FINTECH LAW REPORT
E-Banking, Payments & Commerce in the Mobile World

May/Jun 2014 ■ Volume 17 ■ Issue 3

The Consumer Financial Protection Bureau as a Privacy & Data Security Regulator

JONATHAN G. CEDARBAUM & ELIJAH ALPER

Jonathan G. Cedarbaum is a Partner in the Government and Regulatory Litigation and Privacy, Information Security, and Communications Groups at WilmerHale. Elijah Alper is a Senior Associate in WilmerHale's Financial Institutions Group. Both are based in WilmerHale's Washington, DC office. Contact: Jonathan.Cedarbaum@wilmerhale.com or Elijah.Alper@wilmerhale.com.

The large-scale data breaches at Target, Neiman Marcus, and eBay are only three of the most visible examples of the growing importance of privacy and data security to the payments system. As firms in the financial sector and the broader payments system—and their vendors—have become more and more dependent on digital methods of storage and transmission of information, protecting that information, from both external attack and internal loss, has increasingly become a high priority of senior management and boards of directors. Regulatory agencies in turn—at the state and federal levels, as well as in other countries—have greatly increased their focus on companies' privacy and data security practices, both as they may affect consumers and as they may influence companies' financial soundness.

Some regulators have developed guidance or standards applying across many sectors of the economy. In October 2011, for example, the Securities and Exchange Commission (SEC) issued guidance alerting all publicly traded corporations that they need to consider cybersecurity incidents in making disclosures about material financial risks in their periodic securities filings.[1] In February 2013, President Obama issued an executive order requiring, among other things, the development of voluntary cybersecurity standards for all elements of the economy deemed to be "critical infrastructure," including the financial system.[2] This February, the National Institute of

CONTINUED ON PAGE 4

Content HIGHLIGHTS

THOMSON REUTERS

41099046

CONTINUED FROM PAGE 1

Standards and Technology (NIST) published the first version of the required standards, providing an important roadmap for all companies to consider in assessing and improving their data security practices.[3] The Federal Trade Commission (FTC) has dramatically stepped up its enforcement efforts concerning companies' privacy and data security policies, pressing to establish data security obligations under its broad authority to police "unfair" trade practices and requesting enhanced rulemaking authority in these domains.[4] In May 2014, to give just one example, the FTC issued a report on data brokers, concluding that these companies operate "with a fundamental lack of transparency" and asking Congress to consider legislation to grant consumers opt-out rights and means to access information about them held by these companies.[5]

Other regulatory efforts have been more sector-specific. In April, for example, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a "Risk Alert" announcing steps being taken by the OCIE to assess cybersecurity preparedness among broker-dealers and investment advisers.[6]

One of the most recent entrants into this rapidly developing domain is the newest federal financial regulator, the Consumer Financial Protection Bureau (CFPB). Created less than four years ago under Title X of the Dodd-Frank Act, the CFPB has rapidly developed wide-ranging regulatory, enforcement, and supervision programs. Concentrating on its core consumer protection mission, the Bureau has so far focused its efforts on laws and rules governing the ways in which the providers of consumer financial products and services subject to its jurisdiction develop, market, and maintain those offerings. The Bureau has only just begun to take its first steps in addressing questions of privacy and data security. But as privacy and data security become ever more important elements of consumer financial products and services, we are likely to see a rapid expansion in the Bureau's attention to data confidentiality and integrity.

This article provides an initial assessment of the CFPB as a privacy and data security regulator. After a brief description of some of the potential threats to privacy and data security facing the consumer financial sector, we describe a number of small steps the CFPB has taken recently to assert its prerogatives as a privacy and data security regulator. We then examine the statutes empowering the CFPB that are most likely to provide the foundation for more extensive CFPB efforts in these areas, and particularly its authority to police unfair, deceptive and abusive practices related to consumer financial products and services. With respect to privacy and data security, the CFPB need not act alone, but may also act as the newest member of the Federal Financial Institutions Examination Council (FFIEC), and so we also note a number of recent FFIEC actions in which the CFPB has joined in addressing new privacy and data security issues. Finally, we describe some of the controversy that has arisen in the past year, particularly in Congress, over the CFPB's own privacy and data security practices.

Some Privacy and Data Security Concerns

Just listing, let alone analyzing, the technological and economic developments pushing privacy and data security to the top of many companies' and regulators' concerns could occupy an entire article. But at least a brief outline of those developments is important to setting the CFPB's activities in context. Three complex and interrelated changes may be captured under the headings of big data, mobility, and "the Internet of things."

By "big data" here, we mean simply the exponential growth over the last 20 years or so in the ability of companies and governments to collect, store, analyze, and exploit collections of data, notably including data on particular individuals. Edward Snowden's revelations about the National Security Agency's surveillance activities have helped make the prospect of this sort of data collection by governments a matter of public debate. But, as the recently released report of the White House task force on big data indicates, the ability to collect and find profitable uses for large collections of information, including particularly personally

identifiable information (PII), has become central to the business models of more and more companies as well.[7] These data collection, retention and analysis capabilities raise concerns both about the privacy of the individuals about whom data has been collected vis-a-vis the entities doing the collecting and about the ability of those entities to protect that data from unauthorized disclosure to third parties.

Sensitive information now has more "mobility" than ever before. Not long ago, digital information resided largely in stationary computers connected, if at all, by wires. Today, mobile devices of many kinds and wireless communications have dramatically expanded the means by and frequency with which digital information is transferred and stored. These changes again raise new challenges for protecting the confidentiality and integrity of the ever larger quantities and types of data being communicated and collected by more and more people, through more and more machines, more and more times per day.

It was the linking together of computers in the Internet that ultimately made possible our increasingly digital economy. In recent years, however, the network of connected devices has exploded beyond computing and communications devices to include more and more machines of all kinds—from cars to copying machines and from industrial control systems to in-home energy controls. By one estimate, the growth of this "Internet of things" will double the number of networked machines over just the next five years from 25 to 50 billion.[8] That growth in connectivity again means more opportunities for innovation, but also for security and privacy vulnerabilities.

Some Initial CFPB Steps

In response to the effects of these changes on providers of consumer financial products and services, the CFPB has begun to take a few first steps into privacy and data security regulation. In the wake of the Target data breach, for example, the CFPB put out a blog post explaining to consumers "[f]our steps you can take if you think your credit or debit card data was hacked" and a more detailed advisory statement on how to respond to data breaches affecting consumer financial information.[9] The CFPB has worked together with other financial regulatory agencies, as described more fully below, on an increasing number of initiatives targeting particular data security threats, the use of social media and cloud computing services by financial institutions, and the privacy considerations involved in combating financial abuse of older individuals.

In May, the Bureau took its first formal action with respect to privacy and data security rules by issuing proposed amendments to the Gramm-Leach-Bliley Act (GLBA) privacy rules, which currently require financial institutions (broadly defined) to mail notices to all of their customers explaining whether and how the institution shares customers' nonpublic personal information.[10] The proposed rule would allow financial institutions to post these notices online rather than mailing them, but only if certain conditions are met.[11] In addition, the CFPB is currently working on proposed revisions to the Home Mortgage Disclosure Act (HMDA) regulations, which, under Dodd-Frank, need to take account of the reporting of additional data elements.[12]

Sources of the CFPB's Privacy and Data Security Authority

These small steps are likely just the beginning. Although to date most public CFPB regulatory and enforcement activity has focused on the terms and processes for offering "core" consumer financial products, such as mortgages and credit cards, the Bureau has considerable authority to regulate privacy and data security matters, should it choose to do so. It can assess civil penalties and take enforcement action against companies, and in some cases against individual executives, if they do not adequately protect the privacy and security of consumer financial data. The sources of the CFPB's authority in this area, as in others, may be placed in two groups: statutory provisions transferred to the CFPB from other agencies and new powers granted in the Dodd-Frank Act.

Inherited Federal Consumer Financial Laws

A key motivation for establishing the CFPB was to centralize regulation and enforcement of federal consumer financial law in a single agency.[13] Before the CFPB, these powers were divided among the many federal banking agencies, the FTC, the Department of Justice, and the Department of Housing and Urban Development.[14] Critics said this division led to uneven supervision and enforcement, and violations by some nonbank actors going undetected or unpunished.[15]

Most, but not all, of this formerly divided authority is now centralized in the CFPB. The Consumer Financial Protection (CFP) Act, enacted as Title X of the Dodd-Frank Act, transferred rulemaking and enforcement authority under a set of 18 "enumerated consumers laws" from various federal agencies to the Bureau.[16] Several of these enumerated consumer laws are particularly relevant to privacy and data security issues, including (*i*) the privacy provisions of the Gramm-Leach-Bliley Act; (*ii*) the Fair Credit Reporting Act (FCRA); and (*iii*) the Electronic Funds Transfer Act (EFTA).

The enumerated consumer laws and their accompanying regulations apply to a range of entities, not just banks or major nonbank financial companies such as mortgage servicers or payday lenders. The Bureau may issue new regulations under these laws, and these rules could also apply to any person to the extent permitted by the underlying statute. Under the FCRA, for example, the CFPB (along with the FTC and in some cases the federal banking agencies) has enforcement authority over credit rating agencies (CRAs), major repositories of consumer financial data, those who furnish this data to CRAs, as well as individuals and companies who obtain this data by requesting consumer credit reports.[17] And, as noted above, under its privacy authority under the Gramm-Leach-Bliley Act, the CFPB has proposed regulations on methods for delivering privacy notices.

The CFPB does *not* have authority over some important provisions relating to identity theft and data security, either because those provisions were carved out of the enumerated consumer laws or because those provisions are unrelated to consumer financial products. Authority over the FCRA's "Red Flags Rules," which require financial institutions to establish guidelines and procedures relating to identity theft, remains with the FTC and the federal banking agencies.[18] And the CFPB also does not have authority over the Gramm-Leach-Bliley Act's "safeguards" rules, which require financial institutions to establish administrative, technical, and physical safeguards to relating to the security and confidentiality of customer information.[19] There too, authority remains with the federal banking agencies and the FTC.

UDAAP

The FTC views data security or privacy breaches as potential violations of Section 5 of the FTC Act, which prohibits "unfair" or "deceptive" acts or practices (UDAP), and the path the FTC has trod may provide a model for the CFPB to follow in exercising its similar power under the CFP Act to take action against unfair, deceptive or abusive practices (UDAAP) by entities within the Bureau's jurisdiction. It remains to be seen whether the FTC's recent efforts to secure judicial approval for a broad reading of its data security enforcement authority under the unfairness prong of Section 5 of the FTC Act may redound to the benefit of the CFPB's authority as well.

The FTC has frequently pursued UDAP enforcement actions for a range of privacy and data security concerns. Since 2013 alone, these have include actions based on allegations that companies inappropriately collected or disclosed private consumer information,[20] did not secure sensitive personal information,[21] made false privacy certification claims,[22] or allowed franchisees to take webcam pictures of consumers in their homes.[23]

Longstanding FTC guidance, adopted by the CFPB, states that a representation, omission, act, or practice is considered deceptive if: (a) there is a representation, omission, or practice that is likely to mislead the consumer; (b) the act or practice would be deceptive from the perspective of a reasonable consumer; and (c) the representation, omission, act, or practice is likely to affect the

consumer's choice or conduct regarding a product or service.[24] In its enforcement actions, the FTC has said that companies can act deceptively if they do not disclose accurately, or at all, how they collect or use personally identifiable information.

An unfair practice is one that (*i*) causes or is likely to cause substantial injury to consumers that is (*ii*) not reasonably avoidable by consumers, when (*iii*) the injury is not outweighed by countervailing benefits to consumers or to competition.[25] The FTC has taken the position that practices permitting the compromise or unauthorized sharing of PII can cause consumers substantial injury, and that consumers often cannot reasonably avoid that injury.[26]

The Bureau also has enforcement authority over unfair or deceptive acts and practices,[27] and the CFP Act grants the Bureau the authority to define and prohibit "abusive" acts and practices as well.[28] Together, this is known as the Bureau's "UDAAP" authority, as compared to the FTC's "UDAP" authority. Unlike the enumerated consumer laws, however, this authority was not transferred from an existing agency but instead is a new grant of power. Therefore, the FTC retains and continues to exercise its existing UDAP authority on privacy and data security matters, and the federal banking agencies retain their UDAP authority over banks.[29] The CFP Act also grants the Bureau authority to define UDAAP through rulemaking, under the same procedures as it might promulgate any other regulations.[30]

While the CFPB's enforcement authority over enumerated consumer laws can apply to any person covered by those laws, its UDAAP authority is limited to consumer financial products and services. The Bureau may use its enforcement authority to prevent any "covered person" or "service provider" from engaging in a UDAAP, but only "in connection with a consumer financial product or service,"[31] and its rulemaking authority is subject to the same limitations.[32]

A "covered person" is a person or institution that offers or provides a "consumer financial product in service,"[33] which is any of a list of products and services, including (with many exceptions) extensions of credit, mortgages, money transmission or exchange, issuing stored value products, payment processors, check cashing, credit reporting, and debt collection.[34] A "covered person" also includes any "related person," which is an individual who has managerial responsibility, controlling shareholder authority, or is otherwise "materially involved" in the management of a person within the Bureau's jurisdiction.[35] The term "related person" also captures independent contractors who knowingly or recklessly violate the law or otherwise breach fiduciary duty.[36] A "service provider" is any entity that "provides a material service to" a covered person, subject to limited exceptions.[37]

While the CFPB's UDAAP authority applies to the limited class of "covered" persons, the Bureau also has the power to declare acts or practices by covered persons "abusive," and it may use this power in privacy and data security enforcement. The CFP Act allows the Bureau to declare an act or practice "abusive" if it is in connection with a consumer financial product or service and it:

(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

(2) takes unreasonable advantage of—
   (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
   (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
   (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.[38]

The CFPB has issued little guidance on how it will interpret the "abusive" standard,[39] and as of early 2014 the CFPB has declared only a few acts or practices "abusive," none of them relating to privacy or data security issues.[40] But it is possible the Bureau could interpret the statutory definition of "abusive" to cover particularly egregious privacy or data security failings.

The CFPB has broad enforcement powers should it find a violation of UDAAP or federal consumer financial law. The Bureau can bring an enforcement action against any "covered person"

(including related persons) or "service provider" that violates the UDAAP prohibition or any "person" that violates a federal consumer financial law.[41] It can not only use any remedies authorized by the individual enumerated consumer laws, but may also order "any appropriate legal or equitable relief" including, among other remedies, rescission of contracts, restitution, disgorgement, and civil money penalties.[42] Finally, the Bureau has its choice of methods to obtain enforcement relief. Against covered persons and service providers, it can issue cease-and-desist orders or obtain consent orders in settlement of those proceedings.[43] And for both covered and non-covered persons, the Bureau has the discretion to proceed in federal district court or through its own administrative procedure process.[44]

Differences Between CFPB & FTC Authority

The CFPB's authority differs from that provided to the FTC in important ways. These differences limit potential CFPB targets but increase the Bureau's powers with respect to those targets.

While the FTC's UDAP authority consists of a broad grant over persons in general, with limited carve-outs,[45] the Bureau's UDAAP authority consists of a grant to a limited class of "covered persons" or "service providers," as described above. The Bureau has no UDAAP authority over covered persons or service providers for activities unrelated to consumer financial products or services. This means the Bureau could not have pursued many of the particular privacy and data security enforcement cases undertaken by the FTC recently, such as those against smartphone maker HTC or Fantage.com, an online multiplayer children's game, because those companies' products and services are not related to consumer financial products or services.[46] But the Bureau will likely concentrate its UDAAP authority on institutions exempted from FTC jurisdiction, such as banks and credit unions within the Bureau's jurisdiction, 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.[47]

While many companies and non-financial activities may be outside the Bureau's UDAAP reach, for those in its jurisdiction the Bureau has more rulemaking and enforcement tools than does the FTC. The Bureau can promulgate UDAAP regulations under standard administrative notice-and-comment procedures. By contrast, the FTC's UDAP 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.[48] The Bureau's enforcement authority exceeds that available to the FTC for UDAP violations. The CFPB can assess civil money penalties for any UDAAP violation, while the FTC can assess penalties only for violations of its cease-and-desist orders.[49]

Finally, the Bureau has more powerful tools to uncover potential privacy and data security violations by covered persons, either under UDAAP or any other statute within its jurisdiction. The CFP Act granted the Bureau examination authority over banks with more than $10 billion in assets, their affiliates (including nonbank affiliates), nonbank mortgage companies, private student lenders, payday lenders, and "larger participants" in the consumer financial market, as defined by rulemaking.[50] Thus far, the Bureau has identified "larger participants" among student loan services, debt collection companies, and credit reporting agencies.[51] This examination authority is comprehensive, mirroring the federal banking agencies' authority over the banks they regulate. The Bureau can conduct detailed, on-site examinations and has asserted access to all records of the covered institutions,[52] including privileged materials.[53] Thus while the FTC must rely on the subpoena or civil investigative demand process to obtain relevant information, the CFPB can simply demand it, even if privileged, if the target falls within its supervisory jurisdiction.

The scope of the CFPB's privacy and data security authorities remain largely untested. Even the FTC, with its much more established track record, is just now pressing for judicial establishment of

its authority to use the unfairness as well as the deceptiveness prong of Section 5 of the FTC Act to pursue data security cases. In the LabMD and Wyndham hotels cases, it has gained the approval of two district court judges. Whether that approval will survive scrutiny by higher courts remains to be seen. The CFPB's authority in this area is also open to potential attack in ways unavailable to the defendants in *Wyndham Hotels*. For example, potential targets of CFPB enforcement could argue that Congress' decision to carve out the FCRA Red Flags Rules and the GLBA Safeguards Rules from CFPB jurisdiction, both of which govern data security, shows Congress's intention that the CFPB not have authority in this area.

The extent to which the FTC's delimitation of its UDAP powers as applied to privacy and data security will carry over to the CFPB's UDAAP authority also remains to be determined, both by the CFPB and by the courts. As data confidentiality and integrity become increasingly important concerns in the provision of consumer financial products and services, though, we can expect the CFPB to make greater efforts to exercise, and thus give shape to, these powers in the years to come.

The CFPB as Member of the FFIEC

The CFPB need not act alone in addressing data security and privacy issues. Upon its creation, it became a member of the Federal Financial Institutions Examination Council (FFIEC), along with the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve System, and National Credit Union Administration (NCUA). The FFIEC serves as a coordinating council for federal financial regulators to make their examination processes as consistent as possible. While the FFIEC has, through its IT Examination Handbook, established guidance on privacy and data security practices of regulated financial institutions for many years, since the CFPB joined the FFIEC the FFIEC has taken a number of steps reflecting its member agencies' heightened concerns with these issues. In July 2012, for example, the FFIEC issued a statement on financial institutions' use of cloud computing services.[54] Later in 2012 and in 2013, the FFIEC revised portions of its IT Examination Handbook dealing with data security. In the summer of 2013, the FFIEC established a separate committee devoted to cybersecurity and critical infrastructure protection. And in the past year, it has put out a series of statements addressing particular data security threats to financial firms.[55]

Perhaps the most consumer-focused of these FFIEC initiatives, and thus the one arguably most related to the CFPB's core mission, was the release in December 2013 of guidance on financial institutions' use of social media.[56] The guidance sets out a risk management framework for regulated entities to assess and mitigate legal, operational, and reputational risks created or heightened by their use of social media as a means of communicating with customers. It notes that privacy and data security requirements, such as those under the Gramm-Leach-Bliley Act and its implementing regulations and under the Children's' Online Privacy Protection Act, need to be translated into the context of social media. Moreover, the guidance notes that:

> **Even when a financial institution complies with applicable privacy laws in its social media activities, it should consider the potential reaction by the public to any use of consumer information via social media. The financial institution should have procedures to address risks from occurrences such as members of the public posting confidential or sensitive information—for example, account numbers—on the financial institution's social media page or site.[57]**

The FFIEC's increased attention to data confidentiality and integrity can be expected to continue for the foreseeable future, and the CFPB will likely play a particularly influential role in shaping FFIEC initiatives with respect to communications with consumers about financial products and services.[58]

Controversy Over the CFPB's Own Privacy and Data Security Practices

Even as financial regulators such as the CFPB have been increasing their scrutiny of the ways in which private institutions guard the privacy and integrity of consumer financial information, financial regulators' own data security and privacy practices have been subjected to closer examination as well. To take one example, the same day that the SEC's OCIE released detailed guidelines for examining the cybersecurity practices of securities firms, the Government Accountability Office (GAO), Congress's all-purpose auditor of executive branch agencies, released its own less-than-entirely flattering assessment of the SEC's information security practices.[59] The CFPB's own privacy and data security track record has also become a target of GAO and congressional scrutiny in recent months.

As part of its regular auditing of the CFPB's annual financial statements, the GAO criticized the CFPB in 2012 for not having developed an information security program meeting all the requirements of the Federal Information Security Management Act (FISMA), the statute establishing federal agencies' data security obligations.[60] Picking up on that assessment and perhaps unhappy about some of the CFPB's demands for large volumes of data from regulated parties, the U.S. Chamber of Commerce and other groups in 2013 released letters or studies suggesting that the CFPB's data collection practices exceeded its statutory authority.[61] In July 2013, Senator Mike Crapo, (R-ID), ranking member of the Senate Banking Committee, asked GAO to investigate whether the CFPB's data collection practices were authorized and consistent with the Dodd-Frank Act's restrictions on gathering of consumers' PII.[62] The GAO has agreed to undertake the study. CFPB officials have repeatedly defended the propriety of their data collection efforts.[63] The GAO study is expected later this year.

Conclusion

As regulatory agencies go, the CFPB is still in its infancy. Its regulatory program is just unfolding, and the contours of its supervision and enforcement powers are still being defined. With respect to privacy and data security in particular, it has just begun to take steps to make itself a player on the regulatory field. The scope of the Bureau's statutory powers, particularly its UDAAP authority, and the growing significance of privacy and data security to the consumer financial sector, however, suggest that we can expect increasing attention by the Bureau to the privacy and data security practices of the companies within its jurisdiction in years to come.

NOTES

1. The SEC guidance is available here: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
2. Executive Order 13,636 is available here: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
3. Version 1.0 of the NIST Cybersecurity Framework is available here: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
4. The lead test case concerning the FTC's data security authority under the unfairness prong of section 5 of the FTC Act is *FTC v. Wyndham Hotels*, Order and Opinion Denying Motion to Dismiss, No. 13-1887 (D. N.J. Apr. 7, 2014) (hereafter "Wyndham Hotels"). In June, the Wyndham district court certified Wyndham's petition for an interlocutory appeal of the FTC authority issue. The Third Circuit has discretion over whether to hear the appeal. For the FTC's desire for additional rulemaking authority, see, e.g., Prepared Statement of the FTC on Data Breach on the Rise: Protecting Personal Information from Harm, before the Senate Committee on Homeland Security and Governmental Affairs (Apr. 2, 2014), *available at*: http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.
5. FTC, Data Brokers: A Call for Transparency and Accountability (May 27, 2014), available here: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
6. The OCIE Risk Alert is available here: http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf. For an initial assessment, see http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179872201.
7. Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

8. Dale Evans, The Internet of Things: How the Next Evolution of the Internet is Changing Everything, *Cisco White Paper* (Apr. 2011), at 3 (predicting "there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020").
9. The blog post, put out on Jan. 27, 2014, can be found here: http://www.consumerfinance.gov/blog/four-steps-you-can-take-if-you-think-your-credit-or-debit-card-data-was-hacked/. The consumer advisory is here: http://files.consumerfinance.gov/f/201401_cfpb_consumer-advisory_card-security.pdf.
10. CFPB, Notice of Proposed Rulemaking: Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act, 79 Fed. Reg. 27214 (May 13, 2014).
11. *Id.* at 27216.
12. *See* CFPB Rulemaking Agenda (Jul. 3, 2013), *available at* http://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3170&Image58.x=58&Image58.y=5&Image58=Submit.
13. *See, e.g.*, About Us: Creating the Consumer Bureau, at http://www.consumerfinance.gov/the-bureau/creatingthebureau/.
14. For example, rulemaking under the Truth in Lending Act was split between the Federal Reserve and FTC, see, *e.g.*, 15 U.S.C. §§ 1603(a), 1632(d)(5); rulemaking under the Real Estate Settlement Procedures Act was conducted by HUD, see, e.g., 12 U.S.C. §§ 2605(j), 2607(d); and the federal banking agencies asserted enforcement jurisdiction for each of these laws over the banks they regulate, see 12 U.S.C. § 1818(i) (granting the agencies the authority to assess penalties for any violation of law).
15. *See, e.g.*, Elizabeth Warren, Unsafe at Any Rate, *Democracy*, (Summer 2007) (stating that the "splintered regulatory framework has created regulatory loopholes and timid regulators").
16. *See* 12 U.S.C. 5581(c)(2) (transferring enforcement authority from prudential regulators to the CFPB). Congress later granted the Bureau authority over the Military Lending Act as well. See National Defense Authorization Act for Fiscal Year 2013 § 661.
17. *See* 15 U.S.C. § 1681s (describing FTC and CFPB authority over the FCRA); 12 U.S.C. § 5564 (authorizing the Bureau to commence civil actions against "any person" who violations a Federal consumer financial law).
18. 12 U.S.C. § 5481(12)(F) (including as an "enumerated consumer law" the "Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), except with respect to sections 615(e) and 628 of that Act (15 U.S.C. 1681m(e), 1681w)").
19. *Id.* at § 5481(12)(J) (including as an "enumerated consumer law "sections 502 through 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802-6809) except for section 505 as it applies to section 501(b))").
20. *E.g.*, FTC Approves Final Order Settling Charges Against Flashlight App Creator (Apr. 9, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app; FTC Approves Final Order Settling Charges Against Compete, Inc. (Feb. 25, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/02/ftc-approves-final-order-settling-charges-against-compete-inc.
21. Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers; Accretive Health Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Dec. 31, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/accretive-health-settles-ftc-charges-it-failed-adequately-protect; FTC Approves Final Order Settling Charges Against HTC America Inc. (Jul. 2, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/07/ftc-approves-final-order-settling-charges-against-htc-america-inc.
22. FTC Settles with Children's Gaming Company For Falsely Claiming To Comply With International Safe Harbor Privacy Framework (Feb. 11, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-settles-childrens-gaming-company-falsely-claiming-comply.
23. Aaron's Rent-To-Own Chain Settles FTC Charges That it Enabled Computer Spying by Franchisees (Oct. 22, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.
24. *See* CFPB Supervision and Examination Manual (Oct. 2012) (CFPB Manual) at UDAAP 5.
25. *Id.* at UDAAP 1-2.
26. See supra notes 18-19.
27. See 12 U.S.C. §§ 5531(a), 5536.
28. See *id.* § 5531(d) (defining types of acts or practices that could be defined as "abusive").
29. See *id.* § 5581(b)(5)(C) ("No provision of this title shall be construed as modifying, limiting, or otherwise affecting the authority of the Federal Trade Commission (including its authority with respect to affiliates [of large banks] under the Federal Trade Commission Act or any other law, other than the authority under an enumerated consumer law to prescribe rules, issue official guidelines, or conduct a study or issue a report mandated under such law.").
30. 12 U.S.C. § 5531(b) ("The Bureau may prescribe rules applicable to a covered person or service provider identifying as unlawful unfair, deceptive, or abusive acts or practices . . . .").

31. 12 U.S.C. § 5531(a).
32. 12 U.S.C. § 5531(b).
33. 12 U.S.C. § 5481(6).
34. 12 U.S.C. § 5481 1002(5) & (15).
35. 12 U.S.C. § 5481 1002(25).
36. *Id.*
37. 12 U.S.C. § 5481 1002 (26).
38. 12 U.S.C. § 5531(d).
39. The CFPB Examination Manual merely restates the statutory test provided in the CFP Act. See CFPB Examination Manual at UDAAP.
40. The CFPB has identified two practices that it believes qualify as abusive: (1) enrolling consumers in a debt relief program the company knows the consumers could not complete, see *CFPB v. Amer. Debt Settlement Solutions*, Stipulated Final Judgment, No. 9:13-cv-80548-DM M (S.D. Fla. Jun. 7, 2013); and (2) collecting on loans that were void under state law (*e.g.*, due to usury caps or licensing requirements), see *CFPB v. CashCall, Inc. et al*, Compliant, No. 1:13-cv-13167 (D. Mass. Dec. 16, 2013).
41. 12 U.S.C. §§ 5563-5564.
42. *Id.* § 5565.
43. 12 U.S.C. § 5563(b).
44. 12 U.S.C. §§ 5563 (administrative authority), 5564 (litigation authority).
45. *See* 15 U.S.C. §§ 44, 45 (granting FTC UDAP authority over "persons, partnerships, or corporations" and excepting non-profit corporations, banks, common carriers, and other specific entity types).
46. See *supra* note 19-21. The FTC's most recent Privacy and Data Security Update can be found at http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.
47. For example, in November 2013, the CFPB released an advanced notice of proposed rulemaking for debt collection that requested information on "[w]hat privacy and data security concerns [the Bureau should] consider when owners of debts provide, or debt buyers and third-party collectors obtain, access to documentation and information when a debt is sold or placed for collection." The ANPRM is available here: https://www.federalregister.gov/articles/2013/11/12/2013-26875/debt-collection-regulation-f.
48. *See* Pub. L. 93-637, 15 U.S.C. § 2301 et seq. (1975).
49. 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").
50. *See* 12 U.S.C. §§ 5514 (authority over certain nonbanks), 5515 (authority over large banks and their affiliates).
51. As an example, the CFPB's rule defining larger participants in the consumer reporting market became effective September 30, 2012 and can be found here: http://files.consumerfinance.gov/f/201207_cfpb_final-rule_defining-larger-participants-consumer-reporting.pdf.
52. For example, the Bureau's examination manual for FCRA compliance directs examiners to assess an institution's policies and practices regarding information sharing and identity theft protections. *See* CFPB Manual at FCRA 4, 57, *et al.*
53. *See* CFPB Bulletin 12-01 (November 2012) (requiring supervised institutions to "provide all documents and other information" responsive to a Bureau request and prohibiting them from "selectively withhold[ing] responsive documents based on their judgment that such materials are not necessary to the Bureau's execution of its responsibilities or that other materials would be sufficient to suit the Bureau's needs"). The bulletin also asserts that entities "must comply" with Bureau requests for privileged information.
54. The cloud computing statement can be found here: http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.
55. These statements can be found here: http://ithandbook.ffiec.gov/reference-materials.aspx.
56. See Social Media: Consumer Compliance Risk Management Guidance, 78 Fed. Reg. 76297 (Dec. 17, 2013).
57. *Id.* at 76304.
58. For another joint effort, involving not only the FFIEC agencies, but also the SEC and FTC, see the Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Americans (Sept. xx, 2013), *available at* http://files.consumerfinance.gov/f/201309_cfpb_elder-abuse-guidance.pdf.
59. See GAO, Information Security: SEC Needs to Improve Controls over Financial Systems and Data (Apr. 17, 2014).
60. See GAO, Management Report: Opportunities for Improving the Bureau of Consumer Financial Protection's Internal Controls and Accounting Procedures 7-9 (May 21, 2012).
61. For the U.S. Chamber of Commerce's concerns, see: http://www.centerforcapitalmarkets.com/wp-content/uploads/2010/04/2013-6-19-CFPB-letter-on-data-collection.pdf.
62. Senator Crapo's letter is available here: http://www.crapo.senate.gov/issues/banking/documents/CrapoGAORequestre.CFPBData.pdf.
63. See, *e.g.*, Testimony of Richard Cordray, House Comm. On Fin. Servs., (Jan. 28, 2014) (stating that the Bureau makes "every effort" to apply privacy and security safeguards to the data it collects).