U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

October 31, 2017

TO: Members, Subcommittee on Digital Commerce and Consumer Protection

FROM: Committee Majority Staff

RE: Hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce"

I. INTRODUCTION

The Subcommittee on Digital Commerce and Consumer Protection will hold a hearing on Wednesday, November 1, 2017, at 10:30 a.m. in 2123 Rayburn House Office Building. The hearing is entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

II. WITNESSES

- Francis Creighton, President and CEO, Consumer Data Industry Association;
- James Norton, Adjunct Lecturer, Johns Hopkins University Zanvyll Krieger School of Arts and Sciences;
- Anne P. Fortney, Esq., Partner Emeritus, Hudson Cook; and
- Bruce Schneier, Adjunct Lecturer in Public Policy, Harvard Kennedy School.

III. BACKGROUND

Over 145 million Americans' sensitive personal information was stolen from Equifax's system earlier this year.[1] Equifax failed to update its system to address a known vulnerability and as a result names, full nine-digit Social Security numbers, birthdates, addresses, and, in some cases, driver's license numbers, credit card numbers, and credit dispute information were taken.[2]

[1] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628; https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821; http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-20171003-SD002.pdf

[2] *Id*. *See also* "Oversight of the Equifax Data Breach: Answers for Consumers," Hearing Before the Subcomm. on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Statement of Richard F. Smith, former Chairman and CEO, Equifax, Inc.), at http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf

The Equifax breach affects nearly 50 percent of the total U.S. population, and is the fourth largest data breach, according to press reports.[3] Recent data from the Identify Theft Resource Center (ITRC) indicates that as of October 27, 2017, over 1,100 data breaches have occurred this year, exposing over 171.6 million records.[4] According to a November 2016 ITRC report, there were more than 165 million Social Security numbers exposed in 2015, more than 10 times the number compromised in 2014.[5] According to a Javelin Strategy & Research Study, in 2016, approximately 15.4 million Americans were victims of fraud or identity theft (an increase of 2 million victims from the previous year), losing a total of $16 billion to criminals.[6] The Javelin study also found in 2016 that "card-not-present" fraud rose significantly due to the growth of online e-commerce, account takeover incidence and losses rose notably, and that new-account fraud continued.[7]

Hackers, criminals, and nation-states are working to find vulnerabilities and overcome cyber-defenses, to acquire and exfiltrate data, and to exploit that data for their own gain. According to the 2017 Verizon Data Breach Investigations Report (DBIR), 75 percent of the data breaches were perpetrated by outsiders, 51 percent were perpetrated by organized criminal groups, and 18 percent were perpetrated by state-affiliated actors.[8] The DBIR also found, as it pertains to breach tactics, 62 percent of data breaches featured hacking, 51 percent included malware, and 81 percent of hacking-related breaches leveraged either stolen and/or weak passwords.[9] Other findings included 66 percent of malware was installed via malicious email attachments, 73 percent of breaches were financially motivated, 21 percent were related to espionage, 27 percent were discovered by third parties, and 61 percent of the data breach victims in this year's report are businesses with under 1,000 employees.[10]

A. CREDIT REPORTS

Consumer reporting agencies are firms that prepare credit reports based upon individuals' financial transactions history to provide such reports to third parties.[11] For example, lenders use

---

[3] https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/
[4] http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReportSummary2017.pdf
[5] http://www.idtheftcenter.org/images/page-docs/NewAccountFraud.pdf
[6] https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
[7] *Id*.
[8] 2017 Verizon Data Breach Investigations Report (10th Edition) - Executive Summary, at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[9] *Id*.
[10] *Id*.
[11] A consumer reporting agency is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

credit reports and related data and information to "determine the likelihood that prospective borrowers will repay their loans."[12] The consumer data industry also collects and disseminates consumer information to insured depository institutions, insurance companies, payday lenders, and merchants, to name a few, "to identify and evaluate potential loss risks before entering into financial relationship with new consumers."[13] Equifax is one of the three largest national providers of credit reports. The three major credit reporting agencies (CRAs) have over 200 million credit records.[14] However, they are not the only CRAs; there are several hundred smaller, niche CRAs that specialize in the collection of information to develop credit reports for different industries and regions.[15] A credit report typically includes information like name, address, birthdate, Social Security number, as well as data on "credit repayment, tenant payment, employment, insurance claims, arrests, bankruptcies, and check writing and account management."[16]

Firms that use credit reports may also supply or furnish data and information to CRAs, acting as so-called "furnishers."[17] Furnishers report a "tradeline" account associated to a particular consumer to a CRA. A tradeline serves as a "record of the transaction (payment) activity associated with the account."[18] To become data furnishers, "firms must be approved and comply with the policies of a CRA, such as fee registration requirements."[19] Additionally, "entities that elect to become furnishers face legal obligations under the Fair Credit Reporting Act (FCRA)."[20] Different CRAs may or may not collect the same information on the same individuals. According to the Congressional Research Service, "consumer reports obtained from different CRAs on the same consumer are likely to differ due to different policies adopted by furnishers, CRAs, or both."[21]

---

[12] Congressional Research Service Report no. R44125, "Consumer and Credit Reporting, Scoring, and Related Policy Issues," by Darryl Getter (July 30, 2015) (hereinafter "CRS Report no. R44125").
[13] *Id*.
[14] https://www.nytimes.com/2015/03/10/business/big-credit-reporting-agencies-to-overhaul-error-fixing-process.html
[15] Consumer Data Industry Association, "About CDIA," at https://www.cdiaonline.org/about/index.cfm?unItemNumber=515; "List of Consumer Reporting Agencies," issued by the Consumer Financial Protection Bureau, at http://files.consumerfinance.gov/f/201604_cfpb_list-of-consumer-reporting-companies.pdf; http://www.experian.com/rentbureau/renter-credit.html; CRS Insight.
[16] CRS Report no. R44125.
[17] https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-information-furnishers-need-know; https://consumercomplianceoutlook.org/2012/second-quarter/furnishers-compliance-obligations/
[18] CRS Report no. R44125.
[19] http://www.equifax.com/business/data-furnishers/; https://www.experian.com/innovation/thought-leadership/business-resources-consumer-data-reporting.jsp
[20] CRS Report no. R44125; https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-information-furnishers-need-know; https://consumercomplianceoutlook.org/2012/second-quarter/furnishers-compliance-obligations/
[21] CRS Report no. R44125.

B. FEDERAL REGULATION OF CRAs

1. Fair Credit Reporting Act

The FCRA requires CRAs to "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[22] The FCRA limits the use of credit reports and access to credit data to those who have a legally permissible purpose, and requires that CRAs employ "reasonable efforts" to verify the identity of those to whom they supply credit reports and that the recipient has a permissible purpose to use the report.[23] Credit reports may be provided for particular purposes including making decisions involving credit, insurance, tenant screening, and employment screening. The FCRA also imposes certain responsibilities on firms that "collect, furnish, and use the information contained in consumers' credit reports."[24] Under 15 U.S.C. § 1681, a violation of FCRA constitutes an unfair or deceptive act or practice in commerce, in violation of section 5(a) of the Federal Trade Commission Act.

In 2012, the Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) transferred most of the FCRA rulemaking and enforcement responsibilities to the Consumer Financial Protection Bureau (CFPB).[25] The CFPB coordinates enforcement activities with the Federal Trade Commission's enforcements under the Federal Trade Commission Act.[26] Since 2012, the CFPB has subjected "larger participants" in the credit reporting industry to limited regulatory supervision.[27] Prior to 2012, CFPB did not actively supervise CRAs for FCRA compliance on an on-going basis.[28] Section 1002(12)(J) of the Dodd-Frank Act excluded financial institutions' information security safeguards under section 501(b) Gramm-Leach-Bliley Act (GLBA) from the CFPB's rulemaking, examination, and enforcement authority.[29]

---

[22] 15 U.S.C. § 1681(b)
[23] 15 U.S.C. § 1681e(a)
[24] Congressional Research Service Insight, "The Equifax Data Breach: An Overview and Issues for Congress," by N. Eric Weiss (September 29, 2017).
[25] Pub. L. 111-203 (July 21, 2010).
[26] https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act
[27] In July 2012, the CFPB announced it would for "first time supervise consumer reporting agencies that have more than $7 million in annual receipts. The CFPB's supervisory authority extends to an estimated 30 companies that account for about 94 percent of the market's annual receipts. Altogether, the three largest credit reporting companies issue more than 3 billion consumer reports a year and maintain files on more than 200 million Americans." https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-to-superivse-credit-reporting/
[28] *Id.*
[29] https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf

2. Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act requires federal financial institution regulators to establish data protection standards "for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[30] CRAs are subject to these data protection and confidentiality provisions of section 501(b) of the GLBA.

The Federal Trade Commission established the GLBA requirements through the "Safeguards Rule," which took effect in 2003.[31] The Safeguards Rule requires financial institutions to have a written information security plan that describes their program to protect customer information.[32] As part of its plan, each company must: 1) designate a program manager or team to coordinate its information security program; 2) conduct risk assessment to customer information, and evaluate the effectiveness of the current safeguards for controlling these risks; 3) design and implement a safeguards program that mitigate information risks, and regularly monitor and test it; 4) select service providers that can maintain appropriate safeguards, and make sure contracts with service providers and vendors requires them to maintain safeguards; and 5) evaluate and adjust the program periodically in light of relevant circumstances. The Safeguards Rule also requires companies to assess and address the risks to customer information in all areas of their operation.

3. Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act prohibits "unfair and deceptive acts or practices in or affecting commerce."[33] The FTC uses section 5 to enforce against companies that make deceptive claims regarding privacy or security they provide for consumer information. The Commission also uses section 5 to enforce against unfair practices that are likely to cause consumers substantial injury that are neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.[34]

As noted above, the FTC enforces the Safeguards Rule (implemented in GLBA), which sets forth data security requirements for financial institutions within the FTC's jurisdiction, and the FCRA rules dictating that consumer reporting agencies use reasonable procedures to ensure

---

[30] Section 501(b) of the Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act), Pub. L. 106-102, enacted Nov. 12, 1999.
[31] 16 CFR § 314.
[32] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule
[33] 15 U.S.C. § 45.
[34] https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf

that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information.[35]

C. STATE DATA SECURITY AND BREACH NOTIFICATION LAWS

Forty-eight States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification requirements. Twelve States have enacted legislation dealing with commercial data security.[36] The majority of those States have tied the standard to "reasonable" security. State laws in this area typically define personal information in terms of data that may lead to identifying a specific individual (e.g., a combination of first, middle, or last names; Social Security numbers; State identification numbers) and data that may lead to financial harm (e.g., financial account number; pins; passcodes).

IV. ISSUES

The following issues may be examined at the hearing:

- The legal and regulatory framework for CRAs, including the safeguards framework in GLBA and consumer protections contained in the FCRA.

- Current cybersecurity standards, trends, best practices, and emerging threats, particularly with respect to known cybersecurity vulnerabilities.

- The relationship between data breaches and incidence of identity theft and fraud.

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Melissa Froelich or Paul Jackson of the Committee staff at (202) 225-2927.

---

[35] In August 2017, the online tax preparation service (TaxSlayer, LLC) agreed to settle Federal Trade Commission allegations that it violated the Safeguards Rule by failing to develop a written comprehensive security program until November 2015 (other violations were alleged). https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges

[36] Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.