



THE CHAIRMAN

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 30, 2010

The Honorable Mary L. Landrieu
Chairwoman
Committee on Small Business & Entrepreneurship
United States Senate
428A Russell Senate Office Building
Washington, DC 20510

Dear Chairwoman Landrieu:

This third annual report is made in accordance with Section 212(a)(6) of the amended Small Business Regulatory Enforcement Fairness Act ("SBREFA").

Since we submitted our second annual SBREFA report on June 4, 2009, the Federal Trade Commission ("Commission" or "FTC") has issued one rule subject to Section 212 of SBREFA:¹

Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act ("GLB Act"), 16 C.F.R. Part 313: On November 17, 2009, after prior notice and comment, the Commission and seven other agencies announced a model privacy form that financial institutions may rely on as a safe harbor to provide disclosures under the privacy rules.² 74 Fed. Reg. 62,890 (Dec. 1, 2009) at 62,965-74 (amendments to Commission rules at 16 C.F.R. Part 313). With the exception of certain amendments effective January 1, 2012, the rules became effective on December 31, 2009. *Id.* at 62,965. The Commission prepared "Final Model Privacy Form Under the Gramm-Leach-Bliley Act A Small Entity Compliance Guide," which is posted at www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_SmallBusinessGuide.pdf.

In the past year, the Commission has also certified to the Small Business Administration that certain other final regulations issued will not have a significant economic impact on a substantial number of small business entities. Nonetheless, the Commission published a Final Regulatory Flexibility Act ("FRFA") analysis along with

¹ Section 212 requires agencies to publish a "small entity compliance guide" for any new rule for which an agency is required to prepare a final regulatory flexibility analysis under section 3(a) of the Regulatory Flexibility Act, which is codified at 5 U.S.C. § 604.

² Pursuant to Section 728 of the Financial Services Relief Act of 2006, P. L. No. 109-351, which added section 503(e) to the Gramm-Leach-Bliley Act ("GLB"), the Commission together with seven other federal agencies were directed to propose a model form that may be used at the option of financial institutions for the privacy notices required under GLB.

these final regulations. We have either made available or are preparing updated compliance materials for each of these rulemakings although not required to do so by SBREFA. A few examples include:

- **Health Breach Notification Requirement for Vendors of Personal Health Records, codified at 16 C.F.R. Part 318:** Section 13407 of the American Recovery and Reinvestment Act of 2009 required that the Commission issue temporary breach notification requirements for vendors of personal health records and third parties that offer products or services through the web sites of vendors of personal health records. The notification requirements are triggered when there is a breach of security with respect to individually identifiable health information. After notice and comment, the Commission issued an interim final rule on August 17, 2009. The Commission has posted "Complying with the FTC's Health Breach Notification Rule" at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus56.pdf>.
- **Prohibitions on Market Manipulation and False Information in Subtitle B of the Energy Independence and Security Act of 2007, codified in 16 C.F.R. Part 317:** Section 811 of the Act prohibits any manipulative or deceptive device or contrivance in connection with the wholesale purchase or sale of crude oil, gasoline or other petroleum distillate in contravention of such rules or regulations as the Commission may prescribe. Section 813 specified the methods of enforcing such a rule. After notice and comment, the Commission announced a final rule on August 6, 2009, that prohibits fraud or deceit in wholesale petroleum markets, and omissions of material information that are likely to distort petroleum markets. The rule was effective on November 4, 2009. The Commission has posted "Guide to Complying with Petroleum Market Manipulation Regulations" at <http://www.ftc.gov/os/2009/11/091113mmrguide.pdf>.

Red Flags Rule

The Identity Theft Red Flags Rule ("Red Flags Rule" or "Rule"), 16 C.F.R. Part 681, was promulgated by the Commission and four other agencies (which have their own comparable CFR sections for entities they regulate), as directed by the Fair and Accurate Credit Transactions Act of 2003. The Rule requires "creditors" and "financial institutions" that have certain "covered accounts" to develop and implement written identity theft prevention programs. These programs must be designed to help identify, detect, and respond to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

We are concerned that the legislation requiring the Red Flags Rule is overbroad and has had unintended consequences; numerous small businesses that regularly permit deferred payments for goods or services are "creditors" that are covered by the Rule. The Commission has no discretion to grant exemptions. The Commission recently further delayed enforcement of the Rule through December 31, 2010, while Congress considers

legislation that would exempt certain low-risk small businesses from the Rule's mandate. The Commission fully supports the effort to limit application of the Red Flags Rule and urges Congress to act quickly to narrow the scope of the Rule. In the interim, we have continued to address the concerns of small businesses.

In the November 2007 final rule announcement, the Commission certified that the Red Flags Rule would affect a substantial number of small business entities but would not have a significant economic impact on those small entities. Thus, the Commission was not obligated to perform a FRFA analysis. Nevertheless, the Commission decided to publish a FRFA analysis in this case. The FRFA analysis carefully addressed concerns of commenters who requested that the implementation date be delayed, that the Commission develop a small business compliance guide, and that we create a certification form for low-risk entities. Indeed, the Commission has been responsive to all these requests.

We have provided several extensions of the enforcement date for the Red Flags Rule and have engaged in extensive outreach and guidance to assist and ease compliance burdens for entities covered by the Red Flags Rule – especially small businesses. The Commission developed a Red Flags Web site (www.ftc.gov/redflagsrule) with articles and other materials, including a detailed business compliance guide that explains what types of entities are covered and provides step-by-step compliance advice, "Fighting Fraud with the Red Flags Rule: A How-To Guide for Business," available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>. And, for entities that have a low risk of identity theft (such as businesses that know their customers personally), the FTC issued an easy-to-use template to help them in developing written identity theft prevention programs to comply with the Red Flags Rule ("Create Your Own Identity Theft Prevention Program: A Guided 4-Step Process," available at www.ftc.gov/bcp/edu/microsites/redflagsrule/diy-template.shtml). As a result, the Commission believes that it has complied fully with its Regulatory Flexibility Act obligations.

* * * * *

For many years, the FTC has had a highly effective program providing compliance assistance to small businesses.³ We plan to continue to refine and improve these efforts.

³ The Commission complements its compliance assistance efforts with consideration of the particular circumstances of a case when enforcing business obligations. As you know, Section 223 of SBREFA (1996) required that agencies establish policies to reduce or waive penalties for small entities in appropriate circumstances. In 1997, the Commission issued a small business leniency policy statement that describes factors that may result in reduction or waiver of penalties. See 62 Fed. Reg. 16,809 (Apr. 8, 1997) (issuing policy); 62 Fed. Reg. 46,363 (Sept. 2, 1997) (responding to comment received). As such cases arise, the Commission considers these leniency factors whenever a civil penalty may be assessed against a small business.

In addition, and beyond SBREFA requirements, the Commission established corporate leniency policies for violations of the Textile and Wool Rules, 67 Fed. Reg. 71,566 (Dec. 2, 2002), the Funeral Rule

The Honorable Mary L. Landrieu
Page 4

If you have any questions, please contact Christian S. White, the Deputy General Counsel for Legal Counsel and Small Business Coordinator at the Commission, at (202) 326-2476.

Respectfully,

/signed/
Jon Leibowitz
Chairman

cc: The Honorable Nydia M. Velázquez
Chairwoman
Committee on Small Business
U.S. House of Representatives

(through the Funeral Rule Offender Program), and the Franchise Rule (through the Franchise Rule Alternative Law Enforcement Program) that have helped in fostering a more cooperative, less threatening regulatory environment for small entities. These policies have helped increase overall compliance with the rules while minimizing the burden on business of correcting certain minor or inadvertent errors that are not likely to injure consumers.



THE CHAIRMAN

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 30, 2010

The Honorable Nydia M. Velázquez
Chairwoman
Committee on Small Business
U.S. House of Representatives
2361 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Velázquez:

This third annual report is made in accordance with Section 212(a)(6) of the amended Small Business Regulatory Enforcement Fairness Act ("SBREFA").

Since we submitted our second annual SBREFA report on June 4, 2009, the Federal Trade Commission ("Commission" or "FTC") has issued one rule subject to Section 212 of SBREFA:¹

Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act ("GLB Act"), 16 C.F.R. Part 313: On November 17, 2009, after prior notice and comment, the Commission and seven other agencies announced a model privacy form that financial institutions may rely on as a safe harbor to provide disclosures under the privacy rules.² 74 Fed. Reg. 62,890 (Dec. 1, 2009) at 62,965-74 (amendments to Commission rules at 16 C.F.R. Part 313). With the exception of certain amendments effective January 1, 2012, the rules became effective on December 31, 2009. *Id.* at 62,965. The Commission prepared "Final Model Privacy Form Under the Gramm-Leach-Bliley Act A Small Entity Compliance Guide," which is posted at www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_SmallBusinessGuide.pdf.

In the past year, the Commission has also certified to the Small Business Administration that certain other final regulations issued will not have a significant economic impact on a substantial number of small business entities. Nonetheless, the Commission published a Final Regulatory Flexibility Act ("FRFA") analysis along with

¹ Section 212 requires agencies to publish a "small entity compliance guide" for any new rule for which an agency is required to prepare a final regulatory flexibility analysis under section 3(a) of the Regulatory Flexibility Act, which is codified at 5 U.S.C. § 604.

² Pursuant to Section 728 of the Financial Services Relief Act of 2006, P. L. No. 109-351, which added section 503(e) to the Gramm-Leach-Bliley Act ("GLB"), the Commission together with seven other federal agencies were directed to propose a model form that may be used at the option of financial institutions for the privacy notices required under GLB.

these final regulations. We have either made available or are preparing updated compliance materials for each of these rulemakings although not required to do so by SBREFA. A few examples include:

- **Health Breach Notification Requirement for Vendors of Personal Health Records, codified at 16 C.F.R. Part 318:** Section 13407 of the American Recovery and Reinvestment Act of 2009 required that the Commission issue temporary breach notification requirements for vendors of personal health records and third parties that offer products or services through the web sites of vendors of personal health records. The notification requirements are triggered when there is a breach of security with respect to individually identifiable health information. After notice and comment, the Commission issued an interim final rule on August 17, 2009. The Commission has posted “Complying with the FTC’s Health Breach Notification Rule” at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus56.pdf>.
- **Prohibitions on Market Manipulation and False Information in Subtitle B of the Energy Independence and Security Act of 2007, codified in 16 C.F.R. Part 317:** Section 811 of the Act prohibits any manipulative or deceptive device or contrivance in connection with the wholesale purchase or sale of crude oil, gasoline or other petroleum distillate in contravention of such rules or regulations as the Commission may prescribe. Section 813 specified the methods of enforcing such a rule. After notice and comment, the Commission announced a final rule on August 6, 2009, that prohibits fraud or deceit in wholesale petroleum markets, and omissions of material information that are likely to distort petroleum markets. The rule was effective on November 4, 2009. The Commission has posted “Guide to Complying with Petroleum Market Manipulation Regulations” at <http://www.ftc.gov/os/2009/11/091113mmrguide.pdf>.

Red Flags Rule

The Identity Theft Red Flags Rule (“Red Flags Rule” or “Rule”), 16 C.F.R. Part 681, was promulgated by the Commission and four other agencies (which have their own comparable CFR sections for entities they regulate), as directed by the Fair and Accurate Credit Transactions Act of 2003. The Rule requires “creditors” and “financial institutions” that have certain “covered accounts” to develop and implement written identity theft prevention programs. These programs must be designed to help identify, detect, and respond to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft.

We are concerned that the legislation requiring the Red Flags Rule is overbroad and has had unintended consequences; numerous small businesses that regularly permit deferred payments for goods or services are “creditors” that are covered by the Rule. The Commission has no discretion to grant exemptions. The Commission recently further delayed enforcement of the Rule through December 31, 2010, while Congress considers

legislation that would exempt certain low-risk small businesses from the Rule's mandate. The Commission fully supports the effort to limit application of the Red Flags Rule and urges Congress to act quickly to narrow the scope of the Rule. In the interim, we have continued to address the concerns of small businesses.

In the November 2007 final rule announcement, the Commission certified that the Red Flags Rule would affect a substantial number of small business entities but would not have a significant economic impact on those small entities. Thus, the Commission was not obligated to perform a FRFA analysis. Nevertheless, the Commission decided to publish a FRFA analysis in this case. The FRFA analysis carefully addressed concerns of commenters who requested that the implementation date be delayed, that the Commission develop a small business compliance guide, and that we create a certification form for low-risk entities. Indeed, the Commission has been responsive to all these requests.

As you know from our separate May 26, 2009 letter to you,³ we have provided several extensions of the enforcement date for the Red Flags Rule and have engaged in extensive outreach and guidance to assist and ease compliance burdens for entities covered by the Red Flags Rule – especially small businesses. The Commission developed a Red Flags Web site (www.ftc.gov/redflagsrule) with articles and other materials, including a detailed business compliance guide that explains what types of entities are covered and provides step-by-step compliance advice, "Fighting Fraud with the Red Flags Rule: A How-To Guide for Business," available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>. And, for entities that have a low risk of identity theft (such as businesses that know their customers personally), the FTC issued an easy-to-use template to help them in developing written identity theft prevention programs to comply with the Red Flags Rule ("Create Your Own Identity Theft Prevention Program: A Guided 4-Step Process," available at www.ftc.gov/bcp/edu/microsites/redflagsrule/diy-template.shtm). As a result, the Commission believes that it has complied fully with its Regulatory Flexibility Act obligations.

* * * * *

For many years, the FTC has had a highly effective program providing compliance assistance to small businesses.⁴ We plan to continue to refine and improve these efforts.

³ A copy of this prior communication is enclosed for your convenience.

⁴ The Commission complements its compliance assistance efforts with consideration of the particular circumstances of a case when enforcing business obligations. As you know, Section 223 of SBREFA (1996) required that agencies establish policies to reduce or waive penalties for small entities in appropriate circumstances. In 1997, the Commission issued a small business leniency policy statement that describes factors that may result in reduction or waiver of penalties. See 62 Fed. Reg. 16,809 (Apr. 8, 1997) (issuing policy); 62 Fed. Reg. 46,363 (Sept. 2, 1997) (responding to comment received). As such cases arise, the Commission considers these leniency factors whenever a civil penalty may be assessed against a small business.

The Honorable Nydia M. Velázquez

Page 4

If you have any questions, please contact Christian S. White, the Deputy General Counsel for Legal Counsel and Small Business Coordinator at the Commission, at (202) 326-2476.

Respectfully,

/signed/
Jon Leibowitz
Chairman

Enclosure

cc: The Honorable Mary L. Landrieu
Chairwoman
Committee on Small Business & Entrepreneurship
United States Senate

In addition, and beyond SBREFA requirements, the Commission established corporate leniency policies for violations of the Textile and Wool Rules, 67 Fed. Reg. 71,566 (Dec. 2, 2002), the Funeral Rule (through the Funeral Rule Offender Program), and the Franchise Rule (through the Franchise Rule Alternative Law Enforcement Program) that have helped in fostering a more cooperative, less threatening regulatory environment for small entities. These policies have helped increase overall compliance with the rules while minimizing the burden on business of correcting certain minor or inadvertent errors that are not likely to injure consumers.



THE CHAIRMAN

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

May 26, 2009

The Honorable Nydia M. Velázquez
Chairwoman
Committee on Small Business
U.S. House of Representatives
Washington, DC 20515-0315

Dear Chairwoman Velázquez:

Thank you for your letter of April 8, 2009, concerning the Federal Trade Commission's ("FTC" or "Commission") Red Flags Rule. In your letter you pose two questions regarding the application of the Rule to small businesses in general and health professionals in particular. First, you ask if such businesses are properly covered by the Rule as "creditors" as that term is defined by law. You also question whether the FTC performed a proper analysis of the impact of the Rule on small businesses under the Regulatory Flexibility Act ("Reg Flex"). Your questions focus on the extent to which the Red Flags Rule may place burdens on these businesses.

Initially, as you know, the Commission further extended until August 1, 2009, the enforcement date for the Red Flags Rule. (The Commission had previously extended the enforcement date by six months.) The Commission was aware that some entities, particularly smaller and low risk organizations, were still unclear about the scope of the Rule and how best to comply with it. We are also aware that some assert that they should not be covered within the scope of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which they believe was written too broadly. Delaying enforcement of the Red Flags Rule should give Congress time to consider its position.

To address the lingering uncertainty about the Rule's scope and application, the Commission has developed a Web site (www.ftc.gov/redflagsrule) with articles, a business compliance guide – *Fighting Fraud with the Red Flags Rule: A How To Guide for Business* – and other materials. In addition, the Commission has released a compliance template for low risk entities. This template provides step-by-step instructions and a framework for drafting a written Identity Theft Prevention Program; entities can fill out the relevant information directly online and print the document. This template is available at: www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm. Further, I understand that the American Medical Association ("AMA") itself has developed a compliance template that focuses on identity theft risks and responses that are unique to medical practitioners. The additional time, coupled with these compliance tools, should enable organizations that have not

The Scope of the Rule

With respect to your first question about covering health care providers as “creditors” under the Rule, we believe that the plain language and purpose of the underlying statute (FACTA) and the Rule dictate that health care professionals are covered by the Rule when they regularly defer payment for goods or services. We also believe that implementation of the Rule will help reduce the incidence of medical identity theft, and that the burden on health care professionals need not be substantial.

We have included a copy of a letter to the AMA that more fully sets out our position on the application of the Red Flags Rule to health care providers. This letter explains that the Red Flags Rule is designed to address all forms of identity theft. Although the crime most commonly occurs in financial transactions, there are increasing concerns about identity fraud in the context of medical care. Medical identity theft may arise when a patient seeks care using the name or insurance information of another person, which can result in both false billing and potentially life-threatening corruption of a patient’s medical records. Congress revisited the medical identity theft issue in enacting the American Recovery and Reinvestment Act of 2009, which among other things required the Commission to initiate a rulemaking related to breaches by online vendors of personal health records, or by related entities, that collect consumers’ individually identifiable health information.

The letter also explains that the Red Flags Rule applies to “creditors” and “financial institutions,” which are statutorily defined terms.¹ The statute provides no exemptions, nor does it give the Commission the discretion to grant an exemption.² Because the Rule’s obligations are risk-based, however, the steps covered entities must take to address potential identity theft need only be commensurate with the risks they encounter. Accordingly, as a practical matter, the Rule should not impose significant burdens on health care providers where the risk of identity theft is low. For such health care providers, an appropriate Red Flags program might consist of little more than checking a photo identification at the time services are sought or when accepting a new patient, and, in the event the office is notified – for example by a consumer or law enforcement – that the person’s identity has been misused, having appropriate procedures in place such as not billing the victim or not reporting the debt on her credit report. The compliance templates from the FTC (and for health care providers, the AMA) should help low risk entities in developing these programs.

¹ In particular, the FACTA, which amended the Fair Credit Reporting Act, defines “creditor” by reference to the Equal Credit Opportunity Act (“ECOA”). The ECOA defines “creditor” as “any person who regularly extends, renews or continues credit...” and defines “credit” as “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.”

² See *Public Citizen v. FTC*, 869 F.2d 1541, 1557 (D.C. Cir. 1989) (“[A]gencies surely do not have inherent authority to second-guess Congress’ calculations. . . . [A]bsent an express grant of authority to change the terms of the statute, we will not imply agency authority to alter the statutory mandate.”).

The Rulemaking Process

In your letter, you also question whether health care professionals had sufficient notice of the Red Flags rulemaking. You assert that such persons were not mentioned in the Rule itself and that the reference in the Federal Register notice to “creditors in the health care field” did not provide sufficient notice to health care professionals. You urge the Commission to engage in a new rulemaking specific to the application of the Red Flags Rule to health care providers.

It is true that health care providers – along with many other businesses and organizations – were not specifically mentioned in the Rule. As the Commission noted in the Federal Register notices for the proposed and final Rules, the breadth of the definition of “creditor” as dictated by FACTA would have made it highly impractical to attempt to include a comprehensive list of every type of business potentially covered by the Rule, as some businesses inevitably would be left off the list. The Commission specifically noted that “[G]iven the coverage of the proposed Rule, a very large number of small entities across almost every industry could be subject to the Rule” and “the entities under the FTC’s jurisdiction are so varied that there are no general sources that provide a record of their existence.”³ Thus, it was neither feasible nor prudent that the FTC attempt to enumerate all of the entities or industry sectors that might be covered by the Rule.

Nonetheless, the Commission believes that the notice provided was appropriate and adequate. The Notice of Proposed Rulemaking (“NPRM”) makes clear that the Rule’s coverage of “creditors” is the same as that of the ECOA, as dictated by the FACTA. The ECOA and its implementing regulation, Regulation B, have been in effect for almost 35 years. Indeed, the Board of Governors of the Federal Reserve Board (“Federal Reserve Board”), in promulgating Regulation B pursuant to its authority under the ECOA, *see* 15 U.S.C. 1691(b), noted that doctors and dentists extend “credit” when they permit their patients to defer payment of fees.⁴ Ten years later, the Federal Reserve Board reconfirmed this point in its Official Staff Commentary.⁵

Furthermore, two years before the Red Flags Rule was promulgated, the Federal bank regulatory agencies promulgated a rule on the use of medical information in credit determinations also under the FACTA, in which they reaffirmed that health care providers can be “creditors.” The agencies expressly explained that “[c]reditors include depository

³ 71 Fed. Reg. 40,786, at 40,806 (July 18, 2006) and 72 Fed. Reg. 63,718 at 63,750 (Nov. 9, 2007).

⁴ *See* 40 Fed. Reg. 49,298, at 49,304 (Oct. 22, 1975).

⁵ The Official Staff Commentary states: “[i]f a service provider (such as a hospital, doctor, lawyer, or merchant) allows the client or customer to defer the payment of a bill, this deferral of a debt is credit for purposes of the regulation, even though there is no finance charge and no agreement for payment in installments.” 12 CFR 202.3. 50 Fed. Reg. 48018, 48,048-48,055 (Nov. 20, 1985).

institutions as well as entities that are neither depository institutions nor affiliates of depository institutions, such as independent finance companies, loan brokers, *health care providers*, and automobile dealers.” (Emphasis added).⁶

Thus, the Commission reasonably concluded that health care professionals were aware or had reason to be aware that they could be creditors for the purposes of the FACTA, and could file a comment on this issue during the NPRM proceeding. Indeed, one organization submitted a comment squarely recognizing the risk of medical identity theft, and urging that the final Rule address how the Rule would apply to creditors in the medical context. See World Privacy Forum (Sept. 18, 2006) *available at* www.ftc.gov/os/comments/redflags/523455-00020.pdf. This comment resulted in the discussion of the coverage of health care providers in the Federal Register notice for the final Rule, which you point out in your letter.

In sum, the Commission believes that it provided appropriate notice about the broad application of the “creditor” definition during the rulemaking process.

Regulatory Flexibility Act

Your letter also questions whether the Commission met the requirements under Reg Flex in promulgating the Rule. You point out that considering the views of small firms provides agencies with a better-informed rulemaking process that ultimately results in more effective regulations. The Commission agrees that soliciting and considering the comments of small businesses during the rulemaking process is extremely valuable, and it strives to do so in all relevant rules, consistent with Reg Flex requirements.⁷

As you know, Reg Flex imposes certain procedural requirements that each federal agency must follow when engaged in rulemaking. The Commission, when issuing the proposed and final versions of the Rule, certified that it would affect a substantial number of small businesses, but would not have a significant economic impact on those small entities.⁸ Thus, the Commission was not obligated to perform a Reg Flex analysis. Nevertheless, to ensure the most complete record, the Commission decided to publish a Reg Flex analysis in this case.⁹

In its initial regulatory flexibility analysis (“IRFA”), the Commission estimated that the proposed regulations would cover approximately 11.1 million entities “across almost every

⁶ Fair Credit Reporting Medical Information Regulations, 70 Fed. Reg. 70,666 (Nov. 22, 2005).

⁷ See 71 Fed Reg. 40,805; 72 Fed Reg. 63,749.

⁸ 71 Fed Reg. at 40,805; 72 Fed Reg. at 63,749.

⁹ 71 Fed Reg. at 40,805.

industry,” ninety percent of which were expected to qualify as small businesses.¹⁰ The Commission recognized that the proposed requirements would involve some increased costs for affected parties, but since it was likely that many affected entities already engaged in various activities to minimize losses due to fraud, it was expected that the impact of the Rule would “be merely incremental and not significant.” Due to the flexible, risk-based nature of the proposed Rule, the Commission stated that it did not expect any significant legal, professional, or training costs to comply with the Rule, and expected that the costs of compliance for low-risk entities would be “quite modest.”¹¹ The NPRM requested comment on the number of small businesses that would be covered by the Rule, the costs of compliance for small businesses, and the need, if any, for alternative compliance methods that would reduce the economic impact of the Rule on small businesses.¹²

In publishing the final regulations, the Commission affirmed its initial conclusions.¹³ In its final regulatory flexibility analysis (“FRFA”), the Commission also addressed the concerns of commenters who stated that the projected time for compliance had been underestimated, and requested that the implementation date for the final Rules be delayed by six months for small businesses. Commenters also asked the Commission to consider developing a small business compliance guide and creating a certification form for low-risk entities. For example, *see* Comment of Office of Advocacy, U.S. Small Business Administration (Sept. 18, 2006) available at www.ftc.gov/os/comments/redflags/523455-00024.pdf.

In light of these comments, the Commission increased its estimate of the time required to comply with the final Rule for both low-risk and high-risk entities, noting, however, that covered entities with a low risk of identity theft would only need to develop a streamlined program.¹⁴ The Commission and the other Agencies also set the compliance deadline for November 1, 2008, providing all entities with more than the requested six months needed to comply with the Rule.¹⁵ In addition, the Commission agreed to develop a small business compliance guide prior to the enforcement deadline, and consider whether to include a model form.¹⁶ As described above, the Commission has since published both a small business compliance guide and a template for low risk entities.

¹⁰ *Id.* at 40,806.

¹¹ *Id.*

¹² *Id.* at 40,807.

¹³ 72 Fed Reg. at 63,751.

¹⁴ *Id.* at 63,749-63,750.

¹⁵ As described *infra*, the Commission later postponed its enforcement date for an additional nine months.

¹⁶ *Id.* at 63,752.

As you note in your letter, a rule may be invalidated in certain cases where the issuing agency does not conduct any regulatory flexibility analysis,¹⁷ or certifies that there is no significant economic impact to small businesses in contradiction with the results of its own Reg Flex analysis.¹⁸ However, unlike the cases cited in your letter, the Commission has prepared both an initial and final Reg Flex analysis; conducted a reasonable, good faith effort to analyze and address the impact of the Red Flags Rule on small businesses; and responded appropriately to the comments received.¹⁹ As a result, the Commission believes that it has complied fully with its Reg Flex obligations.

Outreach and Assistance

The Commission has taken a number of steps to assist and ease compliance burdens for the entities covered by the Rule. Initially, as discussed above, the Agencies provided a compliance date of November 1, 2008, eleven months after the effective date of January 1, 2008, to allow entities time to develop their programs. Notwithstanding that allowance, FTC staff heard concerns from covered entities in certain industries that they were uncertain of their compliance obligations. As a result, the Commission initially granted an additional six month enforcement delay until May 1, 2009. As noted at earlier, the Commission has further extended the enforcement delay to August 1, 2009, to enable covered entities to develop and implement their Identity Theft Prevention Programs.

Throughout this time, FTC staff maintained an expansive outreach effort to educate the many different types of covered entities about the Rule. This included numerous speaking engagements, webinars, and teleseminars, as well as the release of general and industry specific articles (including an article for health care providers²⁰). Staff also responded to inquiries by telephone and email through our dedicated email box (RedFlags@ftc.gov). FTC staff also has worked with a number of trade associations that have chosen to develop model policies or specialized guidance for their members, published *Fighting Fraud with the Red Flags Rule: A How To Guide for Business*, and established a dedicated website

¹⁷ *AFL v. Chertoff*, 552 F. Supp. 2d 999, 1004 (N.D. Cal. 2007) (granting preliminary injunction preventing agency from enforcing a rule when the agency failed to conduct a final Reg Flex analysis).

¹⁸ See *North Carolina Fisheries Ass'n v. Daley*, 27 F. Supp. 2d 650, 655 (E.D. Va. 1998) (rejecting the certification when the agency consciously ignored its own data and selected a flawed methodology for analyzing impact of a rule on small businesses).

¹⁹ See *United States Cellular Corp. v. FCC*, 254 F.3d 78, 88-89 (D.C. Cir. 2001) (noting that an agency complies with Reg Flex when it undertakes a "reasonable, good-faith effort to carry out [Reg Flex's] mandate.") (quoting *Alenco Communications, Inc. v. FCC*, 201 F.3d 608, 625 (5th Cir. 2000)). See also *Nat'l Coalition for Marine Conservation v. Evans*, 231 F. Supp. 2d 119, 143 (D.D.C. 2002) (distinguishing *North Carolina Fisheries Ass'n*, 27 F. Supp. 2d at 659-60, and finding that an agency satisfied the procedural requirements of Reg Flex when it published both an IRFA and FRFA during rulemaking, and did not consciously ignore data or select a flawed methodology for its analysis on the burdens of the rule).

²⁰ See "The Red Flags Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft" available at <http://www.ftc.gov/bcp/edu/pubs/articles/art111.shtm>.

(www.ftc.gov/redflagsrule). FTC staff has offered to work with trade associations for health care providers on outreach and guidance regarding the Rule, and is pleased that the AMA developed such a template. As noted earlier, the Commission also has prepared a template to further help low-risk entities in drafting their streamlined programs to comply with the Rule (www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm).

Conclusion

The Commission is sensitive to regulatory burdens placed on businesses and organizations with limited resources, particularly in the current economic climate. The Red Flags Rule requires *reasonable* policies and procedures to identify, detect, prevent, and mitigate identity theft and has a flexible, risk-based structure to allow entities to design a program that is tailored to the nature of their business. This approach should place a minimal burden on covered businesses, while protecting consumers from the serious consequences from identity theft. The additional extension for enforcement of the Rule should allow companies to put reasonable policies and procedures in place, and give Congress time to consider the views of those who take issue with their coverage by FACTA.

Thank you once again for bringing this matter to the FTC's attention. If you or your staff have any additional questions or comments or wish to provide additional information, please contact me at (202) 326-3400 or Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2946.

Respectfully,

/signed/
Jon Leibowitz
Chairman