



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document:	Letter correspondence to or from the Government Accountability Office (GAO) in the possession of the Federal Trade Commission (FTC) GAO liaison, 2015
Requested date:	13-March-2017
Released date:	13-July-2017
Posted date:	23-July-2018
Source of document:	Freedom of Information Act Request Office of General Counsel Federal Trade Commission 600 Pennsylvania Ave., NW Washington, D.C. 20580 Fax: (202) 326-2477 Email: <a href="mailto:FOIA@FTC.GOV">FOIA@FTC.GOV</a>

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

JUL 13 2017

Re: FOIA-2017-00636  
Government Accountability Office  
Correspondence

This is in response to your March 13, 2017 Freedom of Information Act request, as amended, seeking access to all letter correspondence to or from the Government Accountability Office (GAO) during calendar years, 2015, 2016, and 2017 to date. You also specified that you were seeking records in the possession of our GAO liaison. In accordance with the FOIA and agency policy, we have searched our records as of March 14, 2017, the date we received your request in our FOIA office.

We have located approximately 61 pages of responsive records. I am granting partial access to the accessible records. Portions of these pages fall within one or more of the exemptions to the FOIA's disclosure requirements, as explained below.

Some information is exempt from disclosure under FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E). Exemption 7(E) protects information that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. *See Foster v. DOJ*, 933 F. Supp. 687(E.D. Mich. 1996).

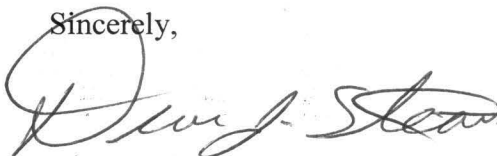
We have determined that 41 pages of responsive records are under the purview of GAO. We have referred this request to the GAO for their review and direct response to you.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

You also may seek dispute resolution services from the FTC FOIA Public Liaison Richard Gold via telephone at 202-326-3355 or via e-mail at [rgold@ftc.gov](mailto:rgold@ftc.gov); or from the Office of Government Information Services via email at [ogis@nara.gov](mailto:ogis@nara.gov), via fax at 202-741-5769, or via mail at Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740.

If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Katie Baker at 202-326-2869.

Sincerely,

A handwritten signature in black ink, appearing to read "Dione J. Stearns". The signature is fluid and cursive, with a large initial "D" and "S".

Dione J. Stearns  
Assistant General Counsel

Enc. 1 CD-20 pages

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

Limited Official Use Only



Office of the Secretary

January 20, 2015

The Honorable Ronald Harold Johnson  
Chairman  
The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security & Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Chairman Johnson and Ranking Member Carper:

Pursuant to 31 U.S.C. § 720, this letter describes actions that the Federal Trade Commission (FTC) has taken and will take in response to the recommendations of the Government Accountability Office ("GAO") in its report entitled *INFORMATION SECURITY: Federal Trade Commission Needs to Address Program Weaknesses* (GAO-15-76SU) (released for Limited Official Use Only on November 20, 2014) ("LOUO Report").

As part of its ongoing policy, enforcement, and education activities to promote consumer privacy and data security, the FTC is keenly aware of its obligations to protect information against unauthorized access, use, disclosure, disruption, modification, or destruction. The FTC has always acknowledged that maintaining sound and reasonable privacy and information security programs requires a continuous process of monitoring, evaluating, updating, and improving. The FTC believes that, in accepting and implementing GAO's recommendations, the FTC will continue to improve its existing information security documentation, processes, and procedures, and thereby continue to reduce potential risks to FTC information systems and data.

#### **GAO Reports**

At the request of then Chairman Thomas R. Carper and Ranking Member Tom Coburn of the Senate Committee on Homeland Security and Governmental Affairs, GAO reviewed the information security and privacy programs of small agencies. GAO selected six agencies to review the extent to which i) small agencies were implementing federal information security and privacy laws and policies, including the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the E-Government Act of 2002, and guidance from the Office of

Management and Budget (OMB) and the National Institute of Standards and Technology (NIST); and ii) the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) were overseeing and assisting implementation of those programs.

On June 25, 2014, GAO released a public report, *INFORMATION SECURITY: Additional Oversight Needed to Improve Programs at Small Agencies* (GAO-14-344) (“Public Summary Report”),<sup>1</sup> which summarized the results of its review of the six agencies without expressly linking specific findings to specific agencies. The FTC’s official agency response is included as an Appendix to the Public Summary Report.

On November 20, 2014, GAO issued a separate Limited Official Use Only Report, *INFORMATION SECURITY: Federal Trade Commission Needs to Address Program Weaknesses* (GAO-15-76SU) (“LOUO Report”),<sup>2</sup> which followed up on the Public Summary Report by providing FTC-specific findings and recommendations. The FTC’s official agency response is included as Appendix III to the LOUO Report.

Because the FTC was in compliance with all of the privacy-related requirements that GAO reviewed, GAO made no recommendations and required no action with regard to the FTC’s privacy program.

For the information security program, FTC staff addressed and resolved all but three of GAO’s findings before the LOUO Report was issued. Those three findings and accompanying action items are listed under the Recommendations for Executive Action, LOUO Report at 20:

- (1) Ensure all employees and contractors with significant network and system security roles have completed specialized, role-based security training.
- (2) Update the plans of action and milestones to include all OMB-recommended elements for the BCP Internet Lab System.
- (3) Fully implement a continuity of operations plan by (1) finalizing and implementing a contingency plan, continuity of operations plan, and disaster recovery plan; (2) updating the business impact analysis; (3) obtaining an alternate location for data processing, storage, and telecommunications; and (4) ensuring FTC emergency monitors receive emergency preparedness training at least annually in accordance with FTC policy.

In addition, GAO identified three technical findings regarding access controls and made related recommendations in Appendix II to the LOUO Report:

(1) (b)(7)(E)

(2)

<sup>1</sup> The Public Summary Report is available online at <http://gao.gov/products/GAO-14-344>.

<sup>2</sup> The LOUO Report was transmitted to the Senate Committee on Homeland Security and Governmental Affairs and the Senate Committee on Commerce, Science, and Transportation.



(3) (b)(7)(E)

As the FTC's official responses to the LOUO Report and the Public Summary Report make clear, the FTC shares GAO's recognition of the importance of sound privacy and data security processes and procedures at government agencies and of the related challenges faced by small federal agencies. As the LOUO Report and the FTC's official response note, the FTC was already working to address GAO's findings, including the three Recommendations for Executive Action, and the FTC had already provided GAO with information that the FTC believed to be sufficient to close the three technical findings. Finally, as noted in the FTC's official responses, none of the potential risks associated with GAO's findings and technical findings indicate an imminent or substantial threat to FTC information systems or data, or suggest that the FTC's information security program is unsound.

### **FTC Response**

The FTC has made significant progress in implementing GAO's three Recommendations for Executive Action. Under GAO procedures, the recommendations will remain open until GAO conducts an annual review of the recommendations, determines that FTC actions have resolved them, and formally closes the recommendations. In order of the recommendations as listed by GAO, staff have

1) (b)(7)(E)

2)

3)

In addition, as stated in the LOUO Report, the FTC has addressed, and believes it has resolved, all three of GAO's technical recommendations and has provided supporting documentation to GAO. Namely, staff have

1) (b)(7)(E)


2)

3)

### **Conclusion**

The Commission appreciates GAO's review of the FTC's information security and privacy programs and the recommendations it offered to the FTC. The FTC takes seriously its responsibility to protect and safeguard its systems and the information they contain. The FTC will continue to implement GAO's Recommendations for Executive Action during FY2015, as discussed above, and will continue to work with GAO to provide the documentation and information necessary to close the remaining recommendations.

By direction of the Commission.

  
Janice Podoll Frankle  
Acting Secretary

cc: Gregory C. Wilshusen, Director  
Dr. Nabajyoti Barkakati, Chief Technologist  
Government Accountability Office  
Information Security Issues

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

Limited Official Use Only



Office of the Secretary

January 20, 2015

The Honorable Jason Chaffetz  
Chairman  
The Honorable Elijah Cummings  
Ranking Member  
Committee on Oversight and Government Reform  
United States House of Representatives  
Washington, D.C. 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

Pursuant to 31 U.S.C. § 720, this letter describes actions that the Federal Trade Commission (FTC) has taken and will take in response to the recommendations of the Government Accountability Office ("GAO") in its report entitled *INFORMATION SECURITY: Federal Trade Commission Needs to Address Program Weaknesses* (GAO-15-76SU) (released for Limited Official Use Only on November 20, 2014) ("LOUO Report").

As part of its ongoing policy, enforcement, and education activities to promote consumer privacy and data security, the FTC is keenly aware of its obligations to protect information against unauthorized access, use, disclosure, disruption, modification, or destruction. The FTC has always acknowledged that maintaining sound and reasonable privacy and information security programs requires a continuous process of monitoring, evaluating, updating, and improving. The FTC believes that, in accepting and implementing GAO's recommendations, the FTC will continue to improve its existing information security documentation, processes, and procedures, and thereby continue to reduce potential risks to FTC information systems and data.

### **GAO Reports**

At the request of then Chairman Thomas R. Carper and Ranking Member Tom Coburn of the Senate Committee on Homeland Security and Governmental Affairs, GAO reviewed the information security and privacy programs of small agencies. GAO selected six agencies to review the extent to which i) small agencies were implementing federal information security and privacy laws and policies, including the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the E-Government Act of 2002, and guidance from the Office of



Management and Budget (OMB) and the National Institute of Standards and Technology (NIST); and ii) the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) were overseeing and assisting implementation of those programs.

On June 25, 2014, GAO released a public report, *INFORMATION SECURITY: Additional Oversight Needed to Improve Programs at Small Agencies* (GAO-14-344) (“Public Summary Report”),<sup>1</sup> which summarized the results of its review of the six agencies without expressly linking specific findings to specific agencies. The FTC’s official agency response is included as an Appendix to the Public Summary Report.

On November 20, 2014, GAO issued a separate Limited Official Use Only Report, *INFORMATION SECURITY: Federal Trade Commission Needs to Address Program Weaknesses* (GAO-15-76SU) (“LOUO Report”),<sup>2</sup> which followed up on the Public Summary Report by providing FTC-specific findings and recommendations. The FTC’s official agency response is included as Appendix III to the LOUO Report.

Because the FTC was in compliance with all of the privacy-related requirements that GAO reviewed, GAO made no recommendations and required no action with regard to the FTC’s privacy program.

For the information security program, FTC staff addressed and resolved all but three of GAO’s findings before the LOUO Report was issued. Those three findings and accompanying action items are listed under the Recommendations for Executive Action, LOUO Report at 20:

- (1) Ensure all employees and contractors with significant network and system security roles have completed specialized, role-based security training.
- (2) Update the plans of action and milestones to include all OMB-recommended elements for the BCP Internet Lab System.
- (3) Fully implement a continuity of operations plan by (1) finalizing and implementing a contingency plan, continuity of operations plan, and disaster recovery plan; (2) updating the business impact analysis; (3) obtaining an alternate location for data processing, storage, and telecommunications; and (4) ensuring FTC emergency monitors receive emergency preparedness training at least annually in accordance with FTC policy.

In addition, GAO identified three technical findings regarding access controls and made related recommendations in Appendix II to the LOUO Report:

(1) (b)(7)(E)

(2)

<sup>1</sup> The Public Summary Report is available online at <http://gao.gov/products/GAO-14-344>.

<sup>2</sup> The LOUO Report was transmitted to the Senate Committee on Homeland Security and Governmental Affairs and the Senate Committee on Commerce, Science, and Transportation.

(3) (b)(7)(E)

As the FTC's official responses to the LOUO Report and the Public Summary Report make clear, the FTC shares GAO's recognition of the importance of sound privacy and data security processes and procedures at government agencies and of the related challenges faced by small federal agencies. As the LOUO Report and the FTC's official response note, the FTC was already working to address GAO's findings, including the three Recommendations for Executive Action, and the FTC had already provided GAO with information that the FTC believed to be sufficient to close the three technical findings. Finally, as noted in the FTC's official responses, none of the potential risks associated with GAO's findings and technical findings indicate an imminent or substantial threat to FTC information systems or data, or suggest that the FTC's information security program is unsound.

### **FTC Response**

The FTC has made significant progress in implementing GAO's three Recommendations for Executive Action. Under GAO procedures, the recommendations will remain open until GAO conducts an annual review of the recommendations, determines that FTC actions have resolved them, and formally closes the recommendations. In order of the recommendations as listed by GAO, staff have

1) (b)(7)(E)

2)

3)

In addition, as stated in the LOUO Report, the FTC has addressed, and believes it has resolved, all three of GAO's technical recommendations and has provided supporting documentation to GAO. Namely, staff have

1) (b)(7)(E)

2)

3)

### **Conclusion**

The Commission appreciates GAO's review of the FTC's information security and privacy programs and the recommendations it offered to the FTC. The FTC takes seriously its responsibility to protect and safeguard its systems and the information they contain. The FTC will continue to implement GAO's Recommendations for Executive Action during FY2015, as discussed above, and will continue to work with GAO to provide the documentation and information necessary to close the remaining recommendations.

By direction of the Commission.

  
Janice Podoll Frankle  
Acting Secretary

cc: Gregory C. Wilshusen, Director  
Dr. Nabajyoti Barkakati, Chief Technologist  
Government Accountability Office  
Information Security Issues



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

Office of the General Counsel

~  
David C. Shonka  
Principal Deputy General Counsel

~  
Direct Dial  
(202) 326-2436

November 13, 2015

David C. Maurer, Director  
Homeland Security and Justice  
U. S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Maurer:

Pursuant to your "Identity Theft Protection Services" engagement (Code 100263), we met with your staff to discuss their information needs. At that time, they requested that we provide them with a copy of the response from our Chairwoman to the letter from the Committee on Energy and Commerce of the U.S. House of Representatives, dated July 9, 2015. Under our agency's Rules of Practice, I am authorized to release this nonpublic information to you without restrictions. A copy of the Chairwoman's letter is attached.

Sincerely,

A handwritten signature in blue ink, appearing to read "David C. Shonka", is positioned above the printed name.

David C. Shonka  
Principal Deputy General Counsel

Attachment





OFFICE OF THE  
CHAIRMAN

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON D.C. 20580

August 14, 2015

The Honorable Fred Upton  
Chairman  
Committee on Energy and Commerce  
United States House of Representatives  
2125 Rayburn House Office Building  
Washington, D.C. 20515-6115

Dear Chairman Upton:

Thank you for your letter seeking information regarding credit freezes. Protecting consumers against identity theft and its consequences is a critical component of the Commission's consumer protection mission, which we pursue through our law enforcement, consumer and business education, and policy work. I appreciate your commitment to supporting identity theft victims and hope the information enclosed will assist the Committee in its important work on the issue.

Before addressing your specific concerns, it would be helpful to provide some background on the Commission's jurisdiction and work in addressing identity theft. The Commission has been directed by Congress to act in the interest of all consumers to prevent deceptive or unfair acts or practices, pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58. Congress has also enacted other statutes that specifically empower the Commission to address credit and identity theft, including the Fair Credit Reporting Act (FCRA) and the Identity Theft Assumption and Deterrence Act (ITADA).

The FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies (CRAs).<sup>1</sup> The FCRA protects information collected by various CRAs, such as credit bureaus and tenant screening services, by limiting who may access the reports and outlining specific legal obligations for CRAs and the companies that furnish information to CRAs. The FCRA also gives consumers valuable tools to help prevent or detect identity theft, including fraud alerts, extended fraud alerts, and free copies of credit reports. To ensure compliance with the FCRA, the Commission pursues an aggressive enforcement program aimed at the main players in the credit reporting system: CRAs; those who furnish information to CRAs; and consumer report users. The Commission shares enforcement authority for this statute

---

<sup>1</sup> The Commission enforces the FCRA, as amended by that Fair and Accurate Credit Transactions Act of 2003 (FACTA).

with the Consumer Financial Protection Bureau (CFPB), but the CFPB alone has rulemaking authority and regulatory authority in this area.

Under the ITADA, the Commission is the central clearinghouse for identity theft complaints. The Commission logs identity theft complaints, provides victims with relevant information, and refers their complaints to appropriate entities, such as national CRAs and other law enforcement agencies. The Commission established the Consumer Sentinel Network as the clearinghouse for consumer complaints, including identity theft complaints, and provides an annual report analyzing the complaints. Further, the Commission creates and distributes numerous publications and conducts outreach to consumers on a host of issues, including identity theft.

In addition, consumer and business education is an important part of the Commission's mission. As part of the Commission's efforts to inform consumers about identity theft and steps they may take to mitigate harms, the Commission creates educational resources that are available both online and in print, as further outlined below. IdentityTheft.gov is a website created by the Commission, and it has served as a centralized source of information for potential identity theft victims for years. The site, and many educational pieces, discuss tools available to consumers to combat identity theft, and one such tool is the credit freeze. Also known as a security freeze, a credit freeze can limit harm resulting from identity theft by restricting access to a credit report, which makes it more difficult for identity thieves to open new accounts in a consumer's name.

It is important to note that the credit freeze is a tool made available to consumers through state law.<sup>2</sup> The first credit freeze law was enacted in 2003, and as more and more states enacted such legislation, the three large nationwide CRAs voluntarily implemented processes that, for a fee, enabled consumers in states without freeze laws to place freezes. State laws generally enable CRAs to charge a fee for placing and lifting a credit freeze—which typically must be placed, and lifted, for each of the three large nationwide CRAs—but many state laws allow identity theft victims to place a credit freeze for free.

Please find below more detailed responses to your specific inquiries about credit freezes.

- 1) Do you have evidence that consumers are currently aware of the option to freeze their credit to prevent their information from being used by cyber criminals to establish new lines of credit? Has your agency received any feedback from consumers about the current security freeze laws? If so, what is that feedback?**

Given its mission and the serious and widespread harm caused by identity theft, the Commission has devoted significant resources to studying the issues around identity theft, educating consumers about identity theft prevention and resolution, and tracking related

---

<sup>2</sup> All fifty states and the District of Columbia have enacted statutes that allow for credit freezes. The exact provisions and allowance for fees under each law vary greatly by state. See Consumer Report Security Freeze State Laws, National Conference of State Legislatures, available at <http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx> (last visited July 16, 2015).



complaints through the Commission's Consumer Sentinel Network, as mentioned above. These activities are summarized below.

### Identity Theft Taskforce – Study and Comments

As you may be aware, a decade ago, the Commission, along with the Department of Justice, convened the President's Identity Theft Task Force.<sup>3</sup> Among other things, the task force charged the Commission with coordinating a plan to prevent identity theft and help victims recover. As part of that effort, in 2012, the Commission performed a survey to assess consumer awareness of certain rights established under the FCRA.<sup>4</sup> While the survey did not specifically inquire about security freezes, as the right to a freeze emanates from state law and not the FCRA, the survey results suggest that a relatively small percentage of identity theft victims are aware of their rights under the FCRA that relate to their credit reports, including blocking and fraud alerts (discussed below).

The Commission also sought public comments on the impact and effectiveness of credit report freezes in 2008, as part of its efforts to understand the effectiveness of tools in this area.<sup>5</sup> Several commenters contended that credit freezes are effective in preventing some identity theft harms by preventing the release of a credit report and the issuance of new lines of credit, but recognized that credit freezes are not a silver bullet to preventing all types of fraud.<sup>6</sup> In particular, credit freezes do not address employment-related identity theft, medical identity theft, and identity theft relating to existing accounts. Additionally, some commenters expressed support for a centralized source for consumers to implement credit freezes, akin to how AnnualCreditReport.com provides consumer access to annual free credit reports for each of the three largest CRAs.<sup>7</sup> Since 2008, consumer advocates generally have continued to encourage consumers' use of credit freezes as a tool to prevent new account fraud.<sup>8</sup>

### Consumer Education

One measure of consumer awareness of credit freezes is the number of consumers who have accessed the Commission's published educational information on credit freezes. These

<sup>3</sup> See The President's Identity Theft Task Force Report, (Sept. 2008), *available at* <https://www.ftc.gov/reports/presidents-identity-theft-task-force-report>.

<sup>4</sup> Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims, Commission Staff, (March 2012), *available at* <https://www.ftc.gov/reports/using-facta-remedies-ftc-staff-report-survey-identity-theft-victims>.

<sup>5</sup> The Commission received approximately fifty comments in response to its request. See Comments on Project P075420: Impact and Effectiveness of Credit Report Freezes, *available at* <https://www.ftc.gov/policy/public-comments/initiative-227>.

<sup>6</sup> See e.g. Comment of Wells Fargo & Co., at 2; Comment of American Financial Services Association, at 1; Comment of AARP, at 1; and Comment of Navy Federal Credit Union, at 2, *available at* <https://www.ftc.gov/policy/public-comments/initiative-227>.

<sup>7</sup> See e.g. Comment of New York Public Interest Group, at 4, Comment of Navy Federal Credit Union, at 2; and Consumers Union, at 10, *available at* <https://www.ftc.gov/policy/public-comments/initiative-227>.

<sup>8</sup> See e.g. "How I Learned to Stop Worrying and Embrace the Security Freeze," Krebs on Security, *available at* <http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/>; Consumers at Risk: Tips When Experiencing a Data Security Breach, National Consumer Law Center, Dec. 19, 2013, *available at* [www.nclc.org/images/pdf/pr-reports/pr-creditcardbreach2013.pdf](http://www.nclc.org/images/pdf/pr-reports/pr-creditcardbreach2013.pdf).

materials are available on [IdentityTheft.gov](http://IdentityTheft.gov) and on the FTC's consumer education website, at <http://www.consumer.ftc.gov>. In particular, in the past six months, we have seen a sustained and significant rise in interest regarding our credit freeze materials. For example, *Credit Freeze FAQs*, which is available on our website, rarely received more than 300 page visits per day prior to February 2015.<sup>9</sup> Since late February 2015, the page has received between 1,000 and 3,000 page visits per day. The Commission has also published *Extended Fraud Alerts and Credit Freezes*<sup>10</sup> and *Taking Charge*, a comprehensive guide for consumers on identity theft that discusses a number of steps consumers can take to protect themselves (including credit freezes).<sup>11</sup> In addition to the publications noted above that specifically address credit freezes, the Commission has published many other consumer and business education brochures and other materials that relate to identity theft. These materials are available online at <https://www.ftc.gov>. Many of these consumer education publications and websites are available in Spanish as well. Commission staff also routinely engage in outreach to law enforcement, consumer groups, and others on the issue of identity theft. As part of these efforts, staff routinely highlight the availability of credit freezes.

### IdentityTheft.gov

In addition, the Commission recently embarked on an effort to expand our online identity theft resources for consumers. An executive order, *Improving the Security of Consumer Financial Transactions*, requested that the Commission streamline and consolidate resources at our website [IdentityTheft.gov](http://IdentityTheft.gov) and enhance the functionality of the site by coordinating with CRAs to simplify the reporting and remediation process.<sup>12</sup> In May, we announced the new upgrades to the [IdentityTheft.gov](http://IdentityTheft.gov) website—also available in Spanish at [RobodeIdentidad.gov](http://RobodeIdentidad.gov). The revised site walks people through the recovery process and helps them understand which recovery steps should be taken upon learning their identity has been stolen, including the option to place a credit freeze. It also provides sample letters and other helpful resources. In addition, the site offers specialized tips for specific forms of identity theft, including tax-related and medical identity theft, and provides advice for people who have been notified that their personal information was exposed in a data breach. Accordingly, the website stands as a centralized source of information on identity theft. Currently, the Commission is working to expand the site further to provide tailored advice, resources, and specific model letters to address individual consumers' needs.

<sup>9</sup> Credit Freeze FAQs, available at <http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#difference>.

<sup>10</sup> Extended Fraud Alerts and Credit Freezes, available at <http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes#order>.

<sup>11</sup> Taking Charge, available at <https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf>. This publication alone has been distributed on paper to, or viewed online by, approximately 1 million consumers so far in Fiscal Year 2015.

<sup>12</sup> Exec. Order No. 13681, 79 Fed. Reg. 63,491 (Oct. 23, 2014), available at <http://www.archives.gov/federal-register/executive-orders/2014.html>.



## Consumer Sentinel

As noted above, the Commission operates the Consumer Sentinel Network to track consumer identity theft and fraud complaints.<sup>13</sup> Over 50 entities refer complaints to Consumer Sentinel, including states' attorneys general, the CFPB, the Privacy Rights Clearinghouse, and the Internet Crime Complaint Center.<sup>14</sup> Over 2,000 federal, state, and local law enforcement agencies have access to these complaints.

Through Consumer Sentinel complaints,<sup>15</sup> studies, and interactions with consumers and advocates, we know that while many consumers successfully obtain credit freezes through the CRAs' websites,<sup>16</sup> other consumers are not able to do so. Specifically, some consumers cannot successfully authenticate their identity online, precluding them from using the CRAs' websites to access their credit reports or potentially implement freezes. Additionally, CRAs often block access to their websites from foreign internet service providers for security reasons, and so consumers overseas may not be able to access CRAs' websites to get their credit report or implement a freeze.<sup>17</sup> Furthermore, certain of these consumers living abroad may have difficulty implementing a credit freeze for various reasons, and if they do not have state residency, they cannot avail themselves of the right to a credit freeze provided by state law.

Many of the consumers who report their experiences with identity theft to Consumer Sentinel utilize credit freezes to prevent new account fraud. Some note that a more centralized process for implementing credit freezes would benefit consumers by limiting their burden. In addition, consumers complain about the cost of implementing and lifting credit freezes, particularly those who experience identity theft and believe the fees should be waived. Some consumers also register complaints about difficulties or delays they experience lifting credit freezes.

While support for credit freezes as a tool for preventing new account fraud continues, there are limits to its effectiveness. Credit freezes do not prevent existing account fraud, as discussed above, and do not stop financial transactions that occur outside of the credit reporting system, i.e., where the creditor does not first pull the consumer's credit report. The Commission continually reviews feedback consumers provide about their experiences to update its educational and outreach efforts.

---

<sup>13</sup> Consumer Sentinel includes complaints about debt collection, credit reports and financial matters, identity theft, Do-Not-Call Registry violations, online auctions, immigration services scams, business opportunities, and work-at-home schemes, among other issues.

<sup>14</sup> Data Contributors, Consumer Sentinel Network, <https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors>.

<sup>15</sup> Given the nature of the identity theft complaints we receive, and the fact that credit freezes are created by state law, the Commission does not receive extensive feedback on consumers' experiences implementing credit freezes through the complaints themselves.

<sup>16</sup> See Experian, available at <https://www.experian.com/freeze/center.html>; TransUnion, available at <https://www.transunion.com/securityfreeze>; and Equifax, available at [https://www.freeze.equifax.com/Freeze/jsp/SFF\\_PersonalIDInfo.jsp](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp).

<sup>17</sup> Credit Report Access Denied, Kiplinger (June 25, 2007), <http://www.kiplinger.com/article/credit/T017-C001-S001-credit-report-access-denied.html>.

- 2) What, if any, are the regulatory or legislative mechanisms available to reduce the cost of security freezes for consumers? What initiatives are available to relieve the consumer from the cost of setting up and lifting a freeze?

The availability and cost of a credit freeze depends on both state law and the CRA's policies. The cost to the consumer to implement or lift a freeze typically ranges from \$5 to \$10, as set out in state law.<sup>18</sup> The CRA may also assess a fee if a consumer lost his or her PIN, which the CRA provides to the consumer when implementing a freeze and is required to lift the freeze.<sup>19</sup> In many states, a freeze may be provided free of charge to a victim of identity theft, when the victim provides a police report to document the crime.<sup>20</sup> Some states permit guardians to place a special freeze for incapacitated consumers, as well as minor children, which may be free if a file is already in existence with a CRA.<sup>21</sup> In addition, senior consumers may be able to place or lift a credit freeze for free, depending on the state's law.<sup>22</sup>

- 3) Has the Federal Trade Commission explored federal standards for security freezes? What are the existing obstacles to expanding the use of security freezes? How can those obstacles be overcome?

The Commission solicited public comment on a wide range of issues relating to the impact and effectiveness of credit freezes in 2008. At that time, commenters generally did not express support for a federal security freeze standard because the majority of states already had such laws and the CRAs had voluntarily put in place a process for all consumers to implement a freeze. Some, including consumer group commenters, were concerned about preemption of the existing state laws, while the industry association commented that a federal law was not necessary.<sup>23</sup>

One obstacle to expanding the use of security freezes is the fees associated with placing and lifting the freezes. Many consumers can place the freeze for free – principally, by demonstrating that they are victims of identity theft – but this process requires some time and inconvenience. If consumers were able to place and lift freezes at no cost, this would remove potential obstacles: consumers may not want to pay costs associated with placing the freeze, and even if they are willing to pay the initial placement cost, they may believe that they are likely in the foreseeable future to encounter a circumstance that will require them to pay another fee to lift the freeze – which would put them back where they were in the first place. Of course, as industry highlighted, the CRAs incur some costs in placing and lifting the freezes, although the trade association did not enumerate the costs in its 2008 comment.<sup>24</sup>

<sup>18</sup> See Consumers Union Guide to Security Freeze Protection, Consumers Union, *available at* <http://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection/> (last accessed July 17, 2015).

<sup>19</sup> See, e.g., Ariz. Rev. Stat. Ann. §44-1698.

<sup>20</sup> See, e.g., Ga. Code §10-1-913 *et seq.*

<sup>21</sup> See, e.g., S.C. Code Ann. § 37-20-110.

<sup>22</sup> See, e.g., Okla. Stat. Ann. 24, § 156; 73 Pa.

<sup>23</sup> See e.g. Comment of CDIA, at 11; Comment of Consumers Union et al., at 11-12; Comment of USPIRG at 4-5, *available at* <https://www.ftc.gov/policy/public-comments/initiative-227>.

<sup>24</sup> Comment of CDIA, at 7, *available at* <https://www.ftc.gov/policy/public-comments/initiative-227>.

- 4) How can the security freeze process be streamlined, including for parents seeking to freeze the credit of their minor children? How can we make it easier for consumers to place a security freeze at each of the credit bureaus? Could a model like AnnualCreditReport.com be used for this purpose? Are there costs or possible unintended consequences associated with increasing consumer access to security freezes?

A potential model for streamlining the process for credit freezes is the process currently in place for consumers to implement fraud alerts. As provided by the FCRA, to implement a fraud alert with all three national CRAs, a consumer need only contact one of the CRAs, and that CRA in turn must refer the information regarding the fraud alert to each of the other two CRAs.<sup>25</sup> This process relieves the consumer of the burden of reaching out to three separate CRAs.<sup>26</sup> Another potential model for streamlining would be AnnualCreditReport.com, a centralized website for the three nationwide CRAs. Consumers seeking a copy of their credit report can go to this centralized website, which directs them to websites for each of the three CRAs, where they may order one free copy of their report from each of the nationwide CRAs each year. This approach could serve as a model for centralizing information and directing consumers to the appropriate CRA websites to place and lift credit freezes.<sup>27</sup>

With respect to freezes for minors, eighteen states have enacted legislation requiring that CRAs provide a mechanism for parents to request the creation of a non-credit record, link it to their child, and then freeze the record.<sup>28</sup> These statutes generally provide for this process to also protect individuals who are incapacitated or for whom a guardian has been appointed under state law. The processes vary by state, but generally require: (1) the request be submitted in the manner specified by the CRA; (2) the representative provide sufficient proof of identity for the protected consumer and the representative; (3) the representative provide sufficient proof of authority to act on behalf of the protected consumer; and (4) the payment of any applicable fee. The procedural requirements to lift this type of freeze are substantially the same as what is required to implement the freeze. Under the state laws, CRAs generally may charge fees for putting this type of freeze in place (typically \$5 or \$10), but, again, generally provide a fee exemption for those who are victims of identity theft.

One possible downside to placing a credit freeze is the inconvenience to consumers who may need access to credit going forward. Often there is a cost to the consumer to lift a credit freeze, and the lead-time necessary to lift a freeze varies. Consumers seeking a mortgage, loan,

<sup>25</sup> Fair Credit Reporting Act § 605A; 15 U.S.C.SS 1681c-1.

<sup>26</sup> Note, however, that because fees are usually charged with placing the freeze, there would have to be a process at the site either to collect the fee for each CRA, or a process to collect one lump sum from the consumer and distribute the fee to each CRA.

<sup>27</sup> For consumers with a credit report—as opposed to consumers who are “credit invisible”—the process of placing a freeze online is not particularly difficult, but not everyone is familiar with the national CRAs. A centralized source could help these consumers.

<sup>28</sup> The states are: Maryland, Delaware, Michigan, Oregon, Texas, Wisconsin, Florida, Georgia, Indiana, Iowa, Louisiana, New York, South Carolina, Virginia, Tennessee, Connecticut (going into effect October 1, 2015), Maine (going into effect October 1, 2015), and Arizona (going into effect December 31, 2015). See Table 1, attached.



credit card, or other forms of credit will need to lift the freeze either temporarily or permanently, as will those consumers who are applying for jobs, renting apartments, or buying insurance. Further, the consumer will have a different PIN or password for each freeze and will need to store that information and have it readily available to lift the freeze. If the consumer does not have the PIN or password when he or she wants to lift the freeze, there may be delays beyond the three days the CRA generally has to lift the freeze. Consumers could also be negatively affected if the possible delay in lifting the freeze is a longer period than potential creditors, employers, landlords, or salespeople can tolerate. Federal legislation or new state laws could minimize this potential downside—for example, by prohibiting CRAs from charging fees for lifting and replacing freezes, or by requiring CRAs to lift credit freezes more quickly at the consumer's request.

Another unintended consequence that could result from increasing consumer access to credit freezes is that it could dissuade consumers from monitoring bank, credit card, and insurance statements for existing account fraud as carefully as they otherwise would. However, we do not have evidence to suggest that this is currently happening.

- 5) How can federal regulatory or legislative efforts regarding security freezes account for consumers who do not have a credit report? How can consumers who are “credit invisible” initiate a security freeze? What other options might these credit invisible consumers have to protect themselves following a breach?**

Fraud alerts and credit freezes are predicated on the idea that creditors generally will not extend credit to consumers without first assessing the creditworthiness of the consumer. Accordingly, the tools to prevent new account frauds help only those consumers that have credit reports. A consumer without a credit report, also known as “credit invisible,” cannot initiate a credit freeze, as there is no record to freeze. A consumer who lacks a record to freeze is vulnerable to a thief creating a credit report under the consumer's identity. If this occurs, the consumer is no longer credit invisible. The consumer may clean up the information wrongly associated as being his or her credit report through working with the CRAs, and then he or she may be able to freeze the record to prevent further harm. According to a May 2015 study by the CFPB, over 26 million Americans are credit invisible.<sup>29</sup> While children and other classes of vulnerable adults have a tool similar to a credit freeze available to them in a growing number of states, as discussed above, consumers who do not live in these states or do not qualify under the statutory definition do not have a right to the tool. Federal legislation could provide for a tool modeled after the state child credit freeze laws for consumers who do not have credit reports.

- 6) Beyond the credit freeze, are there other protections that are available or can be made available to consumers following a breach of their personal information? For example, is credit monitoring considered a best practice in this area, and what is an appropriate length of time for breached entities to provide credit monitoring following a breach?**

---

<sup>29</sup> Data Point: Credit Invisibles, CFPB Office of Research, May 2015, *available at* [http://files.consumerfinance.gov/f/201505\\_cfpb\\_data-point-credit-invisibles.pdf](http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf).



Beyond credit freezes, there are several other tools available to consumers to help them mitigate potential harms that can arise following a breach of their personal information. The FTC's new identity theft education resource—IdentityTheft.gov—walks consumers through the process of how to resolve identity theft problems and will continue to expand to include new information and resources in the coming months.

Among the tools discussed at IdentityTheft.gov are free credit reports. Consumers can access a free credit report from each of the CRAs every twelve months through AnnualCreditReport.com, and may review the reports to monitor their credit. Commission staff often recommend that consumers consider accessing their credit report from a different CRA at four-month intervals, in order to monitor their report and react to potential new account fraud in a more timely manner.

Under the FCRA, various fraud alerts are available to consumers and they can help mitigate identity theft harm. A fraud alert is a tool intended for those consumers who believe they are identity theft victims. This alert is free to place or remove. Under the FCRA, a consumer who asserts a suspicion that he or she has been, or is about to become, a victim of fraud, including identity theft, may request a CRA include a fraud alert in the file of that consumer for 90 days, and instruct the other CRAs to implement a fraud alert as well.<sup>30</sup> A fraud alert allows creditors to get a copy of a consumer's credit report only when the CRA has taken steps to verify the consumer's identity. For example, if the consumer provides a telephone number when implementing the initial fraud alert, the CRA must call the consumer to verify whether the consumer is the person making the credit request. Fraud alerts may be effective at stopping someone from opening new accounts in a consumer's name, but they do not prevent the misuse of the consumer's existing accounts. The initial fraud alert stays on a consumer's report for 90 days and allows the consumer to order one free copy of his or her credit report from each of the three CRAs. The consumer may renew it after 90 days. The consumer must be sure the CRAs have the correct contact information for the consumer because if the CRAs cannot verify the consumer is seeking credit, they will not release the credit report, which could frustrate those consumers wanting to access new lines of credit.

Another free tool available to consumers under the FCRA, and explained at IdentityTheft.gov, is the extended fraud alert.<sup>31</sup> If a consumer has created an Identity Theft Report,<sup>32</sup> he or she can then place an extended alert on his or her credit report, which will last for seven years. In doing so, the consumer may get two free credit reports within twelve months from each of the three nationwide CRAs, and the CRAs must take the consumer's name off marketing lists for prescreened credit offers for 5 years, unless the consumer asks them to put his or her name back on the list.

The active duty alert is a tool under the FCRA that is designed for military personnel deployed overseas. An active duty alert on a person's credit report means businesses have to

---

<sup>30</sup> Fair Credit Reporting Act § 605A(a); 15 U.S.C. § 1681c-1(a).

<sup>31</sup> Fair Credit Reporting Act § 605A(b); 15 U.S.C. § 1681c-1(b).

<sup>32</sup> An Identity Theft Report is an identity theft affidavit combined with a police report.

take extra steps before granting credit in that person's name.<sup>33</sup> Active duty alerts last for one year, and can be renewed to match the period of deployment. If a consumer is in the military and on deployed status, he or she need contact only one CRA, and that CRA then has a duty to contact the remaining two CRAs to implement the active duty alert.

Another tool available to consumers can help to repair a credit report that reflects account fraud stemming from identity theft. The FCRA enables a consumer to request that a CRA block any information in his or her file that the consumer identifies as information resulting from identity theft.<sup>34</sup> To have information blocked, a consumer must submit a copy of his or her Identity Theft Report to the CRA, indicate which information on the report resulted from identity theft, and explain that the information did not come from a consumer-authorized transaction. If the CRA accepts the consumer's Identity Theft Report, it must block the fraudulent information from the consumer's credit report.

In addition to the protections and remedies available under the FCRA, consumers can often take advantage of various commercial services including credit monitoring, identity monitoring, and identity theft restoration. Credit monitoring services typically do not prevent identity theft, but alert consumers about suspicious activities, such as the opening of a new account. If it was not an authorized transaction, consumers can take action quickly to prevent further harm, such as by closing an unauthorized new account or contesting or blocking erroneous charges. While credit monitoring enables a consumer to mitigate the harm caused by an identity thief, a credit freeze may help prevent the occurrence of the new account fraud altogether.

Identity monitoring is another tool available in the marketplace. Identity monitoring is broader than credit monitoring because it tracks the misuse of a consumer's personal information beyond credit reports. For example, identity monitors comb commercial databases for misuse of personal information, such as payday loan databases, bank and check databases, criminal records, and sex offender registries. Identity monitors typically will monitor the use of consumers' Social Security numbers, even combing the internet for evidence of trading or misuse of personal information.

There is some debate amongst consumers and advocates about the value credit monitoring services may provide consumers. Critics of credit monitoring note that it only provides an after-the-fact alert of an identity theft problem and believe credit-monitoring products are expensive compared to credit freezes. Others argue, however, that credit monitoring, when combined with identity monitoring, can be an effective tool for preventing further harms stemming from identity theft by providing a timely alert to the consumer, and that millions of consumers have purchased credit-monitoring products. It is important to note that many consumers have home or equivalent insurance that contains identity protection for themselves and their families.<sup>35</sup>

---

<sup>33</sup> Fair Credit Reporting Act § 605A(c); 15 U.S.C. § 1681c-1(c).

<sup>34</sup> Fair Credit Reporting Act § 605B; 15 U.S.C. § 1681c-2.

<sup>35</sup> See Buying Homeowners Insurance, *available at*

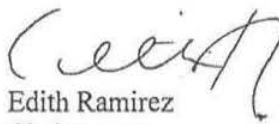
<http://www.checkbook.org/interactive/homeownersinsurance/wdc/article.cfm> (last accessed July 27, 2015);

As you highlight in your letter, the length of time that entities provide credit monitoring after a breach has also been an important area of interest. I note that most companies offer one to two years of credit monitoring, with some exceptions. On balance, I believe a two-year time period is appropriate, though I think this is an evolving area that we should continue to watch closely.

Finally, there are commercial providers that offer identity theft restoration services should identity theft occur. Once personal information is compromised, it is often difficult to determine when it may be misused, how it may be misused, and by whom. Accordingly, restoration services focus on helping the consumer, regardless of the type or source of the identity theft. They typically offer counselling services, communicate with creditors or others on behalf of the consumer, and take other remedial steps to resolve the consumer's problem.

We appreciate your interest in this matter, and hope that the Committee finds the above information helpful. FTC staff will be meeting with your staff to further discuss these issues. As always, please do not hesitate to contact Jeanne Bumpus, our Director of Congressional Relations, at 202-326-2946.

Sincerely,

A handwritten signature in black ink, appearing to read 'Edith Ramirez', with a stylized flourish at the end.

Edith Ramirez  
Chairwoman