



Statement of Francis Creighton

President & CEO

Consumer Data Industry Association

Before the

Subcommittee on Financial Institutions & Consumer Credit

Committee on Financial Services

United States House of Representatives

Hearing on

“Legislative Proposals to Reform the Current Data Security
and Breach Notification Regulatory Regime”

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Subcommittee, thank you for the opportunity to appear before you.

My name is Francis Creighton, and I am 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. Our other members include specialty credit bureaus, resellers and the largest background screening companies. We educate policymakers, regulators, consumers and others on how the responsible use of consumer data empowers economic opportunity.

You have asked me to testify about two legislative proposals: the "Data Acquisition and Technology Accountability and Security Act," and H.R. 4028, the "PROTECT Act of 2017," including any suggestions to improve these legislative proposals. More generally, you have asked me to "address opportunities to reform current federal and state data security regulatory regimes in order to close any gaps in data security and data breach regulation, as well as reduce vulnerabilities or shortcomings in the current regulatory regime." I will endeavor to address these issues, but first would like to provide some context for what the consumer reporting industry does and how we are regulated.

Consumers today benefit from a democratic, accurate and fair credit system. 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. Families buying a home

for the first-time access mortgage products that suit their individual needs and capabilities.

Young people who have new jobs in a new city can go to an auto dealer and drive away with a financed car even without any history in that community. With the rise of the internet, new credit opportunities have expanded even further to meet individual needs.

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 – terms that previously were reserved for the wealthy. Credit reporting companies and other CDIA members are helping solve the problem of the unbanked and credit invisible populations by expanding the kinds of data we collect, giving lenders and others information that allow more consumers to responsibly access traditional financial services and integrate consumers into the mainstream financial system.

Most consumers pay their bills on time, and are rewarded for doing so when they seek out new credit and their report shows a positive history. Without the credit reporting system, lenders would have no way to judge whether an individual applying for credit has previously paid their bills or not. Lenders and other users of credit reports would find it difficult to assess risk in the larger population if 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 greater risk, with the consumer who has been consistently making the right choices losing out.

Credit reports are also important in helping consumers who may not have stellar credit avoid getting shut-out from the credit system altogether. Specifically, “risk based pricing” enables

consumers who may be more of a risk based on their credit payment history to still have access to credit. A broad-based credit reporting system enables lenders to compete, enabling more consumers to get more credit choices and at lower rates as lenders compete for consumers' business.

In creating, amending and affirming the Fair Credit Reporting Act since 1970, Congress has weighed the competing priorities of safety and soundness, privacy, accuracy, security and economic benefits. The result is a detailed regulatory regime limiting the sharing of information for defined permissible purposes only and strict requirements on accuracy, consumer access and correction. Our consumer reporting 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.

Our credit reports tell the story of our individual choices. They are neither positive nor negative; they are simply the best attempt at an accurate portrait of what we have done, and they give lenders and others the tools they need to assess how a particular person will handle her or his obligations in the future. Because credit reports are constantly updated with 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.

Other countries are actively working to emulate our credit system, working with the World Bank¹ and others to bring the kinds of opportunities we have here to the rest of the world. Our credit reporting system is a main reason American consumers have a diverse range of lenders and products from which to choose, in stark contrast to many other financial systems, even those in developed nations.

Credit reports also give a variety of different kinds of lenders access to the same kind of information, giving a local community bank or credit union a chance to compete against a trillion-dollar financial institution. As Richard Cordray, former 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.”²

Credit reports also check human bias and assumptions, providing lenders with 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

¹ See e.g. World Bank. General principles for credit reporting (September 1, 2011) (accessed February 21, 2018), <http://www.worldbank.org/en/topic/financialsector/publication/general-principles-for-credit-reporting>

² Cordray, Richard. Prepared Remarks by Richard Cordray on Credit Reporting (July 16, 2012) (accessed February 22, 2018), <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-by-richard-cordray-on-credit-reporting/>.

consumers and safety and soundness of lending institutions. Without this system, subjective judgements could be based on factors other than the facts of creditworthiness.

This Committee has been at the forefront of ensuring that lenders are making responsible choices, especially in the wake of the 2008 financial crisis. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. Federal regulators require lenders and others, such as Fannie Mae and Freddie Mac, to use credit reports to assess the creditworthiness of prospective borrowers. The proliferation of “NINJA” (No Income, No Job or Assets) loans in the last decade’s mortgage market, when some lenders pulled credit reports but effectively ignored them in return for higher rates, illustrates the importance of using credit reports to protect the financial system³.

Current Law Data Security Requirements for Credit Reporting Companies

Since September of last year, increased attention has been paid to how national CRAs secure credit file information and how that security is regulated. The industry is currently highly regulated, by the states, federal regulators, laws, contracts and other obligations.

³ NINJA lenders operated in a variety of ways – some depended on credit reports, but ignored other aspects of the loan file, such as income or employment status. While there were legitimate reasons for offering some of these loans, the record shows that traditional lending standards were put aside in an effort to maximize the number of loans closed.

The Gramm-Leach-Bliley Act & FTC Safeguards Rule

Credit reporting agencies are recognized as 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 Federal Trade Commission (FTC)⁴. 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 consumer⁵.

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 customer information⁶.

⁴ 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 (Federal Reserve, Office of the Comptroller of the Currency, 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).

⁵ 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).

⁶ 16 C.F.R. § 314.3(a).

Financial institutions, including credit reporting agencies, must also designate an employee to coordinate their comprehensive information security program, as well 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 risks⁷. 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 safeguards⁸.

These are general parameters designed to keep pace with evolving threats. Regulators anticipated that private institutions and their direct regulators and supervisors 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 Act⁹. Under this law the FTC is empowered to take action against any business that engages in "unfair or deceptive acts or practices" ("UDAP"), which the agency has interpreted to include inadequate data security practices¹⁰.

⁷ 16 C.F.R. § 314.4.

⁸ 16 C.F.R. § 314.4(d).

⁹ 15 U.S.C. § 45.

¹⁰ 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) (accessed February 22, 2018), <https://fas.org/sgp/crs/misc/R43723.pdf>.

The FTC requires companies to 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 vulnerabilities¹¹.” 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 information¹².

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 risk¹³.” It is our understanding, for example, that the FTC is the lead agency investigating the Equifax data breach.

The Fair Credit Reporting Act

When credit reporting first began, there was little standardization in the methods used and types of information collected as it was a decentralized, city-by-city, industry. In particular, there was no standard procedure for consumers to find out what was in a credit report and to

¹¹ Federal Trade Commission, “Data Security” (accessed February 22, 2018), <https://www.ftc.gov/datasecurity>.

¹² See, e.g., Federal Trade Commission, “Protecting Personal Information: A Guide for Business” (accessed February 28, 2018), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹³ See Federal Trade Commission, “Privacy and Data Security Update (2016)” (January 2017) (accessed February 22, 2018), <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

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 Fair Credit Reporting Act (FCRA). The FCRA imposed duties on credit reporting companies (referred to as “consumer 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 law 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, led by this Committee, 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 victims¹⁴, 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 of consumer protections. A number of these provisions are designed to protect consumer privacy, such as the aforementioned permissible purpose and credentialing requirements. The

¹⁴ FCRA § 609(e).

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 authorized to receive them, for example, by selling consumers' private information to a litigation opponent or an ex-spouse hoping to find embarrassing information¹⁵.

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 file¹⁶. The 2003 amendments to the FCRA additionally required 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 corrected¹⁷. 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. This notice enables consumers to understand that there may be adverse information in their credit file, and encourages the consumer to obtain a free copy of their credit report to examine it for possible errors.

¹⁵ FCRA § 607(a).

¹⁶ FCRA § 609.

¹⁷ FCRA § 615(a).

In addition, consumers have the right to dispute information in the file, and the credit reporting company is obligated to conduct a reasonable investigation of the dispute¹⁸. Credit reporting companies must also independently employ reasonable procedures to assure maximum possible accuracy of the information in consumer files¹⁹.

The FCRA also requires that credit reporting companies only provide credit reports to legitimate companies or people with a “permissible purpose” to receive such reports, such as credit or insurance underwriting. Companies’ 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 ChoicePoint²⁰, 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. At the time, that was the largest fine ever obtained by the FTC.

¹⁸ FCRA § 611

¹⁹ FCRA § 607(b).

²⁰ 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 February 22, 2018), <https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million>.

The federal FCRA has been around for nearly 50 years, with occasional fine tuning. Two significant revisions occurred in 1996 & 2003 and in 2012 CFPB began supervision and examination of the credit reporting companies for compliance with the FCRA²¹.

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 practices²². 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 disclosure²³. The majority of states require businesses to dispose of sensitive personal information securely²⁴.

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

²² See, e.g., Becerra, Xavier, California Attorney General, “Attorney General Becerra: Target Settles Record \$18.5 Million Credit Card Data Breach Case” (May 23, 2017), (accessed February 22, 2018), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data>.

²³ See National Conference of State Legislatures, “Data Security Laws – Private Sector” (January 16, 2017), (accessed February 22, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

²⁴ See National Conference of State Legislatures, “Data Disposal Laws” (December 1, 2016), (accessed February 22, 2018), <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 information²⁵. 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 additional legal requirements resulting 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 providers²⁶. Pursuant to these FFIEC requirements, financial institutions and their auditors subject the nationwide credit bureaus to dozens of

²⁵ See National Conference of State Legislatures, “Security Breach Notification Laws” (April 12, 2017), (accessed February 22, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

²⁶ See FFIEC, IT Examination Handbook Infobase, “Information Security: Oversight of Third-Party Service Providers,” (accessed February 22, 2018), <https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx>.

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 DSS²⁷.

²⁷ Payment Card Industry Security Standards Council, “Requirements and Security Assessment Procedures, Version 3.2” (April 2016).

CFPB Supervision

While CRAs had been subject to FTC and state law requirements, in 2012 the CFPB became the first *supervisor* of the national credit reporting system, under authority granted to the Bureau by the Dodd Frank Wall Street Reform and Consumer Protection Act. 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 reports²⁸.

Since CFPB supervision began, 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

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

management” that “will reap benefits for consumers – and the lenders that use consumer reports – for many years to come.”²⁹

Legislative Proposals

H.R. _____, the Data Acquisition and Technology Accountability and Security Act

CDIA and our members strongly support a single, preemptive data breach standard for companies across the economy.

Because of the unique liability consumer reporting agencies face under the Fair Credit Reporting Act, such as uncapped statutory damages in class action settings, we believe data breach legislation should be both preemptive of state law and be limited to administrative enforcement. Establishing a uniform national breach standard should not be an opportunity to open up a new cottage industry of trial lawyers suing companies because of technical violations with no consumer harm. Standards should be enforced by the Federal Trade Commission.

A federal data security standard should be flexible and scalable, taking into account the size, scale, scope and sensitivity of the data an organization maintains. The standard should also consider the cost to the enterprise of securing the data. Consumers who are at risk of economic loss as the result of a breach should have timely notice, as should law enforcement and regulators. In addition, consumer reporting agencies should be provided advanced notice

²⁹ See CFPB, “Supervisory Highlights: Consumer Reporting Special Edition, Issue 14, Winter 2017 (March 2017) (accessed February 22, 2018), http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

of a breach so they can be ready to handle the volume of consumer calls that are directed toward them in the case of a breach notification.

The legislation before the Subcommittee today establishes a national standard for both data security and how companies inform impacted people about breaches of the kind of personal information that can be used to set up an account or engage in a financial transaction. The bill's provisions would allow a company's functional regulator to enforce these rules (such as a bank regulator), setting up the FTC as the default regulator for those without a designated regulatory body, with enforcement by state Attorneys General. Since credit bureaus are financial entities under GLBA, they would continue to be subject to the FTC's Safeguards Rule and to civil penalty authority for violations of the breach notification provision of the bill.

The bill's data security provisions for non-financial entities are patterned after those in the Gramm-Leach-Bliley Act, the FTC Safeguards Rule and the Interagency Guidelines referenced earlier. However, the standards in this bill are different -- safeguards would be developed by the covered entities themselves rather than by their regulators. The FTC would not issue regulations implementing this standard for non-financial entities.

The trigger for what constitutes a data breach, "reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss," is a fair approximation to how a breach should be defined in any reasonable setting. Companies who have experienced a breach must

“immediately notify without unreasonable delay”; CDIA suggests “without unreasonable delay” (i.e. not including the word “immediately³⁰”), would be more appropriate.

CDIA is pleased to note that for breaches over 5,000 consumers, credit bureaus can be notified ahead of the general notification. This would help ensure that credit bureaus can prepare our systems for increased consumer contacts that a large breach can generate.

This legislation broadly conforms to the policy goals CDIA members have had for breach notification legislation. As the legislative process moves forward, we anticipate that perfecting amendments may further improve the bill³¹, and we look forward to working with the bill sponsor and other members of the Committee on solving this important problem.

H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology (PROTECT) Act of 2017

H.R. 4028 seeks to secure consumers’ credit information by establishing a uniform national standard on how consumers can freeze their credit reports, creates new standards for the regulation of data security at national CRAs and stops the use of Social Security Numbers (SSNs) in credit reporting.

³⁰ Use of the word “immediately” without qualification would suggest that companies would have to disclose the breach before they understand the extent of the breach, have informed law enforcement or closed the vulnerability.

³¹ For example, the bill’s “substitute notice” provisions could be improved to make it more similar to a number of state laws.

Credit freezes were created to assist victims of identity theft. While they may be useful for some victims of identity theft to help protect their credit, they should not be the first line of defense in identity protection. Instead, consumers should check their free annual credit report to review the credit report for any suspicious activity. Consumers may also consider obtaining credit monitoring services, which are routinely provided free of charge to data breach victims.

An initial fraud alert is the first line of defense for consumers who believe that they are, or are about to become, victims of identity theft. This step may be appropriate for consumers who expect to be credit-active. For free, a consumer can place the initial fraud alert by phone, in writing or via website. If a fraud alert is on a consumer's credit file, lenders are required to contact the individual or take reasonable steps to verify the identity of the applicant before extending a new line of credit or increasing a line of credit. A fraud alert requested at one bureau is shared with the other two bureaus. An "extended alert" beyond the initial 90 days will help consumers who are victims of identity theft, but expect to be credit-active.

Members of the military can place an "active duty alert," which lasts for a year and is another preventative option. Fraud alerts were created by CRAs, and were codified as part of the FACT Act of 2003.

Credit freezes are required by law in every State and are a final line of defense for consumers who are chronically victims of identity theft or who do not plan to be credit active or active in various other commercial situations. Different states permit different fees for setting a freeze. A freeze is, effectively, a consumer telling a credit bureau not to release a credit report unless

the consumer contacts the credit bureau in advance to say otherwise. Such a consumer can only obtain credit by taking the extra step of contacting the credit bureau ahead of time. A freeze remains on the file until the consumer lifts or removes the freeze. While a freeze is in place, the consumer's file continues to be updated to reflect current account balances and payments, as well as for account management and collection processes.

The PROTECT Act aims to establish a uniform standard for freezes. Establishing such a system would eliminate consumer confusion on how to place a freeze and reduce administrative costs by having a single standard for compliance. CDIA's impacted members support the freeze language in H.R. 4028.

The PROTECT Act also establishes a new data security supervisory agency for CRAs. As discussed earlier, the consumer reporting industry is currently regulated in many different ways by many agencies. Specifically, the FTC is the industry's primary regulator, and the CFPB supervises certain aspects of our business. We are also regulated indirectly through the federal financial regulators, through their guidance on service providers and vendors.

We continue to believe that the security incident at Equifax should be fully investigated, and stand ready to work with Congress to address regulatory gaps if any are found.

The PROTECT Act would eliminate the use of SSNs by CRAs by 2020. CDIA and its members believe that this is not a feasible proposal and look forward to working with the bill's sponsor

and the Committee on alternatives to this legislation as well as potential innovations in the market.

The SSN has been with us since 1936, and though originally conceived as an identifier for a specific purpose, over time it has become the major individual identifier in the United States.

The federal government began this process, expanding the use of the SSN first in 1943 and later in 1961 and beyond. The IRS and DOD have been using the SSN as an identifier of taxpayers and military personnel since the 1960's. In the 1980s, this process accelerated, and the SSN began being used for employment eligibility verification, military draft registration, driver's licenses and for operators of stores that redeemed food stamps. In the 1990s, SSN usage expanded into jury selection, federal workers' compensation laws and through welfare reform legislation³².

The widescale usage of SSNs did not happen overnight; it was a decades long process led by Congress and the Executive Branch.

CRA's need SSNs because we have obligations under the FCRA and other statutes to ensure maximum possible accuracy of the data we maintain. The use of SSNs is absolutely critical to meeting this legal obligation. There simply is no other identifier currently in existence that gives us the ability to match consumers with their information with the confidence required to

³² Hearing on the Homeland Security Threat from Document Fraud, Identity Theft, and Social Security Number Misuse, before the Senate Committee on Finance, Sept. 9, 2003 (statement of James B. Lockhart, III, Deputy Commissioner of Social Security, Social Security Administration).

meet our statutory obligation. If we could not use SSNs, credit reports and other documentation would become less reliable and less useful to lenders when making credit decisions.

SSNs are collected by courts for a number of reasons: identification of parties, collection of fines and restitution, facilitation of the collection of judgments by creditors and governments, etc. Courts notify the Social Security Administration that individuals are incarcerated. Without the use of SSNs, the justice system would grind to a halt. And credit bureaus are part of the process courts use to ensure that child support is paid and that information on a credit file is in line with what a court has ruled. Federal law requires state courts to place SSNs in divorce decrees, child support orders and paternity determinations to facilitate child support collection³³.

The lack of full Social Security Numbers and other identifiers has led to a number of liens and judgements no longer appearing on credit reports. Some courts have limited identifying information in their documents and as a result CRAs can no longer be sure that certain liens or judgements apply to a particular consumer. This creates problems across the economy, as a bank may be asked to loan significant funds to an individual subject to a court judgement, and if the consumer does not disclose it, the institution must use some other way to determine if the

³³ Hearing on Enhancing Social Security Number Privacy: Before the Subcommittee on Social Security of the House Ways and Means Committee, June 15, 2004 (107th Cong.) (statement of Mike L. Buenger, President, Conference of State Court Administrators).

debts listed on an application are comprehensive. Service providers provide that service today, but at additional cost.

The private sector uses SSNs for the same reasons as the government: it is the only reliable and universal identifier. It helps ensure that credit reports are accurate and that information is matched with the correct file. It also helps to ensure that when a business requests a credit report about a consumer, the credit bureau is able to return information regarding the correct individual. Millions of Americans share a name and a surprising number of people share a name and date of birth³⁴. Not everyone has a driver's license. Both the public and private sectors need some way to identify people on documents.

However, there should be limitations placed on how SSNs are used. For example, while SSNs are excellent identifiers and are essential for ensuring data accuracy, they should not be used as a sole method to authenticate an individual's identity. No financial institution or other user of a credit report should be using the SSN as a sole means of authenticating the identity of an individual³⁵. And the bulk of industry follows that guidance – if they did not the incidence of new account fraud would be significantly higher. The fact is that financial institutions have many ways of authenticating an individual, without using the SSN. The technology for use in authenticating individual identity is constantly evolving to stay ahead of perpetrators of fraud.

³⁴ Barr, Joseph R. "The Trouble with Names/Dates of Birth Combinations as Identifiers." ID Analytics, Inc. White Paper (April 2011) (accessed February 22, 2018), https://www.idanalytics.com/media/The_Trouble_With-Names_White_Paper_FINAL.pdf

³⁵ Section 326 of the USA Patriot Act does list the SSN as one of the Personally Identifiable Information data elements that a lender must gather as part of the Know Your Customer rules.

Given the many, many public and private sector uses of the SSN, it would be a monumental undertaking to re-code systems cutting across the entire financial services ecosystem (not just consumer reporting agencies) to some new universal identifier and, further, there would be no means of establishing agreement on what other source should be used or created and how consumers themselves would learn how to use this new identifier in lieu of the SSN. This would not be something that could be done in a matter of 22 months. It would be a years-long system migration costing billions of dollars across the economy.

And even if we determined that we do need to move off of SSNs, the question remains what it would be replaced with. The public and private sectors would still need some kind of universal, unique identifier that can be used across platforms and technologies. In order for it to be universal, it would have to be in federal law. Individual companies have been working to innovate in this field, but how would a private company ensure that *every* person in the country has an identifier? This is a difficult challenge.

We look forward to working with the bill's sponsor and all of the Members of the Committee to address this challenge. The way to get at this issue is innovation, but unfortunately this challenge has not yet been overcome.

The consumer reporting industry welcomes efforts to establish a national data breach notification, security and credit freeze standards and to make cybersecurity improvements at the national CRAs. While we believe that parts of the PROTECT Act can be improved, we

appreciate the opportunity to address our industry's regulatory structure. Our industry will continue to work with Congress and the regulatory bodies to ensure the security of consumer information.

Especially in the wake of the security incident announced by Equifax in September, CDIA members are doing everything in their power to ensure consumers have confidence their data are in good hands. Data security is not just our regulatory and legal obligation; it is good business. And it is the right thing to do – for consumers, for our customers and for the entire financial system.

Thank you for the opportunity to appear before you. I look forward to your questions.