IS YOUR BUSINESS RED FLAG COMPLIANT?

By Jennifer R. Rossi and Kori Termine Wisneski

In recent years, concerns about "identity theft" and "data security breaches" have become commonplace, creating an environment of fear and trepidation for both individuals and businesses alike.

In the case of a data security breach, which is an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information (including an individual's Social Security number or credit card number), the effects can be devastating for everyone involved. Because the potential exposure of one data security breach is so great and may affect thousands of individuals, many state and federal governments have enacted legislation and regulations to limit the use of personally identifiable information, particularly in circumstances where such dissemination is wholly unnecessary, and to create a system for limiting exposure if there is a breach.

In the case of identity theft prevention, on the federal level, the Federal Trade Commission ("FTC") amended the Fair Credit Reporting Act ("FCRA") to add the "Red Flags Rule," which requires "financial institutions" and "creditors" maintaining "covered accounts" to establish written programs to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. Because the definitions of these terms are broad and the ramifications of not complying could be severe, many businesses, including lawyers and law firms, have been pressing the FTC to articulate more clearly who is subject to these rules.

The American Bar Association, for instance, has gone so far as to file a lawsuit over this very subject, claiming that lawyers and law firms should not be subject to the Red Flags Rule for a number of reasons and seeking an injunction to block the applica-

tion of the Rule to practicing lawyers and law firms. *See American Bar Ass'n v. Fed. Trade Comm'n*, Dkt. No. 1:09-cv-01636-RBW, District Court for the District of Columbia. On September 23, 2009, the ABA filed a partial motion for summary judgment on the grounds that the FTC's application of the Red Flags Rule to attorneys violates the Administrative Procedure Act as it is "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." *See* Plaintiff's Motion for Partial Summary Judgment, dated September 29, 2009, at 1. After hearing oral argument on this Motion on October 29, 2009, Judge Reggie Walton of the U.S. District Court for the District of Columbia granted the ABA's Motion, issuing an order the following day. *See* Order, dated October 30, 2009. A Memorandum of Decision detailing the basis of the Court's Order is expected to be issued with 30 days. As for the next steps, the parties are now scheduled to submit a joint proposed schedule by November 30, 2009, setting forth deadlines for the ultimate resolution of the matter.

Given the controversy and uncertainty concerning who should comply with the Red Flags Rule, the FTC has delayed its enforcement of the Rule on four separate occasions. The deadline for compliance, however, is now set for June 1, 2010. This article offers the tools necessary to determine whether businesses should be implementing a written Identify Theft Program and offers some guidelines for compliance.

Applicability

Currently, the legislature has not expressly exempted any business from complying with the Identify Theft Red Flags Rule. To first determine whether the Red Flags Rule even applies to you, it is important to know the definitions of some key terminology, such as "creditor" and "financial institution," and to analyze whether your practice or your client's business falls within the ambit of these definitions. The Red Flags Rule adopts the same definition of "creditor" as that used in Section 702 of the Equal Credit Opportunity Act. *See* 15 U.S.C. § 1681a(r)(5). Thus, a "creditor" includes any person who regularly extends, renews, or continues credit or who regularly arranges for the extension of credit. *See* 15 U.S.C. § 1691a(e). A "financial institution," on the other hand, is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, and "any other person that, directly or indirectly, holds a transaction account belonging to a consumer." *See* 15 U.S.C. § 1681a(t).[1] The central issue in determining whether the Red Flags Rule applies is whether the entity in question could arguably be considered a "creditor" who maintains "covered accounts."

More specifically, to determine if you are required to comply with the Red Flags Rule, you need to answer two questions:

1. Does the business in question conduct business in a manner that meets the applicable definition of "creditor"?
2. If so, does it maintain "covered accounts"?

If the answer to both of these questions is "yes," the business should implement a written Identity Theft Prevention Program.

Is the Business a Creditor?

The first inquiry is whether or not the business falls within the definition of "creditor." While a well-founded argument exists that a law firm would not ever be a "creditor" under the Red Flags Rule as a matter of law,[2] lawyers and law firms should also be aware that the FTC disagrees.[3] Only time will tell how this issue will play out in the courts. Thus, it is important to consider not only how our clients are affected by the Rule, but how we, as lawyers, or how our law firms may be affected.

In undertaking this analysis, you should know that the FTC takes the position that the definition of "creditor" is broad and can include businesses that regularly permit a debtor to defer payment for goods or services. For example, under the FTC's interpretation of the current legislation (the Red Flags Rule), if a law firm provides services to a consumer client and regularly permits the client to defer payment for those services to a later date, the law firm or business may be considered a creditor under the Red Flags Rule.[4] The definition of "creditor" is activity-based, not industry-based.

Does the Business Maintain Covered Accounts?

Second, if you determine that the business is a creditor, the next question is whether it maintains covered accounts. "Covered accounts" are accounts that (i) are created primarily for personal or family purposes (such as mortgage loans, automobile loans, cell phone accounts, utility accounts) and that can be paid off over multiple payments, or (ii) have a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

In determining if accounts are covered under (ii) above, consider how they are opened and accessed. Also consider the subjective nature of "reasonably foreseeable risk." Further, it is important to remember that the Red Flags Rule, among other things, is designed to protect personal identifying information from being compromised.

Developing a Program

If you believe that the business qualifies both as a creditor *and* a business that maintains covered accounts, it is required to develop and implement a written Identity Theft Prevention Program by November 1, 2009. The program must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new client accounts and the operation of existing ones. The program must be appropriate to the size and nature of the business or practice and also take into consideration the scope of the business' activities and the type of work it handles. Although there is no one-size fits-all approach (because each program must be appropriately tailored to the concerns of the particular business seeking to implement it), the FTC has provided some guidance that is helpful.

According to the FTC's "How-To Guide for Businesses" on the Red Flags Rule, there is a four step process for ensuring compliance: (1) identify relevant red flags, (2) detect red flags, (3) prevent and mitigate identity theft, and (4) update the program regularly. *See* http://www2.ftc.gov/redflagsrule. Under the first step, you are encouraged to identify the red flags, or the potential patterns, practices, or specific activities indicating the possibility of identity theft, that may be unique to the business.

Once you have identified the red flags of identity theft, you must then lay out procedures for detecting them in the business' day-to-day operations.

Next, when you spot a red flag, your law firm

(continued on next page)

As the ABA fights application of the FTC's Identify Theft Prevention Rule to lawyers, Connecticut businesses must evaluate whether Red Flags applies to them.

or your client must be prepared to respond appropriately and efficiently. The guidelines in the Red Flags Rule offer examples of some appropriate responses, including:

- monitoring a covered account for evidence of identity theft
- contacting the client
- changing passwords, security codes, or other ways to access a covered account
- closing an existing account
- reopening an account with a new account number
- notifying law enforcement; and/or
- determining that no response is warranted under the particular circumstances

In addition to offering the above guidelines, earlier this year, the FTC released a template to assist businesses with low risk of identity theft in complying with the Red Flags Rule. The template, which is labeled as a "Do-It-Yourself Program for Businesses at Low Risk for Identity Theft," is available at http://ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm. While this template offers a good starting point for drafting a written Identity Theft Program, those subject to the Rule should keep in mind that the creation and implementation of an Identify Theft Prevention Program is unique to each business and requires each creditor and financial institution to consider its own practices in creating the program. The FTC's release of this basic template with general headings that requires the user to fill in various fields with answers appropriate to the specific business at issue demonstrates how serious the FTC considers this new rule. Instead of supplying businesses with a model identity theft prevention program, the FTC has merely provided a structured way for creditors and financial institutions to assess and develop the most appropriate program for their businesses.

Finally, the Red Flags Rule requires periodic updates to the program to ensure that it keeps current with identity theft risks. In determining how often such updates should occur, those subject to the Rule should consider changes in technology; new methods to detect, prevent, and mitigate identity theft; changes in the business; and changes in how identity thieves operate.

Administering the Program

The initial written program must get the approval of the appropriate board or managing committee within the business. That governing body or individual must oversee, develop, implement, and administer the program. Responsibilities include assigning specific responsibility for the program's implementation, reviewing staff reports about how the organization is complying with the Rule, and approving important changes to the program. Training of staff is also important as employees at almost every level can play an important role in identity theft deterrence and detection.

Conclusion

However helpful, the guidelines set forth above are only a start. Undoubtedly, it will be some time before either the agencies or the businesses have a solid sense of what constitutes a strong, yet workable theft prevention program. In all likelihood, that understanding will be the product of both consensus and contention. A good faith effort to comply with the Red Flag Rules is an essential start for any business that falls within the definition of "financial institution" or "creditor." With respect to lawyers and law firms, we should pay close attention to the progress of the lawsuit brought by the ABA against the FTC on this issue and any legislative exemption from the Rule. **CL**

Attorney Jennifer R. Rossi leads the Consumer Financial Services Team at regional law firm, Robinson & Cole LLP. Attorney Kori Termine Wisneski is a member of the Consumer Financial Services Team. For more information, please contact Ms. Rossi at jrossi@rc.com or Mrs. Wisneski at kwisneski@rc.com or call 860-275-8200.

Notes

1. In light of this definition, a law firm would not likely ever be considered a "financial institution" under any conceivable analysis.
2. *See e.g.*, *Riethman v. Berry*, 287 F.3d 274 (3d Cir. 2002).
3. The *Riethman* case was addressed in a letter dated February 4, 2009 from the Acting Director of Bureau of Consumer Protection at the FTC to the American Medical Association in which the FTC responded to an inquiry from the AMA on the applicability of the Identity Theft Red Flags Rule to physicians and related health care providers. In that letter, the FTC considered the AMA's position that physicians are not creditors in light of the finding in *Riethman v. Berry*, that a law firm was not an ECOA creditor. In response, the FTC stated "… the Riethman court did not cite or refer to the Official Staff Commentary of Regulation B. This omission is significant because, . . . this Official Commentary explicitly includes lawyers and physicians within the definition of incidental creditor for purposes of the ECOA, and these conclusions should be granted substantial deference." To view the full content of the February 4, 2009 letter referenced in this footnote, visit http://www2.ftc.gov/bcp/edu/microsites/redflagsrule/more-about-red-flags.shtm.
4. In the February 4, 2009 FTC letter referenced in footnote 3, among other things, the FTC stated, "…we believe that the plain language and purpose of the Rule dictate that health care professionals are covered by the Rule when they regularly defer payment for goods or services."