STATEMENT OF ANNE P. FORTNEY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON
DIGITAL COMMERCE AND CONSUMER PROTECTION

ON

Securing Consumers' Credit Data in the Age of Digital Commerce

NOVEMBER 1, 2017

Anne P. Fortney
Hudson Cook, LLP
1909 K Street N.W.
4th Floor
Washington, DC 20006

Summary of Prepared Statement

Consumers today are understandably concerned about the security of their personal identifying information and credit data held by large corporations, including credit reporting agencies and financial institutions.

The credit reporting industry has evolved to meet the need for data upon which banks and other creditors base their financial transactions with consumers. Credit reporting data enables creditors to provide consumers have access to credit at an efficient cost, promotes the safety and soundness of the banking system, and protects against fraud and other crime.

Federal law exists to protect the accuracy, confidentiality, and security of this personal data. The Fair Credit Reporting Act protects consumer data by limiting access to certain specified purposes, notifying consumers about the use of their information, and ensuring that credit data is accurate. The FCRA also protects against the risk of identity theft by allowing consumers to place fraud alerts on their credit files and to block the reporting of fraudulent information. The GLBA Privacy Rule limits how consumer data is shared with third parties, requires notice about how the data is used, and provides for an opt-out right for such sharing. The GLBA Safeguards Rule requires financial institutions (defined to include credit reporting agencies) to keep consumer data secure. Federal agencies, such as the CFPB and the FTC, enforce these laws. State laws and enforcement of those laws also protect consumers' financial data through their own versions of the FCRA, data security laws, and laws requiring data breach notification.

Thus, consumers have many tools through the credit reporting industry to manage and protect their nonpublic personal information. Consumers should use the tools at their disposal.

Prepared Statement

Chairman Latta, Congresswoman Schakowsky, and members of the Subcommittee, thank you for the opportunity to appear before the Subcommittee on Digital Commerce and Consumer Protection.

I am the partner emerita with the Hudson Cook law firm. Our firm specializes in consumer financial services; my practice involved primarily issues arising under consumer protection laws, including the Fair Credit Reporting Act (FCRA),[1] the Gramm-Leach-Bliley Act (GLBA) rules on consumer data privacy and information safeguards,[2] and similar laws. My experience with these laws included service as Associate Director for Credit Practices at the Federal Trade Commission (FTC), as in-house counsel at a retail creditor, and as a practitioner counseling clients on compliance. I also served as a consultant and an expert witness in litigation involving these consumer protection laws.[3] My career involved more than 40 years' experience with the operation of the consumer reporting industry and the use of consumer report and other nonpublic personal information by creditors and others in the consumer financial services industry.

Because of my extensive background and experience, I was particularly pleased to receive this Subcommittee's invitation to testify at this hearing on securing consumers' credit data in the age of digital commerce. Recent media reports and conversations with friends lead me to believe that consumers are understandably concerned about the security of their personal identifying information and credit data held by large corporations, including credit reporting agencies and financial institutions. At the same time, many consumers appear to lack sufficient information about the existing laws designed to protect the accuracy, confidentiality, and security of this

---

1 15 U.S.C. §§ 1681 *et seq.*

2 15 U.S.C. § 6801; GLBA § 501; 16 C.F.R. Parts 313, 314.

3 A detailed description of my background and experience is attached to this statement.

personal data. In addition, consumers may not know about the ways they can personally manage their financial data at credit reporting agencies.

I begin with a brief overview of the evolution and operation of the credit reporting industry in this country. I also discuss the corresponding evolution in the laws that govern this data and other nonpublic consumer financial data and in federal oversight of the industry. I explain how consumers can manage the accuracy and security of their nonpublic personal information, including credit report data. I conclude with suggestions for improving consumers' access to the benefits of the credit reporting industry.

I. Brief History of the Credit Reporting Industry

The credit reporting industry began with the population growth of towns and cities around this country in the late 19th century and with a corresponding growth in the number of customers at banks and retail establishments. Banks and merchants began exchanging information about their customers' behavior in repaying bank loans and merchants' store credit. These information exchanges became formalized in the collection and reporting of this information by trade associations or centralized bureaus. Over time these reporting agencies expanded to serve larger geographic areas, and the American credit reporting industry became increasingly concentrated in fewer companies serving certain regions of the country. Today, there are four principal consumer reporting agencies: Equifax, Experian, Trans Union, and Innovis. Thus, the credit reporting industry evolved to meet the need for data upon which banks and other creditors base their financial transactions with consumers.

The value of credit reporting data depends on the free collection of the data, and the value is greatest when both positive and negative data are included. While consumers do not choose for their data to be in credit reporting agencies, their participation in the consumer financial services

industry results in that data being available for creditors' use in providing credit and other financial products to them and to millions of other consumers.[4] The large data sets of consumers' credit information enables creditors to evaluate credit applicants relative risk and to provide products and services that meet individual consumers' needs. These data sets also provide the factual basis for credit scoring systems. Our consumer financial services industry is entirely dependent upon credit reporting agencies' data.

Moreover, consumers do not select the information collected and maintained by consumer reporting agencies. If they could so, consumers could remove negative, but accurate data.[5] Then, the entire data set would not reflect consumers' true credit risk and would be much less valuable in creditors' lending decisions. Lenders would need to compensate for the incomplete data by assuming less risk in extending credit, and would do so by stricter credit eligibility standards or higher interest rates and fees, or both.

The comprehensive consumer reporting network is an essential element of our consumer credit system, enabling creditors to make credit granting decisions quickly, accurately and efficiently. The benefits of this network include greater competition among creditors, lower credit costs for consumers and enhanced access to credit. The public also benefits when insurers, employers, landlords, merchants, banks, and others use the information to determine a consumer's eligibility for insurance, employment, a government license or for some other business transaction with the consumer (such as to cash a check or rent an apartment). [6]

---

[4] I discuss below how consumers can prevent or restrict the disclosure of their credit file information under certain circumstances.

[5] Consumers sometimes try to have negative, accurate information removed from their files at consumer reporting agencies by using the services of credit repair organizations ("CROs"). These CROs rarely fulfill their promises to remove this data, but to the extent that they succeed through abuse of the FCRA dispute system, they undermine the validity of the credit report data and jeopardize the safety and security of the consumer financial services industry.

[6] *See also* World Bank Credit Reporting Principles report Executive Summary, *available at* http://documents.worldbank.org/curated/en/662161468147557554/pdf/70193-2014-CR-General-Principles-Web-

Credit reporting agency information is also essential for creditors in processing an application for credit. In addition to use in evaluating the creditworthiness of a consumer, creditors must use the credit report information in order to comply with federal laws and regulations.

The Financial Crimes Enforcement Network, FinCEN, requires various players in the financial markets, including banks and credit unions, to 'know your customer,' meaning that they are required to verify the identity of each customer to the extent reasonable and practicable.[7] This requirement is important for safety and soundness, as well as anti-money laundering, reasons. These entities must obtain certain specified items of information and may do so by verifying identity information against information received from a consumer reporting agency.[8] Additionally, The federal banking regulators, through the Federal Financial Institutions Examination Council, the FFIEC, expect financial institutions to implement multifactor authentication controls to mitigate identity risks for certain high-risk transactions.[9] Financial institutions often use consumer report information to ask "out of wallet" questions to customers as part of multifactor authentication. Furthermore, the FFIEC and the banking regulators expect financial institutions to implement a Bank Secrecy Act/Anti-Money Laundering compliance program to ward against money laundering and terrorist financing.[10] Consumer report information is essential to effective customer due diligence.

Ready.pdf, which summarizes the benefits of credit reporting to a country's economy: "Credit reporting addresses a fundamental problem of credit markets: asymmetric information between borrowers and lenders, which may lead to adverse selection, credit rationing, and moral hazard problems." "In competitive markets, the benefits of credit reporting activities are passed on to borrowers in the form of a lower cost of capital, which has a positive influence on productive investment spending."

7 31 C.F.R. § 1020.220(a)(2).

8 31 C.F.R. § 1020.220(a)(2)(ii)(B)(1).

9 Authentication in an Internet Banking Environment (2005 Guidance), *available at* https://www.ffiec.gov/pdf/authentication_guidance.pdf; Supplement to Authentication in an Internet Banking Environment, *available at* https://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

10 FFIEC BSA/AML Examination Manual, Customer Due Diligence, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm.

The Red Flags Rule, promulgated under the FACTA amendments to the FCRA, requires creditors to implement an identity theft prevention program.[11] The program is required to detect whether there are "red flags" indicating identity theft. Consumer report information forms the basis for important red flags, like if there is a fraud alert or notice of address discrepancy, which are regulated by the FCRA,[12] or if a consumer report indicates a pattern of unusual account activity. Finally, the Truth in Lending Act now requires—after Dodd-Frank—that creditors make a reasonable and good faith determination based on verified and documented information that the consumer has a reasonable ability to repay a mortgage loan.[13] Regulation Z, which implements TILA, requires a creditor to consider a consumer's credit history and outstanding obligations, among other things, in deciding whether to extend credit,[14] verifying those items using third-party records like a credit report.[15]

Our credit reporting industry should not, and today does not, operate without regard for consumers' interest in the accuracy, transparency, confidentiality, and security of their consumer report data. As the credit reporting industry evolved, it became increasingly clear that industry standards were needed to protect consumers. The industry trade association, Associated Credit Bureaus,[16] developed such standards. Those became the foundation of the Fair Credit Reporting Act of 1970.

---

11 16 C.F.R. § 681.1(d)(1).
12 FCRA §§ 605(h), 605A, 605B; 15 U.S.C. §§ 1681c(h), 1681c-1, 1681c-2.
13 15 U.S.C. § 1639(c).
14 12 C.F.R. § 1026.43(c)(2).
15 12 C.F.R. § 1026.43(c)(3).
16 Associated Credit Bureaus was the successor to the Consumer Data Industry Association.

II. Fair Credit Reporting Act

A. Overview

When Congress enacted the Fair Credit Reporting Act, it recognized that the safety and soundness of the financial services industry depends on the availability of consumer credit report information.[17] Congress also found that consumers need legal protection with respect to the accuracy, fairness and confidentiality of the information:

> It is the purpose of this title to require that consumer reporting agencies 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 . . ..[18]

This balance of the industry's need for consumer reporting information and consumers' rights is at the foundation of the FCRA. The industry does not have an absolute right to disseminate and use the information, and consumers do not have an absolute right to the privacy of the data. There have been two significant sets of amendments to the FCRA (in 1996 and 2003), and today the Act balances the competing needs of industry with consumers' rights with respect to confidentiality, accuracy, transparency and access, data security and identity theft protection. In the process, the FCRA provides the legal framework for the efficient, fair, and cost-effective credit marketplace upon which our economy depends.

B. Confidentiality and Security

The FCRA's protections for the confidentiality of consumer report data also protect the data from unauthorized access.

The FCRA requires a consumer reporting agency to:

---

[17] FCRA § 602(a); 15 U.S.C. § 1681(a).
[18] FCRA § 602(b); 15 U.S.C. § 1681(b).

- Maintain reasonable procedures to limit the release consumer reports only to persons having a statutorily defined "permissible purpose" to obtain it.[19]
- Require that prospective users of consumer report information identify themselves, certify the purpose for which the information is sought and certify that the information will be used for no other purpose.[20]
- Maintain reasonable procedures to verify the identity of the person seeking the information and the existence of a permissible purpose.[21]
- Maintain reasonable procedures to avoid releasing consumer information to any person not legally authorized to have it or for an unauthorized purpose.[22]
- Keep accurate records of every person who receives a report on a particular consumer and disclose to the consumer on request the identities of these recipients.[23]

C. Transparency and access

Consumers regularly receive notice about the use of credit reports:

- Applications for credit usually include a notice that the lender is will consult with and report data to a consumer reporting agency. These notices typically appear in bold print immediately above the borrower's signature space.
- The FCRA requires lenders to notify consumers if they furnish to a consumer reporting agency, including instances when they furnish negative data.[24] This notice is typically included in every monthly billing statement sent to the consumer.
- Financial institutions that share data with third parties, including consumer reporting agencies, are required to provide privacy notices with detailed information on the covered entity's practices with respect to the sharing of this information.[25] These statements typically inform consumers that information is shared with consumer reporting agencies. These privacy notices are provided when the individual becomes a client of the covered institution and may be sent annually to customers.[26]
- The user of a consumer report that takes "adverse action" against a consumer based in whole or part on information in a consumer report must inform the consumer of the action and of the consumer's rights under the law, including the right to receive a free credit report.[27]

---

19 FCRA §§ 604(a), 607(a); 15 U.S.C. §§ 1681b(a), 1681e(a).
20 FCRA § 607(a); 15 U.S.C. § 1681e(a).
21 *Id.*
22 *Id.*
23 FCRA § 609(a)(3); 15 U.S.C. § 1681g(a)(3).
24 GLBA § 502(a); 15 U.S.C. § 1681s-2(a).
25 15 U.S.C. § 6802(a).
26 16 C.F.R. §§ 313.4, 313.5.
27 FCRA § 615(a); 15 U.S.C. § 1681m(a).

- When the user of a credit report engages in "risk-based pricing" using credit report information, the user must give the consumer a risk based pricing notice or a credit score disclosure.[28] These notices include the consumer's own credit score and the key factors that have negatively affected the score (such as the number of delinquencies, or the existence of a bankruptcy, etc.). They also educate consumers about credit scoring and explain how the consumer's credit score compares to those of other consumers.[29]
- Through the credit score initiative of the Consumer Financial Protection Bureau ("CFPB"), creditors regularly provide their customers with free credit score disclosures.

In addition, under the FCRA, consumers have the right to see all the information about them in a consumer reporting agency's files at any time and may receive a free credit report annually from each of the credit reporting agencies that operate on a nationwide basis.[30] In addition, consumers are entitled to a free credit report upon the consumer's request:

- When the credit report is used in whole or in part by the user in making an "adverse action" determination with respect to the consumer;[31]
- When a notification from a debt collection agency affiliated with the consumer reporting agency stating that the consumer's credit rating may be or has been adversely affected;[32] and
- Annually, if the consumer certifies in writing that the consumer –
    - is unemployed and intends to apply for employment in the 60-day period beginning on the date on which the certification is made;
    - is a recipient of public welfare assistance; or
    - has reason to believe that the file on the consumer at the agency contains inaccurate information due to fraud.[33]

---

28 12 C.F.R. § 1022.72.
29 12 C.F.R. § 1022.73.
30 FCRA § 612(a); 15 U.S.C. § 1681j(a).
31 FCRA § 612(b); 15 U.S.C. § 1681j(b).
32 *Id.*
33 FCRA § 612(c); 15 U.S.C. § 1681j(c).

A consumer may also receive a free credit report from a nationwide consumer reporting agency when the consumer places a fraud alert on his or her credit file at the consumer reporting agency,[34] as further explained below.

Thus, Congressional policy has made the transparency of credit reports and credit scores a top priority. An estimated 120 million credit-score disclosures are distributed each year to consumers when they apply for a mortgage, are denied credit or are offered less favorable credit terms by a lender. In addition, CFPB estimates that roughly 50 million credit scores are delivered to consumers on their monthly billing statements through the scores on statements initiative.[35]

D. Accuracy and Consumer Dispute Resolution

A consumer reporting agency must maintain reasonable procedures to assure the maximum possible accuracy of the consumer report information before releasing it.[36] In addition, consumers have the right to dispute inaccurate information free of charge. [37] If the consumer reporting agency cannot verify the accuracy of the information, it must be corrected or deleted, and the agency must report the results of its determination to the other two consumer reporting agencies.[38] If the dispute is not resolved to the consumer's satisfaction, consumer reporting agencies must allow consumers to include in their file a brief statement that the consumer believes the information to be incomplete or inaccurate.[39]

---

34 FCRA § 612(d); 15 U.S.C. § 1681j(d).

35 CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Reports That More Than 50 Million Credit Card Consumers Have Access to Free Credit Scores" (February 19, 2015), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-reports-that-more-than-50-million-credit-card-consumers-have-access-to-free-credit-scores/.

36 FCRA § 607(b); 15 U.S.C. § 1681e(b).

37 FCRA §§ 611, 623; 15 U.S.C. §§ 1681i, 1681s-2.

38 FCRA § 611(a)(5); 15 U.S.C. § 1681i(a)(5).

39 FCRA § 611(b); 15 U.S.C. § 1681i(b).

II. Other Data Security and Privacy Laws

Consumer data held by consumer reporting agencies is also subject to regulation and protection under other privacy and data security laws. The following is a brief summary of the federal and state regulation of consumers' privacy and data security.

A. GLBA Privacy Rule

The GLBA Privacy Rule seeks to protect consumer financial privacy by providing consumers with notice and choice. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties.[40] The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities."[41] Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties.[42] In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.[43]

The FTC, the federal banking agencies, other federal regulatory authorities such as the Securities and Exchange Commission, and state insurance authorities enforce the GLBA Privacy Rule.[44] Each agency has issued substantially similar rules implementing GLB's privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance

---

40 16 C.F.R. § 313.1(a)(2)
41 16 C.F.R. § 313.3(k).
42 16 C.F.R. § 313.6.
43 16 C.F.R. §§ 313.10, 313.11.
44 15 U.S.C. § 6805.

providers.[45] The FTC has jurisdiction over any financial institution or other person not regulated by other government agencies.[46]

The FTC may bring enforcement actions for violations of the Privacy Rule. The FTC can bring actions to enforce the Privacy Rule in federal district court, where it may seek the full scope of injunctive and ancillary equitable relief.[47]

B. GLBA Safeguards Rule

The GLBA also requires "financial institutions" to ensure the security and confidentiality of the information they maintain on consumers through appropriate safeguards.[48] As with the Privacy Rule, the definition of "financial institution" includes many businesses beyond traditional banks – it applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services.[49] This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers. The GLBA security and confidentiality requirements also apply to companies like credit reporting agencies and payment processors that receive information about the customers of other financial institutions. In addition to developing their own safeguards, financial institutions covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.[50]

The provisions are enforced through the Interagency Guidance issued by the Federal Reserve and the other banking prudential regulators,[51] and through the Safeguards Rule issued by

---

45 15 U.S.C. § 6805(a)(6).
46 15 U.S.C. § 46.
47 15 U.S.C. § 45.
48 16 C.F.R. § 314.3.
49 16 C.F.R. § 314.2(a).
50 16 C.F.R. § 314.4.
51 66 Fed. Reg. 8616 (Feb. 1, 2001).

the FTC.[52] Financial institutions are required to develop an information security plan that describes their program to protect 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. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure their contracts require them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[53]

The requirements are designed to be flexible. Financial institutions should implement safeguards appropriate to their own circumstances. Financial institutions must consider and address any unique risks raised by their business operations, such as the use and location of service providers and data storage facilities.[54]

C. FTC Regulation of Data Security

In addition to enforcing the FCRA and the GLBA privacy and safeguards rule, the FTC uses its enforcement authority under Section 5 of the FTC Act to pursue companies that misrepresent their data security practices or that lack adequate data security measures.[55] Since

---

[52] 16 C.F.R. Part 314.

[53] 16 C.F.R. § 314.4.

[54] *See, e.g.,* 12 C.F.R. Part 30, app. B.

[55] Section 5 prohibits unfair or deceptive acts or practices and provides that an act or practice is unfair if the act or practice (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(a) and (n). *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), *available at* https://fas.org/sgp/crs/misc/R43723.pdf.

2001, the FTC has used its authority to bring enforcement action and obtain settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information. [56]

In addition to the identitytheft.gov website, the FTC has a number of resources to help consumers protect their sensitive information and the steps that a consumer may take if their information is the subject of a breach.[57] The FTC's consumer resources include information about online privacy, computer security, malware, and mobile device security.

D. CFPB Enforcement of Unfair, Deceptive or Abusive Acts or Practices ("UDAAP")

The Consumer Financial Protection Act authorizes the CFPB to enforce civil penalties against entities within its jurisdiction that commit UDAAP violations.[58] The CFPB has used this civil penalty authority in the data security context. In an action against a company for allegedly deceiving consumers about its data security and the security of its online payment platform, the CFPB required the company to enact comprehensive data security measures and policies, including a program of risk assessments and audits, to train employees on the company's data security policies and procedures, and on how to protect consumers' sensitive personal information, to fix any security weaknesses found in its web and mobile applications, and securely store and transmit consumer data, and to pay a $100,000 civil money penalty.[59]

---

[56] FEDERAL TRADE COMMISSION, "Prepared Statement of the Federal Trade Commission on Small Business Cybersecurity: Federal Resources and Coordination Before the Committee on Small Business" (March 8, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1174903/p072104_commission_testimony.pdf.

[57] FEDERAL TRADE COMMISSION, "Privacy, Identity & Online Security," *available at* https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

[58] 12 U.S.C. §§ 5536(a)(1)(b), 5565(c).

[59] CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices" (March 2, 2016) *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

Like the FTC, the CFPB has put out resources to help consumer understand the ways in which they can protect themselves from identity theft.[60]

E. State Attorneys General Enforcement of Data Security Laws

Many state laws regulate aspects of data security that impose obligations on consumer reporting agencies. These laws are categorized as follows:

- General data security laws: at least 13 states require businesses that own, license, or maintain personal information to implement and maintain reasonable security procedures and practices and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. The law in Massachusetts includes 30 discrete obligations concerning administrative, technical, and physical safeguards that organizations must satisfy when handling sensitive personal information.
- Social Security Numbers ("SSN") confidentiality laws: The majority of states require organizations to protect the confidentiality of SSNs.
- Data disposal laws: The majority of states have enacted laws requiring secure disposal of sensitive personal information.

F. State Data Breach Notification Laws

Nearly every U.S. State, the District of Columbia, and several U.S. territories, have enacted laws requiring notification to affected individuals in the event of a security breach of personal information. Most of these laws exempt financial institutions that are supervised by prudential banking regulators and subject to the GLBA Interagency Guidance, discussed above. Consumer reporting agencies are not exempt and must comply with the more than four dozen breach notification laws in the event of a breach.

E. Identity Theft Protections

The 2003 amendments to the FCRA added new protections for consumers against identity theft and other unauthorized access to and use of their data at consumer reporting agencies. These

---

[60] CONSUMER FINANCIAL PROTECTION BUREAU, "Identity Theft Protection Following the Equifax Data Breach" (September 9, 2017) *available at* https://www.consumerfinance.gov/about-us/blog/identity-theft-protection-following-equifax-data-breach/.

protections include the placement of fraud alerts and blocking the reporting of credit report data that reflects identity theft.[61]

1. Fraud Alerts

Under the FCRA, when consumers believe that they may be at risk of fraud or identity theft, they may place fraud alerts on their credit reporting files. There are two kinds of alerts: initial fraud alerts and extended fraud alerts.

A consumer may place an initial alert at no charge by phone, in writing or via the website of any one of the three nationwide credit reporting agencies, and the fraud alert is automatically shared with the other two agencies. An initial fraud alert lasts for 90 days and is renewable upon the consumer's request. When requesting an initial fraud alert, the consumer also may request one free credit report. When a fraud alert is on a consumer's credit file, creditors 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 an existing line of credit.[62]

An extended alert is available for consumers who have become victims of identity theft, but still wish and expect to be credit active. The FCRA allows for a consumer to place an extended alert on the consumer file at no charge for seven years by presenting a copy of a law enforcement report or an FTC identity theft report, which is available at www.identitytheft.gov. Similar to the initial fraud alert, an extended fraud alert filed with one bureau is automatically shared with the other two consumer reporting agencies. However, in contrast to the initial fraud alert, an extended alert requires lenders to actually contact the consumer before extending a new line of credit, increasing a line of credit or issuing a new or replacement card. A consumer can receive two additional free credit reports from each of the three consumer reporting agencies within twelve

---

61 FCRA §§ 605A, 605B; 15 U.S.C. §§ 1681c-1, 1681c-2.

62 FCRA § 605A(a); 15 U.S.C. § 1681c-2(a).

months of placing the extended alert. In addition, the consumer's name is taken off marketing lists for prescreened credit offers for five years.[63]

2. Credit Report Tradeline Blocking

When a consumer observes information in her credit file that is the result of identity theft, she can require the consumer reporting agency to block the reporting of that information. The consumer must: provide appropriate proof of identification and a copy of an identity theft report, tell the consumer reporting agency what information is to be blocked; and provide a statement that the information does not relate to the consumer's transaction. Once the consumer reporting agency receives an appropriate tradeline block information, the agency must stop reporting the information and must inform the furnisher.[64]

F. State Versions of the FCRA and Security Freeze Laws

Many states have enacted their versions of the FCRA in order to further protect consumers under state law.[65] In addition, every State has enacted laws permitting consumers to place a security freeze on the consumer file at each credit reporting agencies. Security freezes may protect consumers from identity theft and may also be used by consumers who do not plan to be credit active. When a freeze is in place, the consumer's file cannot be accessed for purposes involving extension of new or existing credit unless the consumer contacts the credit bureau to lift the freeze.

---

63 FCRA § 605A(b); 15 U.S.C. § 1681c-1(b). The FCRA also permits individuals on active duty to place active duty alerts. § 605A(c); 15 U.S.C. § 1681c-1(c).

64 FCRA § 605B; 15 U.S.C. § 1681c-2.

65 *See, e.g.,* Ariz. Rev. Stat. §§ 44-1691 *et seq.*; Cal. Civ. Code §§ 1785.1 *et seq.*; Conn. Gen. Stat. §§ 36a-695 *et seq.*; Kan. Stat. Ann. §§ 50-701 *et seq.*; LSA-R.S. 9:3571 *et seq.*; Md. Com. Code §§ 14-1201 *et seq.*; Ma. Ann. Laws Ch. 93, §§ 50 *et seq.*; Mont. Code Ann. §§ 31-3-101 *et seq.*; Nev. Stat. §§ 598C.010 *et seq.*; N.H. Rev. Stat. §§ 359-B *et seq.*; N.J. Stat. Ann. §§ 56:11-29 *et seq.*; N.M. Stat. Ann. §§ 56-3-1 *et seq.*; N.Y. Gen. Bus. §§ 380 *et seq.*; Tex. Bus. & Com. Code Ann. §§ 20.01 *et seq.*; 9 V.S.A. §§ 2480a *et seq.*; Wash. Rev. Code Ann. §§ 19.182.005 *et seq.*

Some states further prohibit releasing a frozen file for purposes involving insurance, rental housing, employment, telephone services, utilities, or government benefits.[66]

A freeze remains on the file until the consumer lifts or removes the freeze using a PIN provided at the time of placement. State law permits a fee for placing, lifting and replacing a freeze. These fees are typically between $5-$10 per transaction to impose or lift the freeze, unless the consumer is an identity theft victim.[67]

III. Consumers' Rights and Control Over Personal Data and Consumer Reports

It should now be clear that consumers' personal data at consumer reporting agencies is protected by a comprehensive regulatory scheme at the federal and state level. These laws also provide notice to consumers about the use and their access to consumer report information. Consumers can protect themselves in the following ways:

- Request copies of their credit report from the nationwide consumer reporting agencies.
- Review the contents of the reports for apparent inaccuracies or suspicious activity.
- Dispute any information that the consumer believes to be inaccurate or incomplete with the consumer reporting agency and/or the creditors that provided the information to the agency.
- Read their credit card statements and immediately notify the card issuers of any errors or other billing disputes.
- Check their credit scores when their credit card companies offer that information.
- Read the privacy notices that financial institutions must send if they share the consumers' nonpublic personal information with affiliates for marketing purposes or with nonaffiliated third parties. Opt-out of the disclosure of information when the consumer can restrict its being shared with others.

---

[66] *See, e.g.,* Cal. Civ. Code § 1785.11.2(l); Conn. Gen. Stat. Ann. § 36a-701a(g); Idaho Code Ann. § 28-52-105; La. Stat. Ann. § 9-3571.1(V); Me. Rev. Stat. Tit. 10 § 1310(1)(M); Mich. Comp. Laws Ann. § 445.2513; Minn. Stat. Ann. § 13C.016 subd. 6; Miss. Code Ann. § 75-24-209; Mo. Ann. Stat. § 407.1382(4); Mont. Code Ann. § 30-14-1734(1); Nev. Rev. Stat. Ann. § 598C.380; N.J. Stat. Ann. § 56:11-46(l); N.Y. Gen. Bus. Law § 380-t(m); Tex. Bus. & Com. Code Ann. § 20.038; Utah Code Ann. § 13-45-203; Wash. Rev. Code Ann. § 19.182.170(14); Wyo. Stat. Ann. § 40-12-505.

[67] For those consumers who are not identity theft victims, most states permit one or all of these fees to be charged. *See, e.g.,* Ala. Code § 8-35-2; Cal. Civ. Code § 1785.11.2(m); D.C. Code Ann. § 28-3862; Ga. Code Ann. § 10-1-914; Kan. Stat. Ann. § 50-723(j); Mo. Ann. Stat. § 407.1382(2); N.H. Rev. Stat. Ann. § 359-B:24(I)(b); Ten. Code Ann. § 47-18-2108; and 9 V.S.A. § 248oh(a).

- Read prescreening notices and opt-out of receiving prescreened solicitations if the consumer chooses to do so.[68]

In addition, if consumers are concerned that their credit report data has been hacked or otherwise disclosed to an unauthorized person, consumers can take the following steps to protect themselves from the risk of identity theft or other misuse of the data:

- Place an initial fraud alert, an extended fraud alert, or an active duty alert on the consumer's file at a nationwide consumer reporting agency and obtain a free credit report.
- Enroll in a credit monitoring service. When consumers' sensitive identifying information or credit report information has been involved in a data security breach at a financial institution or credit reporting agency, consumers are usually offered credit monitoring services at no charge for a certain period of time.
- Obtain a security freeze on the consumer's file at the consumer reporting agency. While the freeze may prevent third-party access to the consumer's file, the consumer can obtain credit only by taking the step of contacting the consumer reporting agency in advance of applying for credit and arranging for the freeze to be lifted. For this reason, consumers who are credit active and/or are seeking employment, housing or utility services may find that having a freeze, and then needing to lift it, significantly slows transactions. Presuming the consumer has kept the PIN, most state laws require the consumer reporting agency to lift the freeze within three days of being contacted. Many times, a freeze can be lifted more quickly, but it is not always instantaneous. For example, if the consumer does not have his or her PIN, then the consumer reporting agency must authenticate and verify the consumer, which may take several days, especially if accomplished through the postal system. In addition, because of the unique characteristics of each consumer reporting agencies' system and the fact that a unique PIN must be provided to each consumer from each bureau, security freezes cannot be shared across bureaus and the consumer must place the security at each bureau independently. Thus, a security freeze may delay the consumer's application for credit. So, this option may be the consumer's choice as long as the consumer accepts the consequences of the freeze.

[68] Pre-screened offers of credit and insurance must include a notice informing the consumer that he has been selected to receive the offer because of prescreening. The notice must also tell the consumer how to opt-out of receiving pre-screened solicitations. FCRA § 604(c); 15 U.S.C. § 1681b(c); 16 C.F.R. Part 642.

IV. Conclusion

The laws governing the consumer reporting industry reflect the balance between (a) creditors' need for credit history data in providing credit products and services to consumers in a fair and efficient manner and (b) consumers' needs for privacy, accuracy, and security of the data. As a result, the regulatory controls in place ensure that consumer information is accurate and kept confidential and secure, while also ensuring the availability of the data upon which the consumer financial services industry depends.

These laws also give consumers the tools necessary to ensure the accuracy and completeness of the data, to protect their personal information for its intended use, and to guard against identity theft.