
**Statement of Andrew M. Smith**
**Partner, Covington & Burling LLP**
**On Behalf of the Consumer Data Industry Association**

**Committee on Banking, Housing, and Urban Affairs**
**United States Senate**
**Hearing on "Consumer Data Security and Credit Bureaus"**

**October 17, 2017**

Chairman Crapo, Ranking Member Brown, and members of the Committee, thank you for the opportunity to appear before you. My name is Andrew Smith, and I am a partner at the law firm Covington & Burling LLP, where I co-chair the Financial Institutions Practice Group. I also serve as the Chair of the Consumer Financial Services Committee of the American Bar Association, and I am a Fellow of the American College of Consumer Financial Services Lawyers. Earlier in my career, I worked at the Federal Trade Commission ("FTC"), where I was in charge of the FTC's credit reporting program.

I am appearing today on behalf of the Consumer Data Industry Association.

CDIA is an international trade association with over 140 corporate members – including the three nationwide credit bureaus – that educates policymakers, consumers, and others on the benefits of using consumer data responsibly. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. CDIA member products are used in more than nine billion transactions each year and expand consumers' access to financial services in a manner that is innovative and focused on their

needs. We commend you for holding this hearing, and welcome the opportunity to share our views.

Today, I want to focus on three key points:

- The American credit reporting system provides critically important benefits to consumers and is indispensable to the economy.
- Nationwide credit reporting companies must comply with robust data security standards, because of the direct requirements of federal and state law, but also because of obligations imposed on credit reporting companies by their customers, such as banks who are required by their prudential regulators to audit the data security of their vendors.
- Beyond these data security requirements, credit reporting companies are subject to a pervasive regulatory and supervisory scheme that effectively protects both consumers and the economy, and has persisted for nearly fifty years.

**The National Credit Reporting System**

The national credit reporting system is vital to the health of the economy and to maintaining consumer access to credit. More than two-thirds of U.S. gross domestic product comes from consumer spending, a fact that depends in large part on consumer access to affordable credit. In turn, access to credit on reasonable terms makes it affordable for consumers to make important purchases, such as a home or a car, or even a smartphone.

The credit reporting system is so central to the modern American economy that it can be easy to miss its benefits. For example, today we would never imagine that a cross-country

move might make it difficult or even impossible to rent an apartment, get utilities connected, or obtain a bank account. But before the development of the modern system, moving to a new city potentially meant losing access to critical services and benefits. Without ready access to a consumer report, lenders, landlords, community banks, credit unions, insurance companies, and others had no assurance that you were conscientious and reliable, unless they knew you personally. As Consumer Financial Protection Bureau ("CFPB") Director Richard Cordray has stated,

> Without credit reporting, consumers would not be able to get credit except from those who have already had direct experience with them, for example from local merchants who know whether or not they regularly pay their bills. This was the case fifty or a hundred years ago with "store credit," or when consumers really only had the option of going to their local bank. But now, consumers can instantly access credit because lenders everywhere can look to credit scores to provide a uniform benchmark for assessing risk.[1]

The modern credit reporting system has made it possible for many middle-class consumers to get credit at rates that previously would have been reserved for the wealthy. Now, even those of modest means who have shown themselves to be diligent and conscientious with their money can get affordable credit quickly and with a minimum of effort. Furthermore, in recent years, many credit reporting companies have developed tools to provide lenders with information on the unbanked and other consumers without the type of records that typically

---

[1] Richard Cordray, CFPB, Prepared Remarks by Richard Cordray on Credit Reporting (Jul. 16, 2012), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-by-richard-cordray-on-credit-reporting/.

make up a traditional credit report. These tools allow more consumers to access traditional loans and bank products.

Our credit reporting system today is the envy of the world. It is a key reason why we have such a diverse base of lenders, in contrast to the financial systems of other developed nations. Our system also provides a disproportionate benefit to smaller financial institutions like community banks and credit unions, who have access to accurate and complete data on par with what very large banks have access to. Our financial system works because companies share critical information across the system to benefit everyone.

Ultimately, credit reports tell the story of our good choices and hard work. They speak for us as consumers when we apply for loans and lenders don't know who we are or if we've paid our bills in the past. Further, credit reports are a check on human bias and assumptions that provide lenders with a foundation of facts that tell our story and contribute to equitable treatment for consumers. CDIA members work to act in the best interests of consumers – by ensuring the accuracy and completeness of data in consumer reports, and by providing businesses with the information that they need to ensure consumers are treated fairly.

**Data Security Requirements for Credit Reporting Companies**

We understand that the Committee is particularly interested in understanding the data security requirements and standards that apply to credit reporting companies and the steps these companies take to protect consumer data. Under federal, state, and private contractual frameworks, credit reporting companies are required to protect the sensitive consumer information that they possess, such as by developing, maintaining, and testing the effectiveness

of comprehensive information security programs. These existing frameworks combine to form a robust and comprehensive set of cyber standards that protect the data collected, maintained, and transmitted by credit reporting companies.

The Gramm-Leach-Bliley Act & FTC Safeguards Rule

Credit reporting companies are financial institutions subject to the information security requirements of the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulation, the Standards for Safeguarding Customer Information ("Safeguards Rule") promulgated by the FTC.[2] The Safeguards Rule imposes specific standards designed to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer.[3]

The Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program" that includes appropriate

---

[2] 15 U.S.C. § 6801; 16 C.F.R. pt. 314. The Safeguards Rule applies to financial institutions within the FTC's jurisdiction, which includes credit reporting companies. The federal prudential banking regulators – *i.e.*, the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation – have promulgated similar information security guidance that applies to the financial institutions under their supervision. *See* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, App. B (interagency guidelines as promulgated by the OCC); 12 C.F.R. pt. 208, App. D-2 (as promulgated by the Federal Reserve); 12 C.F.R. pt. 364, App. B (as promulgated by the FDIC) .

[3] 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).

administrative, technical, and physical safeguards to achieve these objectives.[4] This program is required to be tailored to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.[5]

In addition, a financial institution must designate an employee to coordinate the program; identify reasonably foreseeable risks to the security of the information and assess the sufficiency of safeguards; and design, implement, and regularly test safeguards to protect against such risks.[6] Finally, the Safeguards Rule obligates financial institutions to oversee their service providers' cybersecurity practices, both by taking reasonable steps to ensure the institutions only deal with service providers that employ strong security practices, and by entering into contracts with such providers that require them to implement appropriate safeguards.[7]

The FTC Act

Credit reporting companies are also subject to jurisdiction over cybersecurity matters asserted by the FTC under Section 5 of the FTC Act.[8] Pursuant to this statute, the FTC is empowered to take action against any business that engages in "unfair or deceptive acts or

---

4 16 C.F.R. § 314.3(a).
5 *See id.*
6 16 C.F.R. § 314.4.
7 16 C.F.R. § 314.4(d).
8 15 U.S.C. § 45.

practices" ("UDAP"), which the agency has interpreted to include inadequate data security practices.[9]

The FTC requires that a company employ safeguards for data that are "reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[10] While specific cybersecurity requirements under Section 5 are not codified, the FTC has issued detailed guidance that explains what it considers to be reasonable cybersecurity safeguards. These include practices such as encryption, use of firewalls, use of breach detection systems, maintaining physical security of objects that contain sensitive information, and training employees to protect such information.[11] In addition to issuing detailed guidance, the FTC zealously enforces these standards, having brought over 60 cases since 2002 against businesses for putting consumer data at "unreasonable risk."[12]

Fair Credit Reporting Act: Credentialing and Disposal Requirements

The Fair Credit Reporting Act ("FCRA") requires that credit reporting companies only provide credit reports to people with a permissible purpose to receive such reports, such as

---

9 *See id.*; *see also* Cong. Res. Serv., The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority (Sept. 11, 2014), https://fas.org/sgp/crs/misc/R43723.pdf.

10 Fed. Trade Comm'n, Data Security (accessed Dec. 15, 2016), https://www.ftc.gov/datasecurity.

11 *See, e.g.*, Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

12 *See* Fed. Trade Comm'n, Privacy and Data Security Update – 2016 (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

credit or insurance underwriting. More importantly, the law requires that every credit reporting company maintain reasonable procedures designed to ensure that credit reports are provided only to legitimate people for legitimate purposes. These procedures must require that prospective users of credit reports identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. The FTC has brought numerous actions over the years seeking to enforce these provisions, most notably against ChoicePoint, which was alleged to have unwittingly sold credit reports to a ring of identity thieves. In the ChoicePoint case, the FTC collected millions of dollars in consumer redress and civil penalties, including a $10 million civil penalty in connection with the unauthorized disclosure of "nearly 10,000 credit reports," which were allegedly sold by ChoicePoint to persons without a permissible purpose.[13]

The nationwide credit bureaus, and credit reporting companies generally, take these "credentialing" responsibilities very seriously. In addition, the nationwide credit bureaus have been examined by the CFPB with respect to the strength and resiliency of their credentialing procedures. As a part of their credentialing procedures, credit reporting companies maintain detailed written procedures which take into account the risks presented by prospective users and their proposed uses of data. These procedures routinely include:

---

[13] *See* Fed. Trade Comm'n., ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

- site visits to ensure the premises are consistent with the stated business of the prospective customer;
- review of public information sources and public filings to confirm licensure and good standing;
- review of company websites and other public-facing materials;
- checking financial references, including credit reports of owners for certain types of companies, such as those that are not publicly traded;
- specific and detailed contractual representations and warranties, as well as specific certifications, that credit report information will be used only for specified purposes;
- detailed customer on-boarding and training procedures; and
- ongoing monitoring of customers – including transaction testing – to ensure that customers are in fact using credit reports for legitimate and permissible purposes.

In addition to these credentialing requirements, the FCRA prohibits credit reporting companies – and anyone else handling credit report information – from disposing of that information in a manner that is not secure.[14] More specifically, the FTC has made a rule providing that a person who maintains or otherwise possesses credit report information, or information derived from credit reports, must properly dispose of such information by taking reasonable measures to protect against the unauthorized access to or use of the information in connection with its disposal.[15]

---

14 *See* FCRA § 628.

15 *See* 16 C.F.R. § 682.3.

State Law – State Attorney General Enforcement & Breach Notification

In addition to these federal regulatory frameworks, credit reporting companies also have numerous data security obligations under state law. First, credit reporting companies may be subject to data security enforcement of state "mini-FTC Acts" that prohibit unfair or deceptive acts or practices.[16] Further, at least thirteen states require businesses that own, license, or maintain personal information to implement and maintain reasonable security procedures and practices and to protect personal information from unauthorized access, destruction, use, modification, or disclosure.[17] The majority of states require businesses to dispose of sensitive personal information securely.[18]

Moreover, nearly every U.S. state, the District of Columbia, and several U.S. territories have enacted laws requiring notification to affected individuals following a breach of personal information.[19] These laws typically exempt institutions that are supervised by the federal prudential regulators. In contrast, credit reporting companies – which are not supervised by

---

16 *See, e.g.*, Xavier Becerra, Attorney General, Cal. Dep't of Justice, *Target Settles Record $18.5 Million Credit Card Data Breach Case* (May 23, 2017), https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data.

17 *See* Nat'l Conf. of State Legis., Data Security Laws – Private Sector (Jan. 16, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

18 *See* Nat'l Conf. of State Legis., Data Disposal Laws (Dec. 1, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx. At the federal level, the FTC's Disposal Rule regulates the proper disposal of consumer report information. *See* 16 C.F.R. pt. 682.

19 *See* Nat'l Conf. of State Legis., Security Breach Notification Laws (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

the prudential regulators – must comply with the patchwork of more than four dozen breach notification laws if a breach does occur.

Contractual Obligations Imposed Due to Other Regulatory Frameworks

Even beyond these direct legal requirements, the three nationwide credit bureaus – Experian, Equifax, and Transunion – are also subject to substantial additional requirements that result from doing business with other major financial institutions. The information security programs at many credit bureau customers are supervised by federal prudential regulators, *i.e.*, the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, or the National Credit Union Administration. Under comprehensive and detailed information security standards published by the Federal Financial Institutions Council ("FFIEC") – an interagency body of financial regulators – these financial institutions must oversee the information security programs of their third-party service providers.[20] Pursuant to these FFIEC requirements, financial institutions and their auditors subject the nationwide credit bureaus to dozens of information security audits each year, many of which include onsite inspections or examinations, which may take place over a period of several days.

[20] *See* FFIEC, IT Examination Handbook Infobase, *Information Security: Oversight of Third-Party Service Providers*, https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx.

The Payment Card Industry Data Security Standard

The three nationwide credit bureaus also comply with the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS is a set of cybersecurity requirements that are mandatory for all organizations that store, process, and transmit sensitive payment card information of the major credit card associations.[21] The standard requires credit reporting companies to take a number of specific steps to ensure the security of certain data. For example, the PCI DSS requires members to install and maintain firewalls, encrypt the transmission of cardholder data, protect against malware and implement and update anti-virus programs, restrict both digital and physical access to cardholder data, regularly test security systems and processes, and maintain a detailed information security policy for all personnel.[22] The standard imposes further detailed and specific technical requirements for the protection of cardholder data, such as a restriction on service providers' storage of personal identification or card verification numbers after card authorization.[23] In addition, the standard requires a service provider to ensure that any third parties with whom it shares data also comply with the PCI DSS.[24]

All three of the nationwide credit bureaus have been certified by the card networks as "PCI DSS Validated Service Providers," meaning that they are approved to store, process and

---

[21] Payment Card Industry Security Standards Council, *Requirements and Security Assessment Procedures, Version 3.2* (Apr. 2016).

[22] *Id.* at 5.

[23] *See, e.g., id.* at 38-39.

[24] *Id.* at 12.

transmit cardholder data. Service providers that store, process, or transmit cardholder data must be registered with the card networks and demonstrate PCI DSS compliance. PCI DSS compliance validation is required every 12 months for all service providers. As an example, all three nationwide credit bureaus are included on the Visa Service Provider Registry, indicating that they have successfully validated PCI DSS compliance with an on-site assessment, based on the report of an independent Qualified Security Assessor ("QSA"), and have met all applicable Visa program requirements.[25]

**The Fair Credit Reporting Act and CFPB Supervision**

Finally, I want to discuss the consumer protection regime that applies to credit reporting companies under the FCRA. This regime has persisted for nearly 50 years, with occasional fine tuning and two significant revisions, in 1996 and 2003. In addition, in 2012, the CFPB began supervising the credit reporting companies for, among other things, compliance with the FCRA.

When the credit reporting industry first began in the United States, there was little standardization in the methods used and types of data collected. In particular, there was no standard procedure for consumers to find out what was in their credit report and to have erroneous information corrected. In response to these concerns, in 1970 Congress passed the FCRA, which imposed duties on credit reporting companies (referred to as "consumer

---

[25] *See, e.g.*, Visa Global Registry of Service Providers, https://www.visa.com/splisting/index.html.

reporting agencies" under the statute).[26] These duties included providing consumers transparency by requiring lenders and other users of credit reports to notify consumers when they take "adverse action" based on a credit report, providing consumers with access to their file, and providing for a mechanism for consumers to dispute and correct inaccurate or incomplete information.

Building on the core structure of the FCRA, Congress revised the statute in 1996. One of the most important revisions was to impose a set of duties, not just on the credit reporting companies themselves, but on those businesses that furnished the information to the credit bureaus in the first place.[27] In 2003, again building on the FCRA's core structure, Congress again modified the FCRA through the Fair and Accurate Credit Transactions Act, which added certain consumer protections such as free annual credit reports and new protections for identity theft victims.[28]

Under the FCRA, credit reporting companies are subject to a comprehensive regulatory regime that provides many protections to consumers. A number of these provisions are designed to protect consumer privacy, such as the aforementioned permissible purpose and credentialing requirements. The FCRA also includes criminal penalties for people who obtain credit reports under false pretenses or credit reporting companies that knowingly provide

---

[26] *See Fair Credit Reporting Act: How It Functions for Consumers and the Economy: Hearing Before the Subcomm. on Financial Institutions and Consumer Credit of the H. Comm. on Financial Services*, 108th Cong. 129 (2003) (prepared statement of the Federal Trade Commission).

[27] *See, e.g.*, Amending Fair Credit Reporting Act, Sen. Comm. on Banking, Housing, and Urban Aff's, S. Rept. 108-166 (Oct. 17, 2003).

[28] *See* FCRA § 609(e).

credit reports to persons not authorized to receive them, for example, by selling consumers' private information to a litigation opponent or an ex-spouse hoping to find embarrassing information. To further ensure consumer privacy is protected, as I discussed before, credit reporting companies must "credential" users of their consumer reports to confirm they in fact have a permissible purpose to obtain the reports.[29]

Many of the provisions also address the accuracy and completeness of consumer reports. The most basic of these protections is the consumer's right to know what is in his or her file.[30] The 2003 amendments to the FCRA additionally required nationwide credit bureaus and nationwide specialty credit bureaus to provide consumers with free annual disclosures of the information in their file, including through an official website, www.annualcreditreport.com. Further, when a user of a consumer report takes "adverse action" against a consumer on the basis of information in his or her credit report, that user must provide the consumer with a notice that contains information about how the consumer can obtain a copy of his or her credit report and can get errors corrected.[31] For example, if a lender denies a consumer's application because of a low credit score, the lender must provide the consumer with a notice of adverse action. In addition, consumers have the right to dispute the contents of their file, and the credit reporting company is obligated to conduct a reasonable

---

29 *See* FCRA § 607(a).
30 *See* FCRA § 609.
31 *See* FCRA § 615(a).

investigation of the dispute.[32] Credit reporting companies must also independently employ reasonable procedures to maintain the maximum possible accuracy of the information in consumer files.[33]

Finally, in 2012, the CFPB became the first supervisor of the national credit reporting system – the first regulator with examination authority over the credit reporting companies, the users of credit reports, and the companies that furnish information into the credit reporting companies for incorporation into credit reports.[34] Since the CFPB formalized its supervisory authority in January 2012, the nationwide credit bureaus have been subject to essentially continuous examination cycles, where they have been examined for the adequacy of their compliance management systems, their dispute handling procedures, their procedures to ensure the maximum possible accuracy of credit reports, their credentialing procedures, and other important and highly regulated functions. In this supervisory role, the CFPB examines the policies, procedures, controls, and practices of credit reporting companies. The companies expend substantial resources responding to examiner requests and must maintain transparency with their examiners. If the examiners discover any areas in which a credit reporting company is not living up to its obligations, the CFPB can resolve the issue through the supervisory process, or, if the issue is sufficiently serious, choose to bring a public enforcement action. The

---

[32] *See* FCRA § 611.
[33] *See* FCRA § 607(b).
[34] The CFPB has supervisory authority over "larger participants" in the consumer reporting industry, which are defined in 12 C.F.R. § 1090.104.

Bureau recently opined on the success of this regime, concluding that it had produced a "proactive approach to compliance management" that "will reap benefits for consumers – and the lenders that use consumer reports – for many years to come."[35]

* * *

Thank you again for the opportunity to testify before you today. I am happy to answer any questions.

---

[35] *See* CFPB, *Supervisory Highlights: Consumer Reporting Special Edition, Winter 2017* 3 (Mar. 2017), http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.