FTC's Red Flags Rule: Delays Suggest Confusion on the Part of the Industry

LISA J. SOTTO AND BORIS SEGALIS

The authors examine the elements of the Red Flags Rule and explain how to comply with its requirements.

Several months ago, the Federal Trade Commission (the "FTC" or "Commission") postponed enforcement of the provisions of the Identity Theft Red Flags and Address Discrepancies Rule (the "Red Flags Rule" or "Rule") requiring certain financial institutions and creditors to implement an identity theft prevention program.[1] The new deadline — August 1, 2009 — represents a second delay in the enforcement of the Rule. The previous compliance date was May 1, 2009, which was an extension from the original deadline of November 1, 2008. The continuing enforcement delays reflect businesses' ongoing uncertainty about the Rule's intended scope and requirements.

Since the Red Flags Rule came into effect on January 1, 2008, it has become clear that many entities that may be subject to the Rule have experienced significant difficulties in understanding and complying with the

---

Lisa J. Sotto, partner and head of the Privacy and Information Management Practice at Hunton & Williams LLP, focuses her practice on privacy, data security, and information management issues and assists clients in identifying and managing risks in these areas. Boris Segalis is an associate in the firm's New York office focusing his practice on privacy, data security, and information management issues. The authors can be reached at lsotto@hunton.com and bsegalis@hunton.com, respectively.

Published in the July 2009 issue of Privacy & Data Security Law Journal.

Rule. The Rule contains several broad requirements, but it is the mandate to implement an identity theft prevention program that businesses have found perplexing.[2] The FTC has estimated that over 11 million U.S. businesses may be subject to the Rule.[3] Some organizations, such as banks and mortgage lenders, have long had comprehensive identity theft and fraud prevention programs in place and found the Red Flags Rule to be a helpful framework that brought their existing policies and procedures under a single framework.[4] Others, such as health care providers, nonprofit organizations, commercial lenders, retailers, law firms and small businesses, however, were surprised to learn that they could be subject to the Rule. Anecdotal reports suggest that some of these businesses continue to mistakenly assume that the Rule does not apply to them. Others, even after acknowledging that the Rule applies, have struggled to understand what is required for compliance.

There appear to be two primary reasons businesses have struggled with the Red Flags Rule. First, under the FTC's interpretation, the Rule applies to many entities that have little or no prior experience in complying with identity theft regulations. Second, the Rule is unique in that it does not specify the form or content of the required identity theft prevention program, but instead mandates a process that businesses must follow in developing a program tailored to their specific risk level. The required compliance effort may vary based on the types of accounts a business offers or maintains, associated risks and the size of the business.

The FTC is keenly aware of these issues. To address businesses' concerns, the Commission launched a robust outreach effort and has twice delayed the enforcement deadline for the provisions requiring the implementation of an identity theft prevention program. One of the milestones in the Commission's outreach effort was the publication of a compliance guide for businesses. The guide, entitled "Fighting Fraud With The Red Flags Rule: A How-To Guide for Business" (the "Red Flags Guide"), is intended to help businesses understand how to comply with the Rule. Interestingly, it has also reinforced the Commission's broad interpretation of the Rule.[5] Indeed, some commentators have suggested that the Guide significantly exceeded the scope of the Rule. In announcing the latest delay, the FTC acknowledged "the ongoing debate about whether Congress

wrote the [relevant] provision [of FACTA] too broadly."[6] The FTC also issued a compliance template designed to assist financial institutions and creditors "at low risk for identity theft" in developing the identity theft prevention program and a set of FAQs.[7]

While the additional guidance is helpful, for many businesses it will not alleviate the need to undertake a serious compliance effort. Despite the anxiety associated with the Rule, businesses will find that, beyond the veneer of complexity, the Rule is a sensible risk-based framework that should be helpful in combating identity theft-based fraud.

SCOPE OF THE RULE'S IDENTITY THEFT PREVENTION PROGRAM PROVISIONS

The first step in complying with the Rule is determining whether your organization falls within the Rule's scope. The Rule's requirement to implement an identity theft prevention program applies to two categories of entities: (i) "financial institutions," which are defined as banks, savings associations and credit unions, and entities that hold consumer accounts from which account holders can withdraw or direct funds for payment to third parties, and (ii) "creditors," defined as entities that regularly extend, renew, arrange for or continue credit.[8]

Entities that meet the Rule's definition of "financial institution" have voiced few objections about compliance with the Rule. This is not surprising given that most financial institutions are subject to the jurisdiction of the federal banking regulators and are likely to have existing fraud detection and regulatory compliance programs. The definition of "creditor" and the FTC's broad view of that definition, on the other hand, have led to a flood of questions and concerns.

A complicating factor is the FTC's insistence on interpreting the Rule very broadly. In publications, on panels and in the Guide, FTC attorneys have taken the position that the Commission intends to interpret the definition of "creditor" and the types of accounts subject to the Rule broadly. The FTC has stated that medical professionals, nonprofits and government agencies are subject to the Rule if they meet the definition of "creditor." According to the Guide, any business that sells goods or services and al-

Published in the July 2009 issue of Privacy & Data Security Law Journal.

lows customers to pay for them later would be considered a "creditor" under the Rule and, therefore, subject to the provisions requiring the implementation of an identity theft prevention program. Thus, according to the FTC, the definition of "credit" may encompass any "invoice billing" arrangement, including those practiced by law firms, health care providers, manufacturers, utility companies and myriad other businesses that do not require immediate payment for their products or services. Retailers that offer "no interest/no payment" programs that recently have become the norm also are likely "creditors" subject to the Rule.

The scope of the Rule's definition of "creditor" extends beyond entities that offer credit to customers and may include entities that regularly "participate…in credit decisions."[9] Examples of activities that may qualify as "participation in credit decisions" include:

1. Conducting initial assessment of customers' credit applications,
2. Screening applications to determine whether or not to submit them to lenders,
3. Negotiating credit payment terms with customers,
4. Receiving proceeds from a portion of an interest rate on a credit line,
5. Setting the terms of credit,
6. Restructuring the terms of a sale to meet the concerns of a creditor (*e.g.*, by requesting a larger down payment, requesting that the applicant find a cosigner or lowering the price of the item to lower the loan-to-value ratio), or
7. Advocating for extending credit after an initial denial of credit.[10]

Whether an entity is a "creditor" may be a factual inquiry and no factor is necessarily dispositive.[11]

This definition of "creditor" should be particularly troubling for retailers and other businesses (such as airlines) that accept applications for private label or third party credit cards. Even where a business does not evaluate applications but instead passes them on to credit card issuers, the FTC takes the position that these businesses could be subject to the Rule if

they are otherwise involved in the credit card program, as may be the case, for example, with private label cards. Activities such as sharing in the interest rate or advocating for a higher credit limit may bring businesses within the Rule's scope. Indeed, the Red Flags Guide lists as an example of creditors, "retailers that offer financing or help consumers get financing from others…by processing credit applications." During several panel discussions, FTC lawyers have suggested that, at the very least, the issue of whether a business that processes credit card applications is a "creditor" under the Rule is a fact-specific inquiry.

COVERED ACCOUNTS

After a business determines that it is a creditor or financial institution within the meaning of the Rule, the next step is to determine if it offers or maintains any "covered accounts." If it does, the business must develop and implement an identity theft prevention program for those accounts. The requirement to implement an identity theft prevention program applies only to creditors and financial institutions that offer or maintain (i) personal or household accounts that involve or are designed to permit multiple transactions (*i.e.*, consumer accounts) or (ii) other accounts that are associated with a reasonable risk of harm to the entity or its customers from identity theft. In practice, the Rule requires financial institutions and creditors that offer or maintain most consumer accounts to implement an identity theft prevention program. Consumer accounts that involve or are designed to permit multiple transactions are automatically covered by the Rule. Financial institutions and creditors that offer or maintain other accounts (such as business accounts) have the discretion under the Rule to determine whether such accounts must be covered by the program. To make this determination with respect to a non-consumer account, an entity must assess the risk of identity theft associated with the account by considering:

1. Whether the account is of the type that is reasonably susceptible to risk of identity theft,
2. Whether methods that customers may use to open the account are associated with risk of identity theft,

3. Whether methods customers may use to access or use the account and the information that may be accessed are associated with risk of identity theft, and
4. The entity's experience with identity theft issues in connection with the relevant account.

If, based on an evaluation of these factors, the entity determines that the account is associated with a reasonably foreseeable risk of harm from identity theft, the account must be covered by an identity theft prevention program. Examples of business accounts that may be subject to the Rule are accounts offered to or maintained for small businesses or sole proprietorships and business accounts in connection with which a creditor or a financial institution maintains confidential personal information (*e.g.*, outsourcing accounts). Notably, if an entity determines in the initial risk assessment that an account is not associated with a risk of harm from identity theft, it must periodically (at least annually) reassess the risk associated with the account.

It is important to note that the FTC appears to take a broad view of the definition of "covered accounts." The FTC has labeled this approach an "in for one in for all" approach. Thus, a creditor's covered accounts could include any "account" the creditor offers or maintains (which the Rule defines as a continuing relationship) rather than accounts with respect to which the business is a creditor. For example, if an insurance company offers some accounts that allow consumers to pay for policies after the coverage period and other accounts that require periodic payments that prepay coverage (and, therefore, do not involve "credit"), the Guide appears to suggest that all such accounts would be "covered" under the Rule and subject to the identity theft prevention program. In addition, the insurance company would need to evaluate the risk of harm from identity theft associated with any non-consumer credit and non-credit accounts it offers or maintains to determine if those accounts are covered. The implication for financial institutions subject to the FTC's jurisdiction is that coverage of the Rule could extend to non-transactional accounts, *i.e.,* accounts that do not allow check-writing or similar fund transfer privileges.

DEVELOPMENT AND IMPLEMENTATION OF AN IDENTITY THEFT PREVENTION PROGRAM

After an entity determines that it offers or maintains covered accounts, the next step is to determine the scope of its obligations under the Rule. The FTC has continuously emphasized the risk-based nature of the identity theft prevention program provisions. Low risk entities may take advantage of the template program published by the FTC (addressed below).

The Rule does not articulate specific requirements for the identity theft prevention program's form or content, but instead sets forth the process that businesses must follow in developing, implementing and administering the program. This process may be challenging and time-consuming, especially for entities that previously have not taken a comprehensive approach to combating identity theft.

One of the keys to understanding how to develop an identity theft prevention program is deconstructing the Rule's definition of "identity theft." The Rule defines identity theft as fraud that is committed or attempted using identifying information of another person without authority."[12] Accordingly, the Rule may be best viewed as a fraud prevention regulation. Often, rather than attempting to steal an identity, the perpetrator is using personal information he has stolen or otherwise obtained unlawfully to commit fraud. It is important to keep in mind that the purpose of the Rule is to enable businesses to detect the tell-tale signs of this type of fraud (*i.e.,* Red Flags), develop response mechanisms that enable businesses to effectively prevent such fraud (after its signs are detected), and mitigate the damage the fraud may cause.

To do so, entities must (i) identify patterns, practices and activities that indicate the possible existence of identity theft (*i.e.,* Red Flags) in connection with relevant accounts the entity offers or maintains, and (ii) develop methods for detecting and responding to those Red Flags. There is additional guidance in the Rule on developing, implementing and administering the program, including examples of Red Flags and suggested detection and response methods.[13] The FTC has specifically cautioned businesses, however, not to use the guidelines as a substitute for their own efforts to identify Red Flags that are relevant to their business and develop

appropriate detection and response methods.

The initial Red Flags program must be approved by the covered entity's board of directors or, for entities that do not have boards, by senior management. Following initial approval and implementation, covered entities must periodically evaluate the effectiveness of the program and appropriately update the program to reflect the entities' own experiences with identity theft issues as well as changes in relevant business arrangements and known methods of identity theft.

ADMINISTERING THE IDENTITY THEFT PREVENTION PROGRAM

The Rule imposes a number of administrative requirements on covered financial institutions and creditors. Specifically, entities are required to:

1. Assign responsibility for the implementation and administration of the identity theft prevention program,
2. Prepare annual reports to evaluate the program's effectiveness,
3. Periodically update the program (which includes identifying additional covered accounts, if any, and relevant Red Flags), and
4. Train relevant personnel to implement the program effectively.

In addition, entities subject to the Rule are required to take steps to ensure that relevant service providers conduct their activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. Such steps may include contractually requiring the service providers to (i) maintain policies and procedures to detect Red Flags relevant to the functions performed by the service providers, and (ii) either report the Red Flags to the covered entity when they are detected or take appropriate steps to prevent and mitigate identity theft in response to the detected Red Flags. The Rule also requires that relevant service providers be required to periodically submit to audits of their identity theft policies and procedures.[14]

Businesses that are service providers to financial institutions or credi-

tors are likely to receive requests from their customers to (i) confirm that they maintain appropriate identity theft detection, prevention and mitigation policies and procedures, or (ii) monitor for and detect relevant Red Flags and take appropriate remedial action. By developing their own streamlined programs, service providers may avoid having to satisfy myriad Red Flags-related requests from their customers. Service providers also may choose to request from their customers detailed instructions on detecting and responding to Red Flags relevant to the service provider's tasks.

LOW RISK COMPLIANCE TEMPLATE

On May 13, 2009, the FTC published a template designed to assist financial institutions and creditors at low risk for identity theft in developing the identity theft prevention program required by the Rule.[15] While the Rule does not explicitly contemplate a category of entities that are at low risk for identity theft, the imposition of less onerous requirements on lower-risk entities is consistent with the Rule's risk-based approach to combating identity theft. To take advantage of the low risk template, an entity first must assess whether it is at low risk for identity theft. The FTC suggests that low risk may be shown by factors such as knowing customers personally, providing services at customers' homes, not having experienced fraud based on identity theft in the past and being in a line of business in which it is uncommon to experience fraud due to identity theft. These factors are not exhaustive, however, as the template requires entities to also consider their unique circumstances in determining their identity theft risk level. The assessment and the resulting conclusion must be documented in the template.

The FTC template guides low risk entities through the requirements of the Rule by asking them to identify Red Flags they may experience in their business if a consumer tries to obtain a product or service via identity theft. The template assists low risk entities in selecting methods to detect and respond to Red Flags and administering their identity theft prevention programs, including implementing updates and managing service providers. Unlike the Rule, the template requires low risk entities to document only

the final, streamlined program (which may be done by simply printing the completed template). The template also appears to place less emphasis than does the Rule on the process by which the program is developed. The template's program administration requirements are also less onerous than those contemplated by the Rule.

Notably, the template does not address the issue of whether an entity is subject to the Rule; rather, it assists only in the implementation of an identity theft prevention program once the entity has determined that it is subject to the Rule and is a low risk entity. In other words, the template does not assist entities in the determination of whether they are financial institutions or creditors, nor does it assist entities in determining whether they have "covered accounts" that necessitate implementation of an identity theft prevention program, although these issues have been the subject of much debate and confusion among business interests. In order to make these determinations, businesses may look to the Rule and the FTC's guidance documents.

ENFORCEMENT OUTLOOK

The FTC has primary responsibility for enforcing the Red Flags Rule. The Commission will oversee implementation of the Rule by all relevant entities that are not regulated by the federal banking regulators that promulgated the Rule jointly with the FTC. FTC lawyers have indicated that the Commission is in the process of developing an enforcement strategy for the Red Flags Rule. They have suggested that, similar to the FTC's approach to information security, Red Flags enforcement likely will focus on entities that have fundamentally deficient compliance programs or are egregious violators of the Rule. In light of the fact that the FTC views the protection of consumers from identity theft as an essential part of its mission, we can expect the Commission to add the Red Flags Rule as one more enforcement tool in cases of significant data security compromises.

NOTES

[1] The Red Flags Rule implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act ("FACTA"). *See* 15 U.S.C. §§ 1681m(e),

1681c(h). The Rule was promulgated jointly by the FTC and federal banking regulators (the Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision and National Credit Union Administration). The compliance deadline for entities subject to the enforcement jurisdiction of the federal banking regulators was November 1, 2008. *See, e.g.,* 16 C.F.R. §§ 681.1 - 681.3, promulgated by the FTC; 12 C.F.R. §§ 222.82, 90, 91, promulgated by the Federal Reserve; 12 C.F.R. §§ 334.82, 90, 91, promulgated by the FDIC.

[2] *See* 16 C.F.R. § 681.2.

[3] Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, the Federal Trade Comm'n, BNA Audioconference: The Red Flags Rule (Apr. 23, 2009).

[4] Many of these businesses are financial institutions subject to the jurisdiction of the federal banking regulators (such as the FDIC, Federal Reserve and others) and required to comply with the entire Red Flags Rule by November 1, 2008.

[5] The Red Flags Guide was published on March 20, 2009 and is available at www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.

[6] "FTC Will Grant Three-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Adopt Identity Theft Prevention Programs," Apr. 30, 2009, at www.ftc.gov/opa/2009/04/redflagsrule.shtm.

[7] The template is entitled "A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft" and is available at www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm. The FAQs are available at www.ftc.gov/os/2009/06/090611redflagsfaq.pdf. The FAQs were published on June 11, 2009 and, therefore, are not explicitly addressed in this article. A brief overview suggests that while the FAQs present the information in a helpful, user-friendly format, they do not appear to contain information that further clarifies the Rule's requirements.

[8] *See* 15 U.S.C. § 1681a(r)(5), (t); 12 U.S.C. § 461(b)(1)(C); 15 U.S.C. § 1691a(d), (e). As discussed above, with respect to many financial institutions, the Red Flags are enforced by the institutions' functional regulators (the federal banking agencies and the National Credit Union Administration) rather than the FTC.

[9] *See* Regulation B, 12 C.F.R. § 202, implementing the Equal Credit Opportunity Act, 15 U.S.C. § 1691a.

[10] *See, e.g., Treadway v. Gateway Chevrolet Oldsmobile, Inc*., 362 F.3d 971, 979 (7th Cir, 2004); *Barnette v. Brook Rd., Inc*., 457 F. Supp. 2d 647, 655 (E.D. Va. 2006); *Bayard v. Behlmann Auto. Servs.*, 292 F. Supp. 2d 1181, 1186-87 (E.D. Mo. 2003).

[11] *See, e.g., Barnette*, 457 F. Supp. 2d at 655.

[12] *See* 16 C.F.R. § 681.2(b)(8).

[13] *See* 16 C.F.R. § 681 app. A.

[14] This requirement is not explicitly stated in the Rule but is instead based on the requirements the Rule imposes on covered entities to (i) consider service provider oversight arrangements in the risk assessment conducted for periodic identification of covered accounts, and (ii) address service provider oversight arrangements in periodic compliance reports.

[15] The template program is entitled "A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft" and is available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm.