Statement of Francis Creighton

President & CEO

Consumer Data Industry Association

Before the

Subcommittee on Digital Commerce and Consumer Protection

Committee on Energy and Commerce

United States House of Representatives

Hearing on

"Securing Consumers' Credit Data in the Age of Digital Commerce"

November 1, 2017

Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, thank you for the opportunity to appear before you.

My name is Francis Creighton, and in May I became the President & CEO of the Consumer Data Industry Association. CDIA is a trade association representing more than 100 corporate members, including the three nationwide credit bureaus – Equifax, Experian, and Transunion. We educate policymakers, regulators, consumers and others on how the responsible use of consumer data empowers economic opportunity.

With more than two-thirds of U.S. gross domestic product coming from consumer spending, CDIA member products are used in billions of transactions each year and expand consumers' access to financial services in a manner that is innovative and focused on their needs.

Consumers today have access to the most democratic and fair credit system ever to exist. Individual consumers have the liberty to access credit anywhere in the country from a wide variety of lenders based solely on their own personal history of handling credit. This means that when a family tries to buy a house for the first time, they are going to be able to access the right mortgage for their own personal needs. A young person who has a new job and has to buy a car to get to work can go to an auto dealer and drive off the lot even if she or he has no physical history in

that community. Lower income families can access credit through mainstream financial institutions rather than depending upon shadowy lending services.

Today's 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. If a consumer has been a responsible user of credit in the past, lenders and others are more likely to offer credit at the most favorable terms. In fact, credit reporting companies continue to innovate to solve the problem of the "unbanked" or "credit invisible" consumers, who have not had a chance to participate in the mainstream financial system because they have "thin" or no credit files. By expanding the kinds of information that we collect, we are able to give lenders and others information that allows more consumers to access traditional loans and bank products.

Our credit reporting system today is the envy of the world, and other countries actively work to emulate what we do here. It is one of the main reasons American consumers have such a diverse range of lenders and products from which to choose. This stands in stark contrast to many other financial systems, even those in developed nations.

This is a system that works uniquely well for the consumer. Some have suggested that consumers should have the ability to "opt out" of the credit reporting system.

While this may sound attractive at first blush, it would cause massive problems for the credit markets. Consumers effectively opt in whenever they open a credit account; lenders tell consumers in their loan agreements that they will be reporting information to credit bureaus, and then remind them every year with their Gramm-Leach-Bliley Act-mandated annual privacy notice. Lenders have a business incentive to make sure borrowers understand that this information is being shared, as they want to ensure that borrowers understand that there are additional consequences if a borrower does not meet her or his obligation.

Most consumers pay their bills on time; choosing to "opt out" of the system would mean that someone who has always paid their bills on time would have no credit report available reflecting that fact when they seek out new credit. Lenders would have no way to judge whether an individual applying for credit has paid their bills or not. Creditors and other users of credit reports would find it difficult to assess risk in the larger population if there was a sense that credit files were missing important information. The safe and sound choice for a lender would be to raise interest rates on loan products to account for the greater risk faced. And the consumer who has been consistently making the right choices would lose out.

Information is held on credit reports for limited periods of time. If someone closes their accounts and does not access credit, then after seven years, their credit file will become "thin," because they have no outstanding credit. And if they applied for

credit at that point they would likely face the same problems that some in Congress have been trying to address through legislation aimed at helping the "unbanked."

In creating and affirming the Fair Credit Reporting Act over the years, Congress weighed the privacy implications of information sharing and access with the economic benefits to consumers of a robust and efficient credit system, and the safety and soundness of the banking sector. The result is a credit system that other nations seek to emulate: a detailed regulatory regime that limits the sharing of information for permissible purposes only and strict requirements on accuracy, consumer access and correction. Our consumer system protects privacy and ensures that banks have a clear picture of the risk associated with lending to a particular consumer, all of which leads to the most efficient, fair and cost-effective credit system in the world.

Ultimately, our individual credit reports tell the story of our individual choices. They are neither positive nor negative; they are simply our best attempt at an accurate portrait of what we have done, and they give lenders and others the tools they need to make judgements about how a particular person will handle her or his obligations in the future. Because credit reports are always absorbing new information, a single missed payment, for example, is set in the context of years of on-time payments. Our credit reporting system allows for second chances for American consumers.

Without ready access to a consumer report, lenders, landlords, community banks, credit unions, insurance companies, and others have no assurance that a consumer has reliably paid obligations in the past, unless those service providers know the customer personally. As Richard Cordray, Director of the Consumer Financial Protection Bureau (CFPB), said in 2012 at a Field Hearing:

> "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 US credit system contributes to the diversity of business model choices American banking consumers enjoy by providing disproportionate benefits to smaller financial institutions like community banks and credit unions, who have access to accurate and complete information on par with that available to very large banks. Our consumer credit system works whether you are at a global bank or a community-based credit union because companies share critical information across the system to benefit everyone.

[1] Cordray, Richard. Prepared Remarks by Richard Cordray on Credit Reporting (July 16, 2012) (accessed October 23, 2017), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-by-richard-cordray-on-credit-reporting/.

Credit reports are also a check on human bias and assumptions. These reports provide lenders with a foundation of facts that contribute to equitable treatment for consumers. CDIA members establish an accountable and colorblind system for judging creditworthiness designed both for the best interests of consumers and safety and soundness of lending institutions – by ensuring the accuracy and completeness of information in consumer reports, and by providing businesses with the information they need to ensure consumers are treated fairly. Without this system, subjective judgements could be based on factors other than the facts of creditworthiness.

In the wake of the 2008 financial crisis, our country has also redoubled our efforts to ensure more disciplined underwriting and that borrowers have an ability to repay. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. Credit reports are a key way that we protect the consumer finance system by ensuring that banks are not granting credit to those who cannot afford it. This is why federal bank regulators require lenders and others, such as Fannie Mae and Freddie Mac, to use credit reports to assess the creditworthiness of prospective borrowers. One need only remember back to the overuse of "NINJA" (No Income, No Job or Assets) loans in the last decade's mortgage market, when unscrupulous lenders ignored credit reports in return for higher rates, to see the importance of using credit reports to protect the financial system.

This is an extraordinary system. In one sense, lenders take their sensitive customer information, and share it with a trusted third party, so that another financial institution –potentially a competitor—can access that information to make a better lending decision. And this is all done voluntarily, but within a significant regulatory structure[2]. The resulting competition lowers prices to the consumer.

Data Security Requirements for Credit Reporting Companies

The topic of this hearing is "Securing Consumers' Credit Data in the Age of Digital Commerce." Over the course of the rest of this statement I will share the numerous federal, state and private legal regimes under which credit reporting agencies work to secure data.

The Gramm-Leach-Bliley Act & FTC Safeguards Rule

Congress specifically designated credit reporting agencies as financial institutions that are subject to the information security requirements of the Gramm-Leach-Bliley Act (GLBA), designed in part by the predecessor of this Committee in 1999, and its implementing regulation, the Standards for Safeguarding Customer

[2] Student loan servicers are required to report to credit bureaus by law (20 U.S. Code § 1080a). Fannie Mae and Freddie Mac guidelines require credit reporting. Federal banking regulators have strongly encouraged their regulated communities to participate in credit reporting. Non-bank furnishers of data, such as non-bank auto-lenders, landlords and others, participate in the system on a voluntary basis.

Information ("Safeguards Rule") promulgated by the Federal Trade Commission (FTC)[3]. The Safeguards Rule imposes specific standards designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of such records; and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer[4].

The Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program" that includes appropriate administrative, technical and physical safeguards to achieve these objectives. 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].

Financial institutions, including credit reporting agencies, must also designate an employee to coordinate their comprehensive information security program, as well

[3] 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).
[4] 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).
[5] 16 C.F.R. § 314.3(a).

as identify reasonably foreseeable risks to the security of the information. Financial institutions must 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 their service providers employ strong security practices, and by entering into contracts with such providers that require them to implement appropriate safeguards[7].

These common-sense provisions are general parameters designed to allow evolving standards to keep pace with the evolving threat landscape. At their inception lawmakers and regulators anticipated that private institutions and the government overseers closest to the battle lines and with the greatest expertise in these matters would fine-tune industry best practices over time.

The Federal Trade Commission Act (FTC Act)

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

[6] 16 C.F.R. § 314.4.
[7] 16 C.F.R. § 314.4(d).
[8] 15 U.S.C. § 45.

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

The FTC requires that a company employ safeguards for information 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]."

---

[9] See Congressional Research Service, "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority" (September 11, 2014), https://fas.org/sgp/crs/misc/R43723.pdf.
[10] Federal Trade Commission, "Data Security" (accessed October 23, 2017), https://www.ftc.gov/datasecurity.
[11] See, e.g., Federal Trade Commission, "Protecting Personal Information: A Guide for Business" (accessed October 23, 2017), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[12] See Federal Trade Commission, "Privacy and Data Security Update (2016)" (January 2017) (accessed October 23, 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

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 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 permissible 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 multiple actions over the years seeking to enforce these provisions, most notably against ChoicePoint[13], 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.

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

[13] See Federal Trade Commission, "ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress" (January 26, 2006), (accessed October 23, 2017), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

procedures, credit reporting companies maintain detailed written procedures which take into account the risks presented by prospective users and their proposed uses of information. These procedures routinely include:

- 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. More specifically, the FTC issued 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[14].

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[15]. 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[16]. The majority of states require businesses to dispose of sensitive personal information securely[17].

[14] See FCRA § 628.
[15] See, e.g., Xavier Becerra, California Attorney General, "Attorney General Becerra: Target Settles Record $18.5 Million Credit Card Data Breach Case" (May 23, 2017), (accessed October 23, 2017), https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data
[16] See National Conference of State Legislatures, "Data Security Laws – Private Sector" (January 16, 2017), (accessed October 23, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
[17] See National Conference of State Legislatures, "Data Disposal Laws" (December 1, 2016), (accessed October 23, 2017), 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.

Moreover, nearly every state, DC and several U.S. territories have enacted laws requiring notification to affected individuals following a breach of personal information[18]. These laws typically, but do not always, exempt institutions that are supervised by the federal bank regulators, who have their own breach notice regime. In contrast, credit reporting companies – which are not supervised by the bank 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 governmental requirements, the three nationwide credit bureaus – Equifax, Experian and Transunion – are also subject to substantial additional legal requirements that result from doing business with other major financial institutions. The information security programs at many credit bureau financial institution 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), these financial institutions must oversee the information security programs of their third-party service providers[19].

[18] See National Conference of State Legislatures, "Security Breach Notification Laws" (April 12, 2017), (accessed October 23, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[19] See FFIEC, IT Examination Handbook Infobase, "Information Security: Oversight of Third-Party Service Providers," (accessed October 23, 2017), https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx.

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.

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. The standard requires credit reporting companies to take a number of specific steps to ensure the security of certain information. 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. 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. 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[20].

[20] Payment Card Industry Security Standards Council, "Requirements and Security Assessment Procedures, Version 3.2" (April 2016).

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 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.

The Fair Credit Reporting Act and CFPB Supervision

The federal FCRA has been around for nearly 50 years, with occasional fine tuning, two significant revisions (1996 & 2003) and now (starting in 2012) CFPB supervision and examination of the credit reporting companies for compliance with the FCRA[21].

When the credit reporting industry first began in the United States, there was little standardization in the methods used and types of information collected as it was a decentralized, city-by-city, business. In particular, there was no standard procedure for consumers to find out what was in a credit report and to have erroneous information corrected. In response to these concerns, the first voluntary standards of practice were pioneered by the industry in the 1960s and these later served as the basis for many provisions in the first FCRA, which Congress passed in 1970. The FCRA imposed duties on credit reporting companies (referred to as "consumer

[21] Importantly for this discussion – the CFPB does not have supervisory authority over data security matters.

reporting agencies" under the statute), which included requiring lenders and other users of credit reports to notify consumers when they take "adverse action" based on a credit report, requiring the agencies to disclose all information in the credit file to consumers upon request 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 businesses that furnish information to the credit bureaus in the first place. In 2003, again building on the FCRA's core structure, Congress further modified the FCRA by passing the Fair and Accurate Credit Transactions Act, which allowed consumers to receive free credit reports annually and included important new protections for identity theft victims[22], many of which built on industry-set practices already in place at that time.

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 credit reports to persons not

[22] FCRA § 609(e).

authorized to receive them, for example, by selling consumers' private information to a litigation opponent or an ex-spouse hoping to find embarrassing information[23].

The FCRA also addresses the accuracy and completeness of consumer reports. The most basic of these protections is the consumer's right to know what is in the credit file[24]. 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 the file, including through an official website, www.annualcreditreport.com for the nationwide bureaus. Further, when a user of a consumer report takes "adverse action" against a consumer on the basis of information in the credit report, that user must provide the consumer with a notice that contains information about how the consumer can obtain a copy of the credit report and can get errors corrected[25]. 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 the file, and the credit reporting company is obligated to conduct a reasonable investigation of the dispute[26]. Credit reporting companies must also independently employ reasonable procedures to assure maximum possible accuracy of the information in consumer files[27].

[23] FCRA § 607(a).
[24] FCRA § 609.
[25] FCRA § 615(a).
[26] FCRA § 611
[27] FCRA § 607(b).

Finally, in 2012, the CFPB became the first supervisor of the national credit reporting system. The Bureau has examination authority over the credit reporting companies, users of credit reports and companies that furnish information into the credit reporting companies for incorporation into credit reports[28]. 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. 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 enforcement actions. The 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."[29]

---

[28] The CFPB has supervisory authority over "larger participants" in the consumer reporting industry, which are defined in 12 C.F.R. § 1090.104.

[29] See CFPB, "Supervisory Highlights: Consumer Reporting Special Edition, Issue 14, Winter 2017 (March 2017) (accessed October 23, 2017), http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

As I have demonstrated through my testimony: this industry is regulated by multiple federal and state laws, enforced by multiple regulators, including the CFPB, FTC, State Attorneys General, banking regulators and more. And still there was a security breach. I am not here to speak for Equifax[30] specifically on the details of that breach but they have been clear in public testimony that they have closed the vulnerability exploited by the criminal hackers.

What I am here to do today is demonstrate the willingness of our industry to work with Congress and the regulatory bodies to ensure the security of consumer information. We will do everything in our power to ensure our customers have confidence their data is in good hands.

In conclusion, data security is not just our regulatory and legal obligation; it is good business. And it is just the right thing to do – for consumers, for our customers and for the entire financial system.

I look forward to your questions, today and into the future.

[30] Officials at Equifax have had the opportunity to review this testimony, though they did not comment on its preparation.