Responses to Additional Questions for the Record

Questions from the Honorable Robert E. Latta:

Question 1. What regulations currently exist that require CRAs to put in place reasonable practices to protect against cyber-attacks?

Response: As explained in my Prepared Statement, the security and confidentiality requirements of the Gramm-Leach Bliley Act ("GLBA") apply to "financial institutions," a term which is broadly defined to include consumer reporting agencies ("CRAs"). The Federal Trade Commission's Safeguards Rule, 16 C.F.R §§ 314.1 *et seq.*, which implements the GLBA's data security requirements, applies also to CRAs.

The Safeguards Rule establishes the standards for "developing, implementing, and maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information."[1] The Rule makes clear that these standards apply to "any record" containing "nonpublic personal information," another term that is very broadly defined, about a customer that is handled or maintained by the financial institution or its affiliates.[2]

Because the risks encountered by financial institutions, including CRAs, vary with the types of products and services they provide to consumers, the Safeguards Rule imposes a compliance requirement that takes into account the "nature and scope" of the financial institution's activities as well as the "sensitivity of any customer information" that is handled or maintained.[3] That is, the Rule provides a rigorous standard that is designed to be flexible depending upon the identified risks presented by the financial institution's specific business and the types of data received and maintained. Understanding that this obligation is risk-based is critical to recognizing the valuable role the Rule plays in ensuring that customer information is adequately protected.

To meet the Safeguard Rule's standards, a financial institution's written Information Security Program ("ISP") must:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[4]

The written ISP must include a number of required elements designed to ensure that the above-identified objectives are met. These include the following:

1. That one or more employees be specifically designated to coordinate the ISP;

[1] 16 C.F.R. § 314.1.
[2] 16 C.F.R. § 314.2(b).
[3] 16 C.F.R. § 314.3(a).
[4] 16 C.F.R. § 313.3(b).

2. That a risk assessment be completed to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the customer information handled or maintained. Part of this risk assessment must also include the consideration of how the financial institution will detect, prevent and respond to attacks, intrusions and other events that compromise the security of the system;

3. That the implemented safeguards be designed to address the risks identified through the risk assessment. That these safeguards are adequate is ensured by the requirement that the safeguards be regularly tested and monitored to ensure their effectiveness;

4. That any service providers used by the financial institution be overseen to ensure that they too take the steps required to safeguard any customer information that is entrusted to them or that they receive or maintain on behalf of the financial institution; and

5. That the ISP be regularly evaluated and adjusted in light of the results of the required ongoing testing and monitoring to ensure the ISP's continued effectiveness.[5]

The above summarizes just the Safeguard Rule's protections. The Fair Credit Reporting Act ("FCRA") includes its own protections governing the confidentiality of consumer information. For example, the FCRA protects against unauthorized access to consumer report information by imposing the following requirements:

1. CRAs must maintain reasonable procedures to limit the release of consumer report information to only those persons who have a statutorily defined "permissible purpose" to obtain such information; [6]

2. CRAs must require that any person seeking to obtain consumer report information identify themselves, certify the permissible purpose for which the information is sought and certify that the information will be used for no other purpose;[7]

3. CRAs must maintain reasonable procedures to verify the identity of the person seeking the consumer report information and the existence of the permissible purpose certified by the person; [8] and

[5] 16 C.F.R. § 314.4. More information about these requirements may be found on the FTC website: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.
[6] 15 U.S.C. §§ 1681b(a), 1681e(a).
[7] 15 U.S.C. § 1681e(a).
[8] *Id.*

4. CRAs must keep accurate records of every person who receives a consumer report on a particular consumer and, upon the consumer's request, disclose that information to the consumer.[9]

The above FCRA provisions protect consumer report information in two-ways. First, they ensure that only authorized recipients receive the information. Second, they ensure that consumers are able to monitor who receives their information.

In addition to the protections identified above, both the FTC and the Consumer Financial Protection Bureau ("CFPB") have used their authority to bring enforcement actions when data security violations have been identified.

The FTC uses its authority under Section 5 of the FTC Act to pursue companies that misrepresent their data security practices or that lack adequate data security measures.[10] Since 2001, the FTC has used this authority to bring enforcement actions and obtain settlements in approximately 60 cases against businesses that the FTC charged with failing to provide reasonable and appropriate protections for consumer information. [11]

Similarly, the CFPB has used its authority under the Consumer Financial Protection Act ("CFPA") to pursue actions against entities within its enforcement jurisdiction when they commit unfair, deceptive or abusive practices.[12] The CFPB used this authority to obtain civil penalties in the data security context from a company that allegedly deceived consumers concerning the company's data security practices and the security of the company's online payment platform.[13]

[9] 15 U.S.C. § 1681g(a)(3).

[10] 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.

[11] 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.

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

[13] 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/.

Question 1a. Are there any specific gaps in regulation that led to the Equifax breach or was that the result of Equifax simply not doing what they were required to do?

Response: I have not been in a position to investigate the circumstances leading to the Equifax security incident. Rather, my knowledge of the incident is limited to what has been publicly reported in the media and the information available through Equifax's website.[14]

Based on this information, it does not appear that there are gaps in regulation that led to the incident. Moreover, the fact of a breach alone does not establish that the company which was the subject of the breach violated the law. Federal and state regulators recognize that there is no such thing as perfect data security:

> Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[15]

As was explained in response to Question 1, the existing regulatory framework already includes stringent requirements that a CRA protect the security and confidentiality of consumer information. Based on media reports, it appears that Equifax detected the breach, investigated its cause, took steps to stop the breach, notified law enforcement, notified affected consumers who were entitled to direct notice and offered all affected consumers additional tools to protect their identity.[16]

The GLBA and its implementing Safeguards Rule reflect a Congressional and Regulatory balancing of interests between (a) protecting consumer information and (b) ensuring that consumer information is available for limited use and disclosure by financial institutions that provide important products and services to consumers. There are tens-of-thousands of such financial institutions in the U.S. That significant data breaches are so rare that when they occur they draw national media attention is a strong indication that Congress and the FTC have struck the correct balance.

Because my knowledge of the Equifax breach is limited to what is publicly available, I can't comment further on what Equifax may or may not have done prior to the incident.

---

[14] *See,* Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/.

[15] *Commission Statement Marking the FTC's 50th Data Security Settlement*, Federal Trade Commission, Jan. 31, 2014, available at https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[16] *See,* Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/frequently-asked-questions/

Question 2. **Would extending the existing data security requirements for financial institutions to credit bureaus and other companies that sell credit reports have a meaningful mitigating effect on future data breaches?**

Response: As noted in my response to Question 1 above, the FTC's Safeguards Rule already applies to consumer reporting agencies ("CRAs"). The FTC Rule is similar to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information that apply to institutions supervised by the federal financial institution regulatory agencies (the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency). Both the FTC Rule and the Interagency Guidelines were mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999, and both the Rule and the Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of nonpublic personal information.

In addition, as noted in connection with the more than 60 enforcement actions pursued by the FTC against companies who failed to provide adequate protections for consumer information, federal regulators already have strong available tools for ensuring that consumer report information and other information on consumers is protected by applicable law.[17]

Question 3. **What are the Gramm-Leach-Bliley Act consumer protection provisions in force today to ensure financial institutions, like the CRAs, protect consumer's financial information?**

Response: Please see my response to Question 1 which outlines the protections available under the FTC's Safeguards Rule, implementing the Gramm-Leach Bliley Act ("GLBA").

Question 4. **What are the Fair Credit Reporting Act consumer protection provisions in force today to ensure financial institutions, like the CRAs, protect consumer's financial information?**

Response: Please see my response to Question 1 which outlines some of the protections available under the Fair Credit Reporting Act ("FCRA"). Moreover, the FCRA requires that "consumer information," which is any information that is a consumer report or is derived from a consumer report, be disposed of a manner that "protects against unauthorized access to or use of the information…."[18] In addition, the FCRA imposes upon financial institutions and other creditors the obligation to develop and implement identity theft protection programs that are "appropriate to the size and complexity of the financial institution or creditor and the nature

[17] 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.

[18] 15 U.S.C. § 1681w(a); 16 C.F.R. § 682.3.

and scope of its activities."[19] The program must include policies and procedures for responding to security incidents that result in unauthorized access to customer account information held by the financial institution or creditor.[20]

The FCRA also includes provisions which protect consumer information from misuse and provide consumers with powerful tools for protecting themselves from identity theft. These include:

1. The financial institution's obligation to respond to information requests from victims of identity theft by providing the consumer, who provides proper identification, with the business transaction records resulting from the alleged identity theft;[21]

2. The financial institution's obligation to reconcile address discrepancies between the user's file information maintained by the CRA and the address information the user receives from the consumer;[22]

3. The consumer's ability to place fraud alerts in their consumer report file which prohibit the recipients of consumer reports containing such alerts from establishing new accounts or extending credit without first using procedures that are designed to allow the user to form a reasonable belief that it knows the identity of the consumer requesting the credit;[23]

4. The consumer's ability to request that the CRA block the furnishing in a consumer report of any information the consumer identifies as resulting from identity theft;[24] and

5. Limiting the printing of a consumer's credit card number on an electronically printed receipt to just the last 5 digits of the number.[25]

Question 4a. **Under the Fair Credit Reporting Act, a consumer reporting agency may divulge a consumer report only under certain, enumerated conditions, "and no other." In your opinion, would it be a violation of this provision for a credit reporting agency to allow cyber-criminals to access a person's credit report?**

Response: Because a consumer reporting agency's ("CRA's") business depends upon the integrity of the information in its consumer reporting databases, it is inconceivable that it would "allow" a cyber-criminal to access its information systems to obtain a person's consumer

[19] 16 C.F.R. § 681.1(d).
[20] 16 C.F.R. Pt. 681, App. A, Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation.
[21] 15 U.S.C. § 1681g(e).
[22] 15 U.S.C. § 1681c(h); 16 C.F.R. § 641.1
[23] 15 U.S.C. § 1681c-1(h).
[24] 15 U.S.C. § 1681c-2(a).
[25] 15 U.S.C. § 1681c(g).

report. As noted in my response to Question 1, the FCRA requires CRAs to maintain reasonable procedures designed to limit the furnishing of consumer reports to the one of the statutorily defined "permissible purposes." These procedures must require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. In addition, every CRA must make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing a consumer report. No CRA may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a "permissible purpose."[26] If a CRA follows these requirements in providing a consumer report, it should not be liable under the FCRA, even if the user of that report lacks a permissible purpose.

If a CRA failed to have reasonable procedures to avoid providing a consumer report to a person, including a cyber-criminal, that lacked a "permissible purpose," the CRA could be liable under the FCRA. However, if a CRA had insufficient information security safeguards and those deficient safeguards provided a means by which a cyber-criminal could access the information maintained by the CRA for consumer reporting purposes, such a deficient Information Security Program ("ISP") would not be a violation of the FCRA's permissible purpose provisions, but could be a violation of the Safeguards Rule (discussed in response to Question 1 above).

Question 5. **Under the Dodd Frank Act, the Consumer Credit Protection Bureau was given authority to supervise the CRAs. Would that authority have allowed CFPB to direct the CRAs to take steps to ensure they did not allow unauthorized access to individual credit reports?**

Response: The CFPB has supervisory authority over nationwide CRAs with respect to their compliance with certain enumerated consumer financial laws, including the FCRA and CFPA's prohibitions against engaging in unfair, deceptive, or abusive acts and practices.

The CFPB's Examination Procedures for CRAs that are larger participants makes clear that the CFPB has the authority to examine CRAs to determine their compliance with the FCRA's permissible purpose provisions.[27] It also makes clear that this examination process is very detailed, requiring the CRAs to respond to multiple requests for information and documents. These requests are all intended to assess whether the CRAs have the required policies and procedures in place to ensure that consumer report information is only released to those users who have a permissible purpose, have certified that permissible purpose to the CRAs, and for whom the CRAs have completed the process of verifying both the identity of the user and the validity of the certified permissible purpose.[28]

[26] 15 U.S.C. §§ 1681b(a), 1681e(a).
[27] *See,* CFPB Examination Procedures, Consumer Reporting Larger Participants at Procedures 16-19, available at http://files.consumerfinance.gov/f/201209_cfpb_Consumer_Reporting_Examination_Procedures.pdf.
[28] *Id.*

The result of a CFPB examination process could be a report that identifies discrepancies in the CRA's compliance policies and procedures and imposes requirements upon the CRA to address such discrepancies.

Question 6. **Is the regulatory framework for CRA sufficient to protect U.S. consumers from data security and privacy concerns?**

Response: Yes, as explained in the specific response to Question 1, and more generally above, a number of existing laws already provide robust protections for consumer report information maintained by the CRAs.

Question 7. **Could Congress authorize Consumer Financial Protection Bureau to examine CRAs for adherence to the Safeguards Rule?**

Response: Yes, but in the Dodd Frank Act, Congress continued to vest the FTC with the authority to enforce the Safeguards Rule. This seemed appropriate at the time, and continues to seem appropriate given the FTC's developed expertise in the area of data security. In addition to its Safeguards Rule enforcement authority, the FTC retains authority to enforce the FCRA's Disposal Rule, which requires that companies dispose of consumer report information properly in a way that "protect[s] against unauthorized access to or use of the information…."[29]

Question 8. **Could Congress provide the Federal Trade Commission with civil penalties against CRAs for failure to adhere to the Safeguards Rule?**

Response: The FTC's principal tool for the enforcement of the Safeguards Rule is to bring enforcement actions to stop law violations and to require companies to take affirmative steps to remediate unlawful behavior. The FTC may require, when appropriate, implementation of comprehensive privacy and information security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule.

[29] 16 C.F.R. § 682.3(a).

Responses to Additional Questions for the Record

Questions from the Honorable David McKinley

Question 1. **What is the one most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?**

Response: I've not been in a position to investigate the Equifax response to its security incident. So, it is unclear to me whether Equifax could have done more than it did when the security incident was identified. Based on published reports, it appears that Equifax detected the breach, investigated its cause, took steps to stop the breach, notified law enforcement, notified affected consumers who were entitled to direct notice and offered all affected consumers additional tools to protect their identity.[30] From these reports, it appears that Equifax took multiple steps that should enhance Congressional and public confidence that CRAs are able to secure sensitive data. These are also the steps required by existing law, as explained in my detailed responses to questions 1 and 4 above.

Question 2. **What is the one most important thing Congress should do?**

Response: At this time, there is no national standard for when and how companies should notify consumers of data breaches. The FTC has recommended that Congress enact a federal law that would require companies, in appropriate circumstances, to notify consumers when there is a security breach. Although most states have breach notification laws, a consistent national requirement would ensure that all consumers are notified of a security breach when the incident meets a single test, defined by Congress.

Question 3. **I know there are 100s of credit bureaus, but do the three major bureaus maintain an effective monopoly on the supply of credit reports?**

Response: No, the existing nationwide CRAs do not maintain an effective monopoly. The reason there are so few nationwide CRAs is that the financial and technological resources necessary to comply with the myriad of federal and state laws governing the collection, maintenance, and release of consumer report information are so great that only very large corporations can afford them. This is an economic barrier to entry to becoming a nationwide CRA that is a direct result of the highly-regulated CRA marketplace.

[30] *See,* Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/frequently-asked-questions/.

Question 4. **The CFPB has broad authority to bring enforcement case for unfair and deceptive business practices. Are you aware of any CFPB enforcement cases concerning information security using the unfair and deceptive standard?**

Response: As the question notes, the CFPA authorizes the CFPB to seek civil penalties in connection with UDAAP violations for those entities within the CFPB's jurisdiction.[31] The CFPB has used this civil penalty authority in the data security context. In an action against a company for allegedly deceiving consumers about the company's data security procedures and the security of the company's online payment platform, the CFPB required the company to enact comprehensive data security measures (including a data security risk assessment and audit program). In addition, the company was required to train its employees on the company's data security policies and procedures, including on how to protect consumers' sensitive personal information. The company was also required to pay a civil money penalty for its alleged violations.[32]

Question 4a. **Do you understand the Dodd-Frank Act to prevent information security enforcement, even under the broad unfairness and deception standards?**

Response: No, that is not my understanding. The enforcement action referred to in response to Question 4 above is an example of the CFPB using this UDAAP authority in connection in the context of an enforcement action dealing with information security.

[31] 12 U.S.C. §§ 5536(a)(1)(b), 5565(c).

[32] 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/.