PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

On

The Fair Credit Reporting Act, Credit Bureaus, and Data Security

Before the

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

Washington, D.C. July 12, 2018

I. INTRODUCTION

Chairman Crapo and members of the Committee, my name is Maneesha Mithal, and I am the Associate Director for the Division of Privacy and Identity Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to discuss the Fair Credit Reporting Act, credit bureaus, and data security.

Congress enacted the Fair Credit Reporting Act[2] ("FCRA") in 1970, recognizing the importance of "fair and accurate credit reporting" to maintain "the efficiency of the banking system" and "the public[']s confidence" in that system, while at the same time balancing the "need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[3] The FCRA helps to (1) prevent the misuse of sensitive consumer report information by limiting recipients to those who have a legitimate need for it; (2) improve the accuracy and integrity of consumer reports; and (3) promote the efficiency of the nation's banking and consumer credit systems. Since the FCRA's passage, Congress has amended the statute to address developments in the consumer reporting system and the marketplace and to increase consumers' rights and protections with respect to the collection and use of their data.[4]

---

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] 15 U.S.C. §§ 1681-1681x.

[3] *Id.* § 1681(a).

[4] The Consumer Credit Reporting Reform Act of 1996, Title II, Subtitle D, Chapter 1, of the Omnibus Consolidated Appropriations Act for Fiscal Year 1997 (Pub. L. No. 104-208, Sept. 30, 1996), made extensive revisions to the FCRA, including expanding the duties of consumer reporting agencies, increasing obligations on users of consumer reports, and adding furnishers of information to consumer reporting agencies as a category of entities with statutory obligations. There were a number of more modest revisions over the next seven years, the most significant of which was a 1999 amendment that specifically authorized the federal financial agencies to promulgate regulations for the banks and other entities subject to their jurisdiction. The Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (Dec. 4, 2003) ("FACT Act"), added several sections to assist consumers and businesses in combating identity theft and reduce the damage to consumers. The Commission, often in conjunction with the federal financial agencies, issued numerous rules to implement the various FACT Act provisions.

The Commission has played a key role in the implementation, enforcement, and interpretation of the FCRA since its enactment.[5] In the last decade, the Commission has brought over 30 actions to enforce the FCRA against consumer reporting agencies ("CRAs"), users of consumer reports, and furnishers of information to CRAs. As the consumer reporting system evolves and new technologies and business practices emerge, vigorous enforcement of the FCRA continues to be a top priority for the Commission, as well as consumer and business education concerning applicable rights and responsibilities under the statute.

This testimony first provides background on the FCRA. Next, it discusses marketplace developments related to credit report accuracy. It then discusses the Commission's work to enforce the accuracy provisions of the FCRA and educate consumers and businesses about their respective rights and responsibilities under the statute. Finally, it discusses the data security requirements applicable to credit bureaus and the FTC's efforts to promote data security in this sector.

II. BACKGROUND ON THE FCRA

CRAs assemble or evaluate consumer data for third parties to use to make critical decisions about the availability and cost of various consumer products and services, including credit, insurance, employment, and housing.[6] These consumer reports are often used to evaluate the risk of future nonpayment, default, or other adverse events. For example, complete and accurate consumer reports enable creditors to make informed lending decisions, benefitting both creditors and consumers. Errors in consumer reports, however, can cause consumers to be denied

[5] As enacted, the FCRA established the Commission as the primary federal enforcement agency, with wide jurisdiction over entities involved in the consumer reporting system; the primary exceptions to the Commission's jurisdiction are federally regulated financial institutions. *See* 15 U.S.C. § 1681s(a)-(b). Pursuant to the Consumer Financial Protection Act of 2010 ("CFPA"), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (The Dodd-Frank Wall Street Reform and Consumer Protection Act), the Commission shares its FCRA enforcement role with the Bureau of Consumer Financial Protection ("Bureau") in many respects.

[6] 15 U.S.C. § 1681a(d) & (f).

credit or other benefits or pay a higher price for them. Errors in consumer reports can also cause credit issuers to make inaccurate decisions that result in declining credit to a potentially valuable customer or issuing credit to a riskier customer than intended.

The FCRA imposes a number of obligations on CRAs. For example, to protect the privacy of sensitive consumer report information, CRAs must take reasonable measures to ensure that they provide such information only to those who have a statutorily-specified "permissible purpose" to receive it.[7] CRAs must also comply with requirements to help ensure the accuracy of consumer reports, including requirements that CRAs (1) maintain reasonable procedures to ensure the "maximum possible accuracy" of consumer reports[8] and (2) maintain procedures through which consumers can dispute and correct inaccurate information in their consumer reports.[9]

Under the FCRA, if a consumer disputes the completeness or accuracy of information contained in his or her file, the CRA must complete a reasonable investigation within 30 days. The CRA must notify the furnisher of the disputed information within five business days. If a disputed item is found to be inaccurate or incomplete or cannot be verified, the CRA must delete or modify the information and notify the furnisher. In general, the CRA must provide the consumer with written notice of the results of the investigation in accordance with the procedures set forth in the statute within five business days after the completion of the investigation.

[7] *Id.* § 1681b(a), (c). Permissible purposes under the FCRA include, but are not limited to, the use of a consumer report in connection with a determination of eligibility for credit, insurance, or a license; in connection with the review of an existing account; and for certain employment purposes.
[8] *Id.* § 1681e(b).
[9] *Id.* § 1681i(a)-(d)(1).

In addition, the FCRA imposes obligations on those who furnish information about consumers to CRAs, such as entities extending credit. For example, furnishers have a duty to report accurate information and investigate consumer disputes of inaccurate information.[10]

Users of consumer reports have obligations under the statute as well. For example, if a user of a consumer report takes an adverse action against a consumer–such as a denial of credit or employment–based on information in a consumer report, the user must provide an adverse action notice to the consumer, which explains how the consumer can obtain a free copy of the report and dispute any inaccurate information in the report.[11]

III. CREDIT REPORT ACCURACY

In 2012, the Commission published a study of credit report accuracy mandated by the FACT Act, which amended the FCRA.[12] It was the first major study that looked at all of the primary groups that participate in the credit reporting and scoring process—consumers, furnishers (e.g., creditors, lenders, debt collection agencies), the Fair Isaac Corporation (which develops FICO credit scores), and the national credit bureaus.[13] To implement the study, researchers worked with approximately 1,000 consumers to review their free credit reports from the three major credit bureaus. The researchers helped consumers identify and dispute possible errors on their credit reports. According to the study findings, 25% of consumers identified errors on their credit reports that might affect their credit scores and 80% of these consumers who filed disputes experienced some modification to their credit reports. Overall, 13% of consumers experienced a change in their credit scores after a dispute and 5% of consumers experienced an

[10] *Id.*§ 1681s-2(a)-(b).
[11] *Id.* § 1681m(a). The adverse action notice also must include a statement that the CRA that supplied the consumer report did not make the decision to take the adverse action and cannot give the consumer any specific reasons for the decision. *Id.* § 1681m(a)(2)(B).
[12] Pub. L. No. 108-159 (Dec. 4, 2003).
[13] *Section 319 of the Fair and Accurate Credit Transactions Act of 2003: Fifth Interim Federal Trade Commission Report to Congress Concerning the Accuracy of Information in Credit Reports* (Dec. 2012), *available at* https://www.ftc.gov/reports/section-319-fair-accurate-credit-transactions-act-2003-fifth-interim-federal-trade.

increase in their credit scores such that their credit risk tier decreased and the consumer may be more likely to be offered a lower loan interest rate.

There have been significant changes in the marketplace aimed at increasing credit report accuracy since the Commission published its study. For example, the Bureau has been exercising its supervisory authority over the nationwide credit bureaus and it periodically publishes Supervisory Highlights describing its findings. Last year, it published an edition focused on accuracy issues in credit reporting and the handling and resolution of consumer disputes, and it pointed to several specific improvements it directed in these areas.[14]

In addition, in 2015, the nationwide credit bureaus announced a Nationwide Consumer Assistance Plan ("NCAP") as a result of a settlement with over 30 state attorneys general, with a number of provisions designed to improve the accuracy of credit reports.[15] These provisions include requiring all data furnishers to use the most current reporting format; removing any previously reported medical collections that have been paid or are being paid by insurance; requiring debt collectors to regularly update the status of unpaid debts and remove debts no longer being pursued for collection; and implementing an enhanced dispute resolution process for consumers that are victims of fraud or identity theft or are involved in mixed files (where two consumer files are mistakenly mixed together). NCAP contained a phased implementation plan scheduled to be completed this year.

[14] *See Supervisory Highlights Consumer Reporting Special Edition* (Mar. 2, 2017), *available at* https://www.consumerfinance.gov/data-research/research-reports/supervisory-highlights-consumer-reporting-special-edition/.

[15] *See, e.g.*, National Consumer Assistance Plan, News Release (Jun. 9, 2016), *available at* http://www.nationalconsumerassistanceplan.com/news/news-release/.

IV. FTC ACTIVITIES TO PROMOTE CREDIT REPORT ACCURACY

A. Law Enforcement

FCRA enforcement continues to be a top priority for the Commission. With the advent in 2011 of the Bureau's supervisory authority over the nationwide credit bureaus and the coordination efforts between the agencies, the FTC has focused its FCRA law enforcement efforts on other entities in the credit reporting area and other aspects of the consumer reporting industry more broadly.

For example, the FTC settled cases against furnishers that allegedly had inadequate policies and procedures for reporting accurate credit information to CRAs. In *Credit Protection Association, LP*, the Commission alleged that a debt collector failed to have adequate policies and procedures to handle consumer disputes, did not have a policy requiring notice to consumers of the outcomes of investigations about disputed information, and in numerous instances failed to inform consumers of the outcome of disputes.[16] The settlement included $72,000 in civil penalties.[17] And, in *Tricolor Auto Acceptance, LLC*, the Commission alleged that the loan-servicing department of an auto dealer failed to have written policies and procedures designed to ensure that the credit information it reported to CRAs was accurate and failed to properly investigate consumer disputes regarding the accuracy of credit information.[18] The settlement included $82,000 in civil penalties.

---

[16] *U.S. v. Credit Protection Association, LP*, No. 3:16-cv-01255-D (N.D.Tex. filed May 9, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3142/credit-protection-association.

[17] As specified by the Federal Civil Penalty Inflation Adjustment Act of 1990, 28 U.S.C. § 2861, as amended by the Debt Collection Improvements Act of 1996, Pub. L. 104-134, § 31001(s)(1), 110 Stat. 1321-373, in relevant part, civil penalties under the FCRA are capped at $3,500 per violation for violations occurring before August 1, 2016, $3,756 per violation for violations occurring between that date and January 23, 2017, and $3,817 for violations occurring on or after January 24, 2017.

[18] *U.S. v. Tricolor Auto Acceptance, LLC*, No. 3:15-cv-3002 (N.D.Tex. filed Sept. 16, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3073/tricolor-auto-acceptance-llc.

In addition, the FTC has settled cases against background screening CRAs that compile background reports on consumers that may include driving records, employment and education history, eviction records, and criminal records for use in making employment and housing decisions. These settlements include allegations relating to inaccuracies in consumer reports, as well as failures to protect the privacy of consumer reports by ensuring permissible use. For example, in *InfoTrack Information Services, Inc.*, the Commission alleged that a background screening CRA failed to have reasonable procedures to ensure the maximum possible accuracy of consumer report information and, as a result, provided inaccurate information suggesting that job applicants potentially were registered sex offenders.[19] The settlement included $1 million in civil penalties, which was suspended upon payment of $60,000 based on inability to pay. In *Instant Checkmate, Inc.*, the Commission alleged that the CRA compiled public record information into background reports and marketed its services to landlords and employers but failed to comply with several FCRA provisions, including failing to maintain reasonable procedures to ensure the accuracy of its reports, failing to have reasonable procedures to ensure that those using its reports had permissible purposes for accessing them, and providing reports to users that it did not have reason to believe had a permissible purpose to receive them.[20] The settlement included $525,000 in civil penalties.

The FTC has also brought cases against check authorization CRAs for failing to comply with their accuracy obligations. Check authorization companies compile consumers' personal information and use it to help retail merchants throughout the United States determine whether to

[19] *U.S. v. Infotrack Information Services, Inc.*, No. 1:14-cv-02054 (N.D.Ill. filed Apr. 9, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3092/infotrack-information-services-inc-et-al.
[20] *U.S. v. Instant Checkmate, Inc.*, No. 3:14-cv-00675-H-JMA (S.D.Cal. filed Apr. 9, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc.

accept consumers' checks. In its settlements with *Telecheck*[21] and *Certegy*,[22] two of the nation's largest check authorization companies, the Commission charged these companies with failing to follow FCRA accuracy procedures, failing to follow proper procedures for consumer disputes, and failing to establish and implement reasonable written policies regarding the accuracy of information the companies furnish to other CRAs. The FTC obtained $3.5 million in civil penalties against each company.

B. Business Guidance and Consumer Education

The Commission also continues to educate consumers and businesses on their consumer reporting rights and obligations under the FCRA. The FTC has published guidance for employment and tenant background screening companies regarding their obligations under the FCRA, including with respect to accuracy and consumer disputes.[23] For furnishers, the FTC publication *Consumer Reports: What Information Furnishers Need to Know* provides an overview of obligations under the FCRA.[24] Similarly, for users of consumer reports, FTC guidance includes publications for employers, landlords, insurers, and creditors, as well as guidance on secure disposal of consumer information for all businesses.[25]

---

[21] *U.S. v. TeleCheck Services, Inc.*, No. 1:14-cv-00062 (D.D.C. filed Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc.

[22] *U.S. v. Certegy Services, Inc.*, No. 1:13-cv-01247 (D.D.C. filed Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc.

[23] *See What Employment Background Screening Companies Need to Know About the Fair Credit Reporting Act* (Apr. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/what-employment-background-screening-companies-need-know-about; *What Tenant Background Screening Companies Need to Know About the Fair Credit Reporting Act* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/what-tenant-background-screening-companies-need-know-about-fair.

[24] *See Consumer Reports: What Information Furnishers Need to Know* (Nov. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-information-furnishers-need-know.

[25] *See Consumer Reports: What Employers Need to Know* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-what-employers-need-know; *Consumer Reports: What Landlords Need to Know* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-what-landlords-need-know; *Consumer Reports: What Insurers Need to Know* (Nov. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-insurers-need-know; *Using Consumer Reports for Credit Decisions: What to Know About Adverse Action and Risk-Based Pricing Notices* (Nov. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-

The FTC also has a number of user-friendly resources for consumers designed to inform them of their rights under the FCRA and assist them with navigating the consumer reporting system. The publication *Credit and Your Consumer Rights* provides an overview of credit, explains consumers' legal rights, and offers practical tips to help solve credit problems.[26] The FTC also has publications that explain how consumers can obtain their free annual credit reports from each of the nationwide consumer reporting agencies[27] and use the FCRA's dispute procedures to ensure that information in their consumer reports is accurate.[28] For consumers seeking employment or housing, the FTC has materials on employment background checks[29] and tenant background checks.[30] The Commission continues to update and expand its materials as new issues arise.

V. DATA SECURITY

The FTC is committed to protecting consumer privacy and promoting data security in the private sector. The Commission is the nation's primary data security regulator and enforces several statutes and rules that impose data security requirements on companies across a wide spectrum of industries, including credit bureaus. Since 2001, the Commission has undertaken substantial efforts to promote data security in the private sector through enforcement of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, such as businesses making false or misleading claims about their data security procedures, or failing to employ reasonable

---

credit-decisions-what-know-about-adverse; *Disposing of Consumer Report Information? Rule Tells How* (Jun. 2005), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how.

[26] *Credit and Your Consumer Rights* (Jun. 2017), *available at* https://www.consumer.ftc.gov/articles/pdf-0070-credit-and-your-consumer-rights.

[27] *Free Credit Reports* (Mar. 2013), *available at* https://www.consumer.ftc.gov/articles/0155-free-credit-reports.

[28] *See Disputing Errors on Credit Reports* (Feb. 2017), *available at* https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports.

[29] *See Background Checks* (Mar. 2018), *available at* https://www.consumer.ftc.gov/articles/0157-background-checks.

[30] *See* FTC Consumer Blog, *Renting an apartment? Be prepared for a background check* (Nov. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how.

security measures.[31] The Commission is also the federal enforcement agency for the Children's Online Privacy Protection Act ("COPPA"), which requires reasonable security for children's information collected online.[32]

Further, the Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), sets forth data security requirements for financial institutions within the Commission's jurisdiction, which includes credit bureaus.[33] The Safeguards Rule requires financial institutions, or companies that are significantly engaged in offering consumer financial products or services, to develop, implement, and maintain a comprehensive information security program for handling customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The FTC has exclusive enforcement authority with respect to nonbank consumer financial services providers.

Finally, the FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they provide consumer reports have a permissible purpose for receiving that information[34] and also requires the secure disposal of consumer report information.[35] This section describes the FTC's efforts to enforce these laws, educate consumers and businesses, and develop policies in this area.

[31] 15 U.S.C. § 45(a). If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5. Further, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.
[32] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").
[33] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).
[34] 15 U.S.C. § 1681e.
[35] *Id.* § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

A. Law Enforcement

The Commission has brought over 60 law enforcement actions against companies that allegedly engaged in unreasonable data security practices. Last year, the Commission took the unusual step of publicly confirming its investigation into the Equifax data breach due to the scale of public interest in the matter.

The FTC has significant experience with enforcing data security laws against CRAs. In 2006, the FTC brought the seminal *Choicepoint* case against a CRA that sold consumer reports to identity thieves who did not have a permissible purpose to obtain the information under the FCRA, as well as failed to employ reasonable measures to secure the personal information it collected and misrepresented its security practices under Section 5 of the FTC Act.[36] The complaint alleged that ChoicePoint failed to monitor subscribers even after receiving subpoenas from law enforcement authorities alerting it to fraudulent activity. The settlement included injunctive relief, as well as $10 million in civil penalties—the largest FCRA civil penalty in FTC history—and $5 million in consumer redress. A few years later, the FTC settled another action against the company when it suffered a data breach because it turned off a key electronic security tool used to monitor access to one of its databases, in violation of the Commission's order.[37]

The Commission has also brought actions against companies for failing to dispose of consumer report information securely. For example, in the *PLS Financial Services, Inc.* case, the FTC alleged that the company violated the FCRA Disposal Rule by failing to take reasonable steps to protect against unauthorized access to credit reports in the improper disposal of the consumer information, violated the Safeguards Rule requirements for financial institutions to

[36] *U.S. v. Choicepoint, Inc.*, No. 1:06-cv-00198-GET (N.D.Ga. filed Jan. 30, 2006), *available at* https://www.ftc.gov/enforcement/cases-proceedings/052-3069/choicepoint-inc.
[37] *U.S. v. Choicepoint, Inc.*, No. 1:06-cv-00198-JTC (N.D.Ga. filed Oct. 19, 2009), *available at* https://www.ftc.gov/enforcement/cases-proceedings/052-3069/choicepoint-inc.

develop and use safeguards to protect consumer information, and violated the FTC Act by misrepresenting that it had implemented reasonable measures to protect sensitive consumer information.[38] The settlement included injunctive relief and $101,500 in civil penalties.

B. Business Guidance and Consumer Education

In addition to law enforcement, the FTC provides extensive business guidance on data security. The agency's goal is to provide information to help businesses protect the data in their care and understand what practices may violate the laws the FTC enforces. The FTC provides general business education about data security issues, as well as specific guidance on emerging threats.

In 2015, the FTC launched its *Start with Security* initiative, which includes a guide for businesses,[39] as well as 11 short videos,[40] that discuss 10 important security topics and give advice about specific security practices for each. In 2016, the FTC published a business advisory on how the National Institute of Standards and Technology Cybersecurity Framework applies to the FTC's data security work[41] and released an update to *Protecting Personal Information: A Guide for Business*, which was first published in 2007.[42] Last year, the FTC published its *Stick with Security* blog series offering additional insights into the *Start with Security* principles, based

[38] *U.S. v. PLS Financial Services, Inc.*, No. 112-cv-08334 (N.D.Ill. filed Oct. 17, 2012), *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023172/pls-financial-services-inc-et-al.
[39] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[40] *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), *available at* https://www.ftc.gov/news-events/audio-video/business.
[41] FTC Business Blog, *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
[42] *Protecting Personal Information: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

on the lessons of recent law enforcement actions, closed investigations, and experiences companies have shared about data security in their business.[43]

In addition to data security guidance, the FTC provides business guidance related to data breaches. In September 2016, the FTC released *Data Breach Response: A Guide for Business*,[44] and a related video, which describes immediate steps companies should take when they experience a data breach, such as taking breached systems offline, securing physical areas to eliminate the risk of further harm from the breach, and notifying consumers, affected businesses, and law enforcement. The guide also includes a model data breach notification letter businesses can use to get started.

The FTC also provides businesses with specific guidance on emerging threats. For example, most recently the FTC released a staff perspective and related blog post to help businesses prevent phishing scams.[45] Following a workshop,[46] the FTC published a blog post describing ransomware,[47] how to defend against it, and essential steps to take if businesses become victims.[48] Further, the FTC develops targeted guidance for companies in specific industries. For example, staff developed specific security guidance for debt buyers and sellers.[49]

---

[43] FTC Business Blog, *Stick with Security: A Business Blog Series* (Oct. 2017), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

[44] *Data Breach Response: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

[45] FTC Staff Perspective, *Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication* (Mar. 2017), *available at* https://www.ftc.gov/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff; FTC Business Blog, *Want to stop phishers? Use email authentication*, Mar. 3, 2017, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication.

[46] *Fall Technology Series: Ransomware* (Sept. 7, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.

[47] Ransomware is malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom.

[48] FTC Business Blog, *Ransomware – A Closer Look* (Nov. 10, 2016), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.

[49] *Buying or selling debts? Steps for keeping data secure* (Apr. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/buying-or-selling-debts-steps-keeping-data-secure.

The Commission also educates consumers on security. For example, the FTC has provided guidance for consumers on securing their home wireless networks, a critical security step for protecting devices and personal information from compromise. These resources are accessible on the FTC's consumer guidance website, consumer.ftc.gov. The FTC also assists consumers affected by data breaches through its identitytheft.gov website that allows consumers who are victims of identity theft to quickly file a complaint with the FTC and get a free, personalized guide to recovery that helps streamline many of the steps involved. In the wake of the announcement of the Equifax data breach last year, the agency published numerous materials and created a dedicated page on its website, ftc.gov/Equifax, with resources to educate consumers about fraud alerts, active duty alerts, credit freezes and locks, credit monitoring, and how to reduce the risk of identity theft.

C. Policy Initiatives

The FTC engages in a variety of policy initiatives to enhance data security. The FTC has hosted workshops and issued reports to highlight the privacy and security implications of new technologies. For example, last year the FTC hosted a workshop to examine consumer injury in the context of privacy and data security and various issues related to the injuries consumers suffer when information about them is misused.[50] Most recently, the Commission announced plans to hold a series of public hearings on the impact of market developments on competition and consumer protection enforcement, including the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters.[51]

---

[50] *Informational Injury Workshop* (Dec. 12, 2017), *available at* https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.

[51] Press Release, *FTC Announces Hearings On Competition and Consumer Protection in the 21st Century* (June 20, 2018), *available at* https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

VI. CONCLUSION

Thank you for the opportunity to provide the Commission's testimony on credit report accuracy and security. We look forward to continuing to work with Congress and this Committee on these important issues.