers from one of arms-length dealing to one with fiduciary overtones." John Tumilty and Katherine Guarino, *The CFPB's confusing definitions of unfair, deceptive or abusive acts and practices*, INSIDE COUNSEL (Sept. 13, 2012).

[14] *See* Cedarbaum and Alper, *supra* note 7, at 6.

[15] *See* Cedarbaum and Alper, *supra* note 7, at 6–7.

[16] Grande, Allison, *CFPB Taking Privacy Cue From FTC, Official Says*, LAW360 (Nov. 5, 2014), *available at* http://www.law360.com/articles/593890/cfpb-taking-privacy-cue-from-ftc-official-says.

[17] *See* 12 U.S.C. §§ 5563–65; *see also* Cedarbaum and Alper, *supra* note 7, at 8.

[18] *See* Cedarbaum and Alper, *supra* note 7, at 8. *See also* 12 U.S.C. §§ 5514 (authority over certain nonbanks), 5515 (authority over larger banks and their affiliates).

customers about their privacy policies and practices.[19] These privacy notices, which may be mailed to customers or posted online,[20] must disclose:

i. the categories of nonpublic personal information (NPPI) the institution has collected;

ii. the categories of NPPI the institution has disclosed to others;

iii. the categories of affiliates and nonaffiliated third parties to whom the institution may disclose NPPI;

iv. the institution's policies regarding the treatment of a former customer's NPPI;

v. NPPI that has been disclosed to service providers and joint marketers;

vi. an explanation of the opt-out right and methods for opting out; and

vii. the institution's policies for protecting the security and confidentiality of NPPI.[21]

However, a privacy notice's disclosure regarding an institution's security and confidentiality policies for NPPI does not need to disclose information about those policies in great detail, "but instead may [disclose] in general terms who is authorized to have access to the . . . [NPPI] and whether the institution has security practices and procedures in place to ensure the confidentiality of the . . . [NPPI] in accordance with the institution's policies."[22] Still, financial institutions are required to follow the GLBA's "safeguards rules," which instruct financial institutions to establish administrative, technical and physical safeguards relating to the security of customer information.[23] The CFPB does not have authority to enforce the "safeguards rules," which instead are enforced by the FTC and the federal banking authorities.[24]

Regulation P also describes the conditions under which a financial institution may disclose NPPI about consumers to nonaffiliated third parties and provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure.[25] Generally, financial institutions may not disclose a consumer's NPPI to a third party unless the institution provides the consumer with an initial notice of the disclosure and with the ability to opt out of the disclosure.[26]

---

[19] *See* 12 CFR § 1016 (2016).

[20] *See CFPB Finalizes Rules to Promote More Effective Privacy Disclosures*, CONSUMER FINANCIAL PROTECTION BUREAU (Oct. 20, 2014), *available at* http://www.consumerfinance.gov/newsroom/cfpb-finalizes-rule-to-promote-more-effective-privacy-disclosures.

[21] *See Regulation P: Privacy of Consumer Financial Information*, CONSUMER COMPLIANCE HANDBOOK, 5 (2011), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/consumer.pdf.

[22] *See id.* at 6.

[23] *See* 12 U.S.C. § 5481(12)(J) (2014); 15 U.S.C. §§ 6802–6809 (2014).

[24] *See id.*

[25] *See* 12 CFR § 1016 (2016).

[26] *See id.*

ii. The Fair Credit Reporting Act and Regulation V

The FCRA, as implemented by Regulation V, creates a regulatory framework for the furnishing, use, and disclosure of information in decisions made about consumers and in reports associated with credit, insurance and employment.[27] The FCRA became law in 1971 and received considerable amendments in 1996, 2003 and 2010.[28] When the Dodd-Frank Act granted FCRA rulemaking authority to the CFPB, the Bureau restated Regulation V, which is now located at 12 CFR § 1022. Regulation V imposes multiple obligations on entities that count as "consumer reporting agencies."[29] Additionally, the regulation imposes obligations on persons who use consumer report information or give information to consumer reporting agencies.[30]

The FCRA also requires consumer reporting agencies to ensure the accuracy of the data placed in the consumer reporting system, and generally restricts agencies from sharing consumer reports with affiliate companies.[31] However, the statutory definition of "consumer report" contains key exceptions that enable agencies to share this type of information under certain circumstances.[32] For example, the definition of a consumer report does not include a report that contains information solely about transactions or experiences between the consumer and the person making the report.[33] When agencies share this type of information, they are not "consumer reporting agencies" for the purposes of the FCRA.[34]

iii. The Electronic Fund Transfer Act and Regulation E

The EFTA, which the Bureau implemented through Regulation E, requires financial institutions to disclose situations in which they share consumer information with a third party.[35] The Dodd-Frank Act transferred EFTA rulemaking authority from the Board of Governors of the Federal Reserve System to the CFPB. The EFTA seeks to protect individual consumers who engage in electronic fund transfers (EFTs) and remittance transfers.[36] According to the EFTA, "a[n] institution must describe the circumstances under which any information relating to an account to or from which EFTs are permitted will be made available to third parties, not just information concerning those EFTs. The term 'third parties' includes affiliates such as other subsidiaries of the same holding company."[37]

---

[27] *See CFPB Supervision and Examination Manual*, CONSUMER FINANCIAL PROTECTION BUREAU, 48–49 (2012), *available at* http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf.

[28] *See id.* at 48.

[29] *See id.* at 49.

[30] *See id.*

[31] *See id.* at 588–89, 630.

[32] *See id.* at 588–89.

[33] *See CFPB Supervision and Examination Manual*, *supra* note 26, at 588–89.

[34] *See id.*

[35] *See* 12 CFR § 1005 (2016).

[36] *See Regulation E: Electronic Fund Transfer Act*, CONSUMER COMPLIANCE HANDBOOK, 1 (2013), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf.

[37] *See id.* at 7.

III. CFPB'S ENFORCEMENT AUTHORITY

The Bureau has a variety of tools that it can use to encourage and require compliance with federal consumer financial statutes and regulations, including those that pertain to privacy and cybersecurity. The CFPB has the authority to engage in joint investigations and requests for information with other federal agencies.[38] Additionally, the Bureau may issue deposition subpoenas and document subpoenas.[39] To obtain information or tangible things, the CFPB also has the authority to issue civil investigative demands (CIDs) "before the institution of any proceedings under the federal consumer financial law."[40] However, when the Bureau obtains documentary materials or tangible things because of a CID, the materials and things are "subject to requirements and procedures regarding confidentiality, in accordance with rules established by the Bureau."[41] If an entity fails to comply with a CID, the CFPB has the option to ask a district court of the United States to issue an order that enforces the CID.[42]

The Bureau also has non-investigatory enforcement tools. The CFPB has the authority to hold hearings and conduct adjudication proceedings.[43] Additionally, the Bureau may bring civil actions against entities that violate federal consumer financial laws.[44] In the civil actions, the CFPB may seek civil penalties, legal relief and equitable relief, "including a permanent or temporary injunction as permitted by law."[45] Specifically, if the CFPB chooses to enforce its cybersecurity regulations ("a law, rule, or final order or condition imposed in writing by the Bureau"), it could fine an entity up to $5,000 per day for a violation.[46] And if the CFPB chooses to enforce its UDAAP authority (over federal consumer financial laws) to the area of cybersecurity, it could fine an entity up to $25,000 per day for a "reckless" violation, and up to *$1,000,000 per day for a "knowing" violation*.[47] In determining the penalty in any civil action, the Bureau or the court will take into consideration "the size of financial resources and good faith of the person charged; the gravity of the violation or failure to pay; the severity of the risks to or losses of the consumer, which may take into account the number of products or services sold or

[38] *See* 12 U.S.C. § 5562(a)(1) (2014).

[39] *See id.* § 5562(b)(1) (2014).

[40] *See id.* § 5562(c)(1) (2014).

[41] *See id.* § 5562(d)(1) (2014).

[42] *See id.* § 5562(e)(1) (2014). The district court of the United States must be in a judicial district in which the noncompliant entity "resides, is found, or transacts business." *See id.* § 5562(e)(1) (2014).

[43] *See id.* § 5563(a) (2014). When the CFPB conducts an adjudication proceeding, the relief can take various forms, including the following: "(A) rescission or reformation of contracts; (B) refund of moneys or return of real property; (C) restitution; (D) disgorgement or compensation for unjust enrichment; (E) payment of damages or other monetary relief; (F) public notification regarding the violation, including the costs of notification; (G) limits on the activities or functions of the person; and (H) civil money penalties." *See id.* § 5565(a)(2) (2014).

[44] *See id.* § 5564(a) (2014).

[45] *See id.* § 5564(a) (2014). When the CFPB brings a civil action, the relief that it may seek can take various forms, including the following: "(A) rescission or reformation of contracts; (B) refund of moneys or return of real property; (C) restitution; (D) disgorgement or compensation for unjust enrichment; (E) payment of damages or other monetary relief; (F) public notification regarding the violation, including the costs of notification; (G) limits on the activities or functions of the person; and (H) civil money penalties." *See id.* § 5565(a)(2) (2014).

[46] *See id.* § 5565(c)(2)(A) (2014).

[47] *See id.* § 5565(c)(2) (2014).

provided; the history of previous violations; and such other matters as justice may require."[48] Finally, if the Bureau obtains evidence that suggests that an entity has violated a federal criminal law, the Bureau is obligated to "transmit such evidence to the Attorney General of the United States, who may institute criminal proceedings under appropriate law."[49]

IV. CFPB'S PRIVACY AND CYBERSECURITY GUIDANCE

The connectivity of devices in the digital economy has increased, and with it, the number of opportunities for unauthorized access to and unauthorized possession of consumer financial information has also increased. The CFPB has recognized and responded to the increased risks faced by providers of consumer financial products and services, as well as the consumers that entrust their information to those providers. For example, after online hackers breached Target's computer system and stole credit card and personal information from Target's customers in December 2013, the CFPB responded by publishing an advisory statement to consumers on how to protect themselves after a data breach.[50] In the statement, the CFPB advised consumers to immediately contact their banks or credit card providers if they noticed any suspicious activity, and to contact the CFPB if their credit card providers did not respond to the consumers quickly.[51] Also, in October 2014, the CFPB amended the Gramm-Leach-Bliley Act privacy rules to allow financial institutions to post their annual privacy notices on their websites.[52] These privacy notices must explain to consumers whether and how the financial institutions share the consumers' nonpublic personal information.[53]

Additionally, the CFPB has worked with other federal regulatory agencies to establish guidance on privacy and data security practices. When the CFPB came into existence, it became a member of the Federal Financial Institutions Examination Council (FFIEC), which also includes the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the National Credit Union Administration. The FFIEC coordinates the examination processes of these federal financial regulators, and in recent years has established guidance on privacy and data security practices.[54]

Lastly, on October 18, 2017, the CFPB released a guidance (the "Principles") that is intended to outline the agency's "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[55] The Principles

---

[48] *See id.* § 5565(c)(3) (2014).

[49] *See id.* § 5566 (2014).

[50] *See Watch accounts closely when account data is hacked and report suspicious charges*, CONSUMER FINANCIAL PROTECTION BUREAU, 1–3 (Jan. 2014), *available at* http://files.consumerfinance.gov/f/201401_cfpb_consumer-advisory_card-security.pdf.

[51] *See id.*

[52] Smith, Andrew, *CFPB Final Privacy Notice Rule Will Hurt Consumers*, LAW360 (Oct. 28, 2014), *available at* http://www.law360.com/articles/590340/cfpb-final-privacy-notice-rule-will-hurt-consumers.

[53] *See id.*

[54] *See* Cedarbaum and Alper, *supra* note 7, at 9. For more information about the FFIEC, see the King & Spalding 2017 Federal Financial Institutions Examination Council Whitepaper.

[55] *See Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, CONSUMER FINANCIAL PROTECTION BUREAU (Oct. 18, 2017), *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

set forth nonbinding standards for nine facets of data sharing and aggregation practices, in the hopes of enabling companies to balance the competitive and innovative drives with their obligations to protect consumers' information. The nine facets consist of access, data scope and usability, control and informed consent, authorizing payments, security, access transparency, accuracy, ability to dispute and resolve unauthorized access, and efficient and effective accountability mechanisms.[56] Although the CFPB clarified that the Principles do not establish binding requirements and are not intended as a statement of the CFPB's future enforcement priorities, the Principles are nonetheless aligned with the CFPB's prior actions and guidance indicating that consumers should have control over the data used by firms in the financial services market.

V. CFPB'S CYBERSECURITY ENFORCEMENT EFFORTS

A. Dwolla, Inc.

On March 2, 2016, the CFPB concluded its first unambiguous cybersecurity enforcement action. The enforcement action manifested as a consent order with Dwolla, Inc. The consent order penalized the company for engaging in deceptive acts related to its data security practices.

Dwolla operates a payment network that allows a consumer with a Dwolla account — a user — to transfer money to a merchant or another consumer who also has a Dwolla account. To become a user, a consumer must submit his or her name, address, date of birth, telephone number and Social Security number to Dwolla. Users also have the option to link a bank account to their Dwolla account; to do that, the user must submit a bank account number and routing number. Dwolla stores the sensitive personal information that consumers submit.

The CFPB determined that sections 1053 and 1055 of the Consumer Financial Protection Act gave it jurisdiction to evaluate Dwolla's conduct.[57] According to the CFPB, from January 2011 to March 2014, Dwolla represented to consumers that the company used reasonable and appropriate measures to protect user data from unauthorized access.[58] For example, Dwolla related that it encrypted sensitive user data.[59] Additionally, the company represented that its servers, its data centers and the transactions on its payment network complied with the standards issued by the Payment Card Industry Security Standards Council.[60] The CFPB, however, concluded that Dwolla failed to use reasonable and appropriate measures to protect user data from unauthorized access.[61] Among other things, the CFPB determined that Dwolla specifically failed to:

i. adopt and implement data security policies and procedures reasonable and appropriate for the organization;

---

[56] *Id.* at *3-5.

[57] *See In the Matter of Dwolla, Inc.*, *1 (Mar. 2, 2016), *available at* http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

[58] *See id*. at *5.

[59] *See id.* at *6.

[60] *See id*.

[61] *See id*.

ii. use appropriate measures to identify reasonably foreseeable security risks;

iii. ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks;

iv. use encryption technologies to properly safeguard sensitive consumer information; and

v. practice secure software development, particularly with regard to consumer-facing applications developed at an affiliated website, Dwolla Labs.[62]

Additionally, the CFPB determined that the company's servers, the company's data centers and the transactions on the company's payment network were not compliant with the standards issued by the Payment Card Industry Security Standards Council.

Ultimately, the Bureau concluded that Dwolla's representations and the company's poor data security practices violated 12 U.S.C. §§ 5531(a) and 5536(a)(1)(B) because they "constitute[d] deceptive acts or practices."[63] As a punishment for violating the law, the CFPB fined Dwolla $100,000.[64] In addition to the fine, the CFPB required Dwolla to implement certain measures to increase the security of user data. These measures generally included establishing a more comprehensive data security plan, adopting more robust security policies and procedures, conducting frequent and ongoing audits and assessments of the efficacy of its data security policies, and taking affirmative steps to close any vulnerabilities discovered through such self-auditing process.[65] The consent order states that it will remain in effect for five years.[66]

B. ACICS and PHH

Despite the enforcement authority exercised by the CFPB against Dwolla, its authority to investigate similar matters may be challenged in the future. In 2016, the Bureau argued in its investigation of Accrediting Council for Independent Colleges and Schools (ACICS) that its CIDs should be enforced by the courts with few or no questions asked unless the Bureau's authority is "patently lacking." But U.S. District Court for the District of Columbia Judge Richard Leon disagreed, refusing to order ACICS to comply with the Bureau's CID because its proffered justification was delving into "fields not clearly ceded to them by Congress."[67]

The CFPB appealed the decision, and the D.C. Circuit Court heard oral argument in early February 2017.[68] The CFPB argued that because it has authority to investigate for-profit

[62] *See Dwolla*, *supra* note 60, at *7.

[63] *See id.* at *10.

[64] *See id.* at *16.

[65] *See Dwolla*, *supra* note 60, at *12–13.

[66] *See id*. at *23.

[67] *CFPB v. ACICS*, No. 15-838, at *8 (D.D.C. April 21, 2016), available at https://www.documentcloud.org/documents/2808007-CFPB-ACICS-Opinion.html.

[68] Mishkin, Barbara S., *D.C. Circuit Hears Oral Argument on CFPB Authority to Issue CID to College Accrediting Organization*, CFPB Monitor, Ballard Spahr (February 8, 2017), *available at* https://www.cfpbmonitor.com/2017/02/08/d-c-circuit-hears-oral-argument-on-cfpb-authority-to-issue-cid-to-college-accrediting-organization/.

schools in relation to their lending and financial practices, it also has authority to investigate whether *any* entity has engaged in any unlawful acts relating to *accrediting* such schools. The CFPB emphasized that it may issue a CID to *anyone* who might have information relevant to violations of laws enforceable by the Bureau, even if the CFPB could not enforce those laws against the actual recipient of the CID. In contrast, the attorney for ACICS argued that a for-profit school's lending practices have nothing to do with its accreditation process and, therefore, the CID's focus on conduct "in connection with accrediting for-profit colleges" actually does not implicate any consumer financial laws enforceable by the CFPB.[69] On April 21, 2017, the Court held that enforcement of the CID was not appropriate because the CID "failed to advise ACICS of 'the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation,'"[70] and because the Bureau recognized that it did not have authority under the Consumer Financial Protection Act to issue a CID.[71]

The ACICS case is not the only opportunity the D.C. Circuit Court has had to consider the limits of the CFPB's enforcement authority. In June 2015, CFPB Director Richard Cordray exercised his authority to add a $103 million fine to Administrative Law Judge Cameron Elliot's $6.4 million penalty against PHH, a mortgage lender that allegedly illegally referred consumers to mortgage insurers in exchange for kickbacks. PHH subsequently challenged the director's authority to levy such a fine, petitioning the D.C. Circuit to review the constitutionality of the CFPB's action. In October 2016, the Court vacated the fine against PHH, holding that the CFPB's structure violated Article II of the U.S. Constitution because the CFPB operates as an independent agency headed by a single director.[72] The Court reasoned that this leadership structure (created by the Dodd-Frank Act) violated Article II by constituting, for the first time, an independent agency under a single director who was only removable for cause.[73] According to the Court, this structure made the CFPB director the most powerful person in the United States government, aside from the president.[74] The Court struck down the for-cause provision, making the CFPB director removable at will by the president,[75] and continued that "[t]he CFPB therefore will continue to operate and to perform its many duties, but will do so as an executive agency akin to other executive agencies headed by a single person, such as the Department of Justice and the Department of the Treasury."[76] In February 2017, the Court granted the CFPB's request for rehearing en banc, and oral argument was heard on May 24, 2017.[77]

On January 31, 2018, the Court issued its decision, remanding the case to the CFPB for further proceedings after granting in part, and denying in part, the petition.[78] Citing *Humphrey's*

---

[69] *Id.*

[70] *Consumer Financial Protection Bureau v. Accrediting Council for Independent Colleges and Schools*, No. 16-5174, 854 F.3d 683 at *692 (D.C. Cir. 2018).

[71] *Id.* at *691.

[72] *See PHH Corp., et al. v. Consumer Financial Protection Bureau*, No. 15-1177, 2016 WL 5898801, at *4 (D.C. Cir. 2016).

[73] *Id.* at *11.

[74] *Id.*

[75] *Id.*, at *4.

[76] *Id.,* at *18–22.

[77] Order, *PHH Corp., et al. v. Consumer Financial Protection Bureau*, No. 15-1177 (D.C. Cir. Feb. 16, 2017).

[78] *See PHH Corp., et al. v. Consumer Financial Protection Bureau*, No. 15-1177, 881 F.3d 75, at *77 (D.C. Cir. 2018).

Executor v. United States,[79] the Court held that "federal law providing the Director of the CFPB with a five-year term in office, subject to removal by the President only for 'inefficiency, neglect of duty, or malfeasance in office,' is consistent with the President's constitutional authority."[80] PHH's argument that the single-director leadership structure of the CFPB violated Article II did not persuade the Court, which reasoned that accepting an analysis invalidating any independent agency that does not mirror the structure of the 1935-era FTC would "threaten many, if not all, modern-day independent agencies, perhaps including the FTC itself."[81] Ultimately, the Court determined that the structural design of an agency implicates policy determinations that obliged the Court to defer to Congress in this case.[82]

C. Dodd-Frank Deregulation in 2018

Although the D.C. Circuit Court's decision in *PHH Corp.* bolstered the institutional independence of the CFPB, on May 24, 2018, the president signed into law several deregulatory measures to scale back Dodd-Frank, which could affect the CFPB's enforcement authority, arguably including that which relates to data privacy and cybersecurity. Although not the sweeping legislation proposed by the House in 2017 that would have replaced the CFPB with the "Consumer Law Enforcement Agency" and removed the CFPB's authority to take enforcement actions with respect to unfair, deceptive and abusive practices by depository institutions,[83] this legislation still rolls back several banking regulations.[84] For example, Dodd-Frank had subjected banks with $50 million or more in assets to numerous federal regulations, but now, banks with less than $250 billion in assets are no longer subject to some of the more stringent regulations (i.e., no longer considered "too big to fail"), such as a yearly stress test to determine whether the banks could survive another economic downturn.[85] "Only nine U.S.-chartered commercial bank holding companies would meet the definition, according to data from the Federal Reserve."[86] Also, banks with less than $10 billion in assets are exempt from the "Volcker rule," which restricts banks from using consumer and business deposits for speculative investments.[87]

---

[79] *Id.*; *see also* *Humphrey's Executor v. United States*, 295 U.S. 602, (1935) (affirming the constitutionality of the independence of the Federal Trade Commission and protecting agency leadership from at-will removal by the president).

[80] *PHH Corp., et al. v. Consumer Financial Protection Bureau*, No. 15-1177, 881 F.3d 75, at *84 (D.C. Cir. 2018).

[81] *Id.* at *108.

[82] *See id.* at *109-110.

[83] Financial CHOICE Act of 2017, H.R. 10, 115th Cong. (2017).

[84] Economic Growth, Regulatory Relief, and Consumer Protection Act, S.2155, 115th Cong. (2018), accessible at https://www.congress.gov/bill/115th-congress/senate-bill/2155/text.

[85] *Id.*, *see also* Erica Erner and Renae Merle, *Congress Approves Plan To Roll Back Post-Financial-Crisis Rules For Banks*, The Washington Post (May 22, 2018), available at https://www.washingtonpost.com/business/economy/divided-house-passes-major-bank-deregulation-bill-sends-to-trump/2018/05/22/6f3bb562-5dd2-11e8-a4a4-c070ef53f315_story.html?utm_term=.fbb818cac451.

[86] Erik Sherman, *Congress Just Approved A Bill to Dismantle Part Of The Dodd-Frank Banking Rule*, NBC News (May 23, 2013), accessible at https://www.nbcnews.com/business/economy/congress-just-approved-bill-dismantle-parts-dodd-frank-banking-rule-n876516.

[87] *See* S.2155, *see also* Erik Sherman, *Scaling Back Dodd-Frank Is Just The Beginning Of Trump's Run On Deregulation*, NBC News (May 24, 2018), accessible at https://www.nbcnews.com/business/economy/scaling-back-dodd-frank-just-beginning-trump-s-run-deregulation-n877031.

This legislation has created momentum for financial service companies to seek more deregulation, and "[o]ne of the top three [changes] would involve the way the [CFPB] was set up."[88] The CFPB remains insulated from Congress from a budgetary perspective, as it receives its funding from the Federal Reserve. And its one-director setup, as opposed to a commission, allows the director to wield significant authority. Recently, several companies have filed lawsuits against the CFPB claiming that the CFPB's single-director structure is unconstitutional. On one hand, the Southern District of New York held that the CFPB's structure was unconstitutional and therefore the CFPB lacked certain legal and enforcement authority (unrelated to cybersecurity enforcement).[89] In contrast, the Southern District of Mississippi held that the CFPB's structure was constitutional, citing the *PHH Corp.* decision for support.[90] Both cases are currently on appeal in the Second and Fifth Circuits, respectively.[91] While none of the deregulation-related actions taken to date have impacted the CFPB's regulatory authority concerning cybersecurity, the outcome of these lawsuits theoretically could have a significant effect on the CFPB's ability to enforce cybersecurity issues.

VI. ENFORCEMENT TRENDS AND THE CALL TO STRENGTHEN CFPB OVERSIGHT

During Mick Mulvaney's tenure as director of the CFPB (which lasted from November 2017 until December 2018), he attempted to significantly curtail the CFPB's enforcement authority, and frequently commented he felt "[t]he bureau is far too powerful, and with precious little oversight of its activities."[92] The CFPB's enforcement activity under Mulvaney was a bit uneven, but none of the enforcement actions taken or lawsuits filed on behalf of consumers related to cybersecurity or other privacy matters.[93]

In December 2018, Mulvaney was replaced with Kathy Kraninger. Shortly after her appointment, Kraninger stated, "[W]here there are bad actors we absolutely will take the

---

[88] *See* Sherman, *supra* note 87.

[89] *CFPB v. RD Legal Funding*, *LLC*, No. 1:17-cv-008900LAP (S.D. N.Y. Sept. 12, 2018), accessible at https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2018/09/Document-105-Order-17v890.pdf.

[90] *CFPB v. All American Check Cashing, Inc., et al*., No. 3:16-cv-00356-WHB-JCG (S.D. Miss. March 21, 2018), accessible at https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2018/04/USDC-SDMS-Order-denying-judgment-on-pleadings.pdf.

[91] *See* Ballard Spahr LLP, *Fifth Circuit Hears Oral Argument In All American Check Cashing*, JD SUPRA (March 18, 2019), accessible at https://www.jdsupra.com/legalnews/fifth-circuit-hears-oral-argument-in-71395/; *see also* Alan Kaplinsky, *CFPB Files Appeal With Second Circuit In RD Legal Funding Case*, Ballard Spahr LLP (Sept. 17, 2018), accessible at https://www.consumerfinancemonitor.com/2018/09/17/cfpb-files-appeal-with-second-circuit-in-rd-legal-funding-case/.

[92] *See* Flitter, Emily and Thrush, Glenn, *Wells Fargo Said to Be Target of $1 Billion U.S. Fine*, The New York Times (April 19, 2018), *available at* https://www.nytimes.com/2018/04/19/business/wells-fargo-cfpb-penalty.html.

[93] After seven months under Mulvaney's leadership, the CFPB had issued just one enforcement action, which imposed a $1 billion fine on Wells Fargo pursuant to a settlement agreement between the CFPB, the Office of the Comptroller of the Currency and the bank. *See* Flitter and Thrush, *supra* note 92. But in June 2018, the CFPB seemingly kicked its enforcement into high gear, actively pursuing the 50 lawsuits and probes that Mulvaney inherited from the previous director and attempting to "clear cases so the agency can move forward with new enforcement actions." Kate Berry, *In A Twist, Mulvaney Now Defending CFPB Enforcement Powers*, American Banker (July 25, 2018), accessible at https://www.americanbanker.com/news/in-a-twist-mulvaney-now-defending-cfpb-enforcement-powers. In June and July 2018 alone, the CFPB permanently barred a payday loan debt collector from working in the industry and fined an Alabama small-dollar lender over excess interest charges; Citibank agreed to give $335 million in refunds to consumers for miscalculating credit card rates; and Security Finance, a South Carolina installment lender, was fined $5 million for illegal debt collection practices.

enforcement actions to the full extent of the law and make sure we are protecting consumers."[94] But Kraninger has been criticized for the lack of CFPB enforcement actions since the beginning of her tenure. In multiple hearings in March 2019 before the House and Senate, Kraninger was criticized for the number of CFPB enforcement actions in 2018-2019 against lenders who scammed students or minorities: zero.[95] Additionally, in March 2019, the Government Accountability Office (GAO) testified before Congress that the CFPB's oversight of credit reporting agencies (CRAs) was lacking, particularly regarding the data privacy and security practices of CRAs.[96] The GAO recommended that the CFPB (1) identify additional sources of information on larger CRAs and (2) reassess its prioritization of examinations to address CRA data security.[97] Specifically, the GAO recommended that the CFPB require CRAs "to register with it, subject to a rulemaking process and cost-benefit analysis of the burden it could impose on the industry," and "routinely consider factors that could inform the extent of CRA data security risk such as the number of consumers that could be affected by a data security incident and the nature of potential harm resulting from the loss or exposure of information."[98] In response to the GAO's recommendations, the CFPB told the GAO that it "cannot examine for or enforce compliance with the data security standards in provisions of GLBA and FCRA or FTC's implementing rules, even at larger participant CRAs," and that the CFPB "has not reassessed" how to incorporate data security risks in its examinations.[99]

VII. CONCLUSION

Despite recent leadership shake-ups and challenges to its enforcement authority, the CFPB retains the potential to become a powerful regulatory force in the cybersecurity and privacy space. This is due to its expansive authority to make determinations of law and to create regulations relating to consumer financial data, and its significant ability to penalize violations. The consent order against Dwolla, Inc., is the first example of how the CFPB intends to use its authority and assess such penalties. That said, since the appointments of Mulvaney and Kraninger, the CFPB's willingness to exercise its authority and enforce penalties for violations of privacy and cybersecurity laws and regulations appears to have been tempered, at least for the short term. Companies under the CFPB's regulatory authority — particularly CRAs — should carefully follow developments relating to the CFPB's plans to potentially change its examination and enforcement approach concerning data privacy and cybersecurity.

---

[94] Jim Puzzanghera, *New CFPB Director Kathy Kraninger Says She Won't Be A Puppet Of Mick Mulvaney*, Los Angeles Times (Dec. 11, 2018), accessible at https://www.latimes.com/business/la-fi-kathy-kraninger-cfpb-20181211-story.html.

[95] Senator Elizabeth Warren, *Senator Warren Questions CFPB Director Kraninger About Lack of Enforcement Action*, Elizabeth Warren (March 12, 2019), accessible at https://www.warren.senate.gov/newsroom/press-releases/senator-warren-questions-cfpb-director-kraninger-about-lack-of-enforcement-action.

[96] United States Government Accountability Office, *Consumer Data Protection: Action Needed To Strengthen Oversight Of Consumer Reporting Agencies*, Subcommittee on Economic and Consumer Policy, Committee on Oversight and Reform, House of Representatives (March 26, 2019), accessible at https://www.gao.gov/assets/700/697893.pdf.

[97] *Id.*

[98] *Id.*

[99] *Id.*