THE FTC RAISES THE RED FLAG ON IDENTITY THEFT:

THERE'S STILL TIME FOR BUSINESSES TO GET WITH THE "PROGRAM"

By Elan Mizrahi, Esq. and Christopher R. Stovall, Esq.

Jennings, Haug & Cunningham, L.L.P.

Unfortunately in modern free market economies, the very tools which facilitate commerce and promote business—credit cards and credit accounts, payments by mail, electronic transfers, online payment systems, and the like—also create fraud opportunities for the criminally-inclined. The Federal Trade Commission ("FTC") reports that identity theft, in which a person uses another person's identifying information (personal and financial data) without authority to commit a fraud (such as purchasing items on a stolen credit account), now annually claims as many as nine million Americans as its victims.[1] A 2006 Council of Better Business Bureaus study found that consumers and businesses together lost a total of $56.6 billion in 2005 as a result of identity theft.[2] Identity theft is a costly epidemic.

Congress focused on this epidemic in 2003, passing the Fair and Accurate Credit Transaction of 2003 ("FACTA"), Pub. L. 108-159, as an amendment to the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA"). Under new authority granted by FACTA, the FTC and other federal agencies have been working for several years on a series of new regulations to combat identity theft and related problems. On June 1, 2010, a major new development will arrive in the fight against identity theft, as enforcement of the Red Flags Rule, first promulgated in 2007 as part of the FACTA legislation, will begin.[3] The Red Flags Rule, to be located at 16 C.F.R. § 681.2 (referenced in this article as "the Red Flags Rule" or "the Rule"),[4] is premised on the notion that the best defense is a good offense. It requires regulated persons, businesses and organizations to take proactive steps to prevent identity theft from occurring in or through their operations, by adopting written policies identifying and addressing "Red Flags" of identity theft: patterns, practices, or specific activities that indicate the possible existence of identity theft. *See* 16 CFR § 681.2(b)(9). Since other laws already require businesses to safeguard personal information, the Red Flags Rule's purpose is to approach identity theft from the other side—preventing identity theft after personal information is misappropriated.

---

[1] Federal Trade Commission, FIGHTING FRAUD WITH THE RED FLAGS RULE: A How-To Guide for Business 3 (2008) ("*Fighting Fraud*"). As the guide to the Red Flags Rule published by the agency which promulgated the Rule, *Fighting Fraud* is especially important in interpreting and applying the Rule and is cited regularly throughout this article. "[A]n agency's interpretation of its own regulations is entitled to substantial deference and will be accepted unless it is plainly erroneous or inconsistent with the regulation." *Gose v. U.S. Postal Service*, 451 F.3d 831, 836 (Fed. Cir. 2006), quoting *Lacavera v. Dudas*, 441 F.3d 1380, 1383 (Fed.Cir.2006).

[2] Press Release, Council of Better Business Bureaus/Javelin Strategy & Research, New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think (January 31, 2006), *available at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp.

[3] After several prior deferrals, the FTC most recently had intended to begin enforcement of the Red Flags Rule on June 1, 2010. At the request of lawmakers, the FTC has now deferred enforcement through December 31, 2010, while further legislative clarifications are considered. Press Release, Federal Trade Commission, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (May 28, 2010), *available at* http://www.ftc.gov/opa/2010/05/redflags.shtm.

[4] Unless otherwise noted, all Code of Federal Regulations ("CFR") references in this article are to the provisions as they will be numbered as of their currently-scheduled effective date of August 1, 2009, as promulgated by the FTC at 72 Fed. Reg. 63,772-63,774 (November 9, 2007).

Because the Red Flags Rule potentially applies to a universe of businesses besides obvious targets of identity thieves like financial institutions and credit card companies, all American businesses must understand the Rule, determine whether they are subject to it, and comply with it if necessary.[5] Compliance with the Rule involves fairly practical steps that would benefit a wide array of businesses, even those not technically obligated to follow it.

Who must comply with the Red Flags Rule?

The Red Flags Rule requires any "creditor" maintaining one or more "covered accounts" to "develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account." 16 CFR § 681.2(d). A creditor's administration of its Identity Theft Prevention Program in compliance with the Rule will involve proper adoption of the Program, and effective enforcement, training and supervision:

> Your board of directors (or a committee of the board) has to approve your first written Program. If you don't have a board, approval is up to an appropriate senior-level employee. Your Program must state who's responsible for implementing and administering it effectively. Because your employees have a role to play in preventing and detecting identity theft, your Program also must include appropriate staff training. If you outsource or subcontract parts of your operations that would be covered by the Rule, your Program also must address how you'll monitor your contractors' compliance.[6]

With any statute or regulation, the devil in the details often hides in the definitions, and the Red Flags Rule is no exception.

The Rule defines a "creditor" as having "the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies." 16 CFR § 681.2(b)(5). These listed examples do not adequately illustrate the breadth of the definition, because 15 U.S.C. 1681a(r)(5) incorporates the meaning of "creditor" found in the Equal Credit Opportunity Act, 15 U.S.C.A. § 1691a. There, "creditor" means "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C.A. § 1691a(e).

Since any person or business that extends "credit" falls within this very broad definition, the obvious question is what exactly constitutes "credit"? Here again, the Rule borrows from existing federal law: "Credit has the same meaning as in 15 U.S.C. 1681a(r)(5)." 16 CFR § 681.2(b)(4). Again, the incorporated statute itself incorporates the meaning of "credit" found in 15 U.S.C.A. § 1691a, where "credit" means "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." 15 U.S.C.A. § 1691a(d).

---

[5] The requirements of the Red Flags Rule apply equally to "financial institutions" and "creditors" as those terms are defined in the regulation. The Red Flags Rule defines a "financial institution" as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in section 461(b) of Title 12) belonging to a consumer." 16 CFR § 681.2(b)(7) (incorporating definition found at 15 U.S.C. 1681a(t)). This article primarily analyzes the Rule's impact on "creditors," as that term encompasses a much broader array of businesses, many of which are far less accustomed to detecting and addressing identity theft in their regular practices than financial institutions.

[6] *Fighting Fraud* at 4-5. These requirements are found at 16 CFR § 681.2(e).

Basically, anyone who sells property or services without a contemporaneous payment could be a "creditor." Virtually every business aside from pure point-of-sale retailers falls within this definition. The definition appears to exclude retailers who merely accept as payment credit that is "extended, renewed or continued" by third parties, *e.g.*, businesses which allow payment with third-party credit cards. However, the Rule's definitions of "account" and "covered account" clarify this point, specifying that a "covered account" is one the *creditor* offers or maintains that is itself a "continuing relationship" between the customer/debtor and the creditor allowing purchases paid for in installments and over time.[7]

The Rule defines as "account" as follows:

> [A] continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes: (i) An extension of credit, such as the purchase of property or services involving a deferred payment; and (ii) A deposit account."

16 CFR § 681.2(b)(1).

The Rule further defines a "covered account" as:

> (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
>
> (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

16 CFR § 681.2(b)(3).

From these definitions of "account" and the more specific "covered account," one very important point emerges clearly. Although the FCRA is generally considered a *consumer* credit statute, the Red Flags Rule itself clearly also applies to credit accounts extended to *businesses*, for purchases of goods or services *for business purposes*. If our nation's recent recessionary challenges have demonstrated anything, it is that the extension of credit is a primary lubricant necessary to keep the engine of American commerce running smoothly, one without which the entire business-to-business segment of our economy will quickly burn up and seize. Retailers buying inventory for their stores, contractors buying materials for their jobs, auto dealers buying cars for their lots—the examples in which businesses utilize credit (both short term and long) to facilitate both their buying and their selling are too numerous to even begin to catalog.

The breadth (and perhaps overbreadth) of the Rule has compelled much debate over whether the Rule is, in most applications, a remedy without a problem. The debate has delayed enforcement of the Rule since 2007, and has even spawned a preemptive legal challenge. The American Bar Association filed a lawsuit in August 2009 seeking to establish that law firms, where identity theft is largely nonexistent, should be excluded

[7] This conclusion is confirmed in the FTC's guide to the Rule: "Simply accepting credit cards as a form of payment does not make you a 'creditor' under the Red Flags Rule. But if a company offers its own credit card, arranges credit for its customers, or extends credit by selling customers goods or services now and billing them later, it is a 'creditor' under the law." *Fighting Fraud* at 10.

from the Rule, and asserting that the reach of the Rule exceeds the FTC's delegated powers.[8] On October 29, 2009, the U.S. District Court for the District of Columbia granted the ABA's motion for summary judgment, enjoining the FTC's application of the Red Flags Rule to law firms.[9] The FTC has appealed the ruling and briefing in the appeal is ongoing.[10]

Just as the Rule was finally to take effect on November 1, 2009, however, the debate spurred a drive for legislative relief in the form of exemptions for certain small businesses with little or no risk of customer identity theft.[11] On October 20, 2009, the U. S. House of Representatives voted unanimously in favor of H.R. 3763,[12] a bill that would exclude from the meaning of "creditor" under the Red Flags Rule any health care practice, accounting practice, or legal practice with 20 or fewer employees. The bill would also exclude any other business which the FTC determines: (1) knows all its customers or clients individually; (2) only performs services in or around the residences of its customers; or (3) has not experienced incidents of identity theft, and is of a type for which identity theft is rare. The Senate must still pass the legislation and President Obama must sign it before these exemptions become available.[13]

Unless and until such legislation becomes law or the FTC provides further clarifying guidance on the scope of the Rule, the necessity and pervasiveness of business credit counsels that only creditors in rare and unique situations—those indisputably insulated from any "reasonably foreseeable risk to customers … from identity theft" related to credit accounts—can safely afford to read themselves out of this Rule. Be cautioned, however: the FTC considers this analysis entirely fact specific, requiring evaluation creditor by creditor, account by account, rather than permitting the broad categorizing of types of creditors. "The determination of whether your business or organization is covered by the Red Flags Rule isn't based on your industry or sector, but rather on whether your activities fall within the relevant definitions."[14]

---

[8] Press Release, American Bar Association, Federal Trade Commission's "Red Flags Rule" Leads American Bar Association to File Suit: Rule Burdens Lawyers with No Client Benefit and Invades State Regulation of Lawyers (Aug. 27, 2009), *available at* http://www.abanet.org/abanet/media/release/news_release.cfm?releaseid=755.

[9] Statement, American Bar Association, Statement of ABA President Carolyn B. Lamm in American Bar Association vs. Federal Trade Commission: ABA Applauds Injunction, Summary Judgment in Red Flags Suit (Oct. 29, 2009), *available at* http://www.abanet.org/abanet/media/statement/statement.cfm?releaseid=810.

[10] See http://www.abanet.org/poladv/priorities/redflagrule/2010jul22_briefingschedule.pdf.

[11] As noted above, *supra* at n. 3, the legislative activity just before the deadline resulted in the deadline being moved again, to June 1, 2010.

[12] The text of this legislation and its progress can be viewed at http://www.govtrack.us/congress/bill.xpd?bill=h111-3763.

[13] Even the enactment of these exemptions may not halt the ABA's legal challenge to the Rule, however. The ABA's statement on the passage of the House bill calls it "an important recognition that the Federal Trade Commission's interpretation of the Red Flags Rule over-reaches and its application to lawyers is unnecessary," but declares that "more work remains," as the bill is "incomplete and would burden large segments of the public and the FTC with unwarranted bureaucratic procedures." Press Release, American Bar Association, Statement of ABA President Carolyn B. Lamm on House Passage of H.R. 3763, Regarding The FTC "Red Flags Rule" (Oct. 21, 2009), *available at* http://www.abanet.org/abanet/media/statement/statement.cfm?releaseid=802.

[14] *Fighting Fraud* at 9.

At a bare minimum, the Red Flags Rule requires ***any*** "creditor" to periodically review its operations to assess whether the Rule applies to it:

> *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration: (1) The methods it provides to open its accounts; (2) The methods it provides to access its accounts; and (3) Its previous experiences with identity theft.

16 CFR § 681.2(c).

What creditor realistically prefers to gamble with whether the customer credit accounts it maintains carry a "reasonably foreseeable risk" to its customers of suffering identity theft, and not comply with the Rule? Indeed, the FTC's guide to the Rule suggests that even businesses that don't see themselves as subject to much risk of identity theft should adopt a minimal Identity Theft Prevention Program rather than none at all:

> If identity theft isn't a big risk in your business, complying with the Rule should be simple and straightforward, with only a few red flags. For example, where the risk of identity theft is low, your Program might focus on how to respond if you are notified – say, by a consumer or a law enforcement officer – that the person's identity was misused at your business. The Guidelines to the Rule have examples of possible responses. But even a low-risk business needs to have a written Program that is approved either by its board of directors or an appropriate senior employee.[15]

Once a creditor determines that it falls within the incredibly broad scope of the Red Flags Rule, or decides to err on the side of caution, the steps to preparing and implementing the required Identity Theft Prevention Program ("Program") are relatively straightforward. Following the text of the Rule itself, the promulgating regulation provides a number of helpful guidelines and examples to assist creditors in the process. *See* 72 Fed. Reg. at 63,773-63,774 (Appendix A, "Guidelines") (guidelines for developing and maintaining compliant Program) (cited as "Guidelines") and at 63,774 (Supplement to Guidelines) (listing examples of red flags to consider including in Program) (cited as "Supplement to Guidelines"). *Note well*: despite their name, the "Guidelines" are not merely suggestions. The Rule itself mandates that each creditor required to implement a Program "must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate." 16 CFR § 681.2(f).

What are the "Red Flags" of identity theft in your business?

The first step in developing a Program is for a creditor to "[i]dentify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program." 16 CFR § 681.2(d)(2)(i). The Red Flags Rule was developed with an eye toward flexibility rather than a "one size fits all" approach. Thus, in light of the fact that many different types and sizes of businesses fall under its provisions, the Rule specifies that "[t]he Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities." 16 CFR § 681.2(d)(1). The FTC's guide to the Rule stresses that, "[w]hile some businesses and organizations may need a comprehensive Program that

[15] *Fighting Fraud* at 12.

addresses a high risk of identity theft in a complex organization, others with a low risk of identity theft could have a more streamlined Program."[16]

The Guidelines advise that creditors should consider several "risk factors" and several "sources" for appropriate Red Flags to identify in their written Programs. The risk factors include: (1) the types of covered accounts the creditor offers or maintains, (2) the methods the creditor provides to open its covered accounts, (3) the methods the creditor provides to access its covered accounts, and (4) the creditor's previous experiences with identity theft. Guidelines, § II(A). Recommended sources for Red Flags include: (1) incidents of identity theft that the creditor has experienced, (2) methods of identity theft that the creditor has identified that reflect changes in identity theft risks, and (3) applicable supervisory guidance. Guidelines, § II(B).

The Supplement to the Guidelines provides 26 examples of Red Flags that a creditor should consider identifying in its written Program, to the extent the examples are appropriate to the creditor's specific context. The examples are meant to be illustrative rather than exhaustive, and are grouped in five categories:

- Alerts, Notifications or Warnings from a Consumer Reporting Agency
- Suspicious Documents
- Suspicious Personal Identifying Information
- Unusual Use of, or Suspicious Activity Related to, the Covered Account
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

Supplement to Guidelines, generally.

How will your business detect those "Red Flags"?

Once the creditor has identified the appropriate Red Flags for its situation, its Program must establish policies and procedures by which it will "[d]etect Red Flags that have been incorporated into [its] Program." 16 CFR § 681.2(d)(2)(ii). The Guidelines encourage adoption of policies that require the following when dealing with "covered accounts":

> (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and
>
> (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

Guidelines, § III.

What will your business do when it detects a "Red Flag"?

A compliant Program will specify how the creditor will "[r]espond appropriately to any Red Flags that are detected … to prevent and mitigate identity theft." 16 CFR § 681.2(d)(2)(iii). On this point, the Guidelines

[16] *Fighting Fraud* at 5.

provide detailed guidance for creditors to consider in adopting measures appropriate to their unique risks and aggravating factors. Suggested responses to the detection of Red Flags include:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

Guidelines, § IV.

How will your business keep its "Red Flags" program up-to-date?

The final requirement of an acceptable Program is that it contain provisions to "[e]nsure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft." 16 CFR § 681.2(d)(2)(iv). Upon consultation with the Guidelines as mandated by the Rule, creditors will find a list of suggested criteria to use in conducting this periodic review and update of their Programs:

(a) The experiences of the … creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the … creditor offers or maintains; and

(e) Changes in the business arrangements of the … creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Guidelines, § V.

What are the sanctions for noncompliance with the Red Flags Rule?

According to the Frequently Asked Questions[17] section of the FTC's website to help covered entities design and implement identity theft prevention programs, there is no private right of action under the Red Flags Rule. However, consumers can file a complaint with the FTC about a company's Program and the FTC intends to use such complaints filed at www.ftc.gov to target its law enforcement efforts.

[17] The Red Flags Rule: Frequently Asked Questions, Section E, "Red Flags Rule Compliance and Enforcement," *available at* http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm#E.

Only certain federal and state government agencies have jurisdiction to enforce the Rule, but they have a variety of penalties and remedies at their disposal to ensure compliance. The FTC can seek both monetary civil penalties and injunctive relief for violations, generally in a federal lawsuit in which the U.S. Department of Justice represents the FTC. Currently, the law sets $3,500 as the maximum civil penalty per violation, but each instance in which the company has violated the Rule counts as a separate violation. Enforcing agencies can also seek injunctive relief, ordering a noncompliant company to comply with the law in the future on pain of contempt of court (which would entail further penalties and injunctive relief), and requiring the company to provide reports, retain documents, and take other steps to ensure compliance with both the Rule and the court order.

Conclusion

It is hardly debatable that identity theft is an epidemic. What is highly debatable is whether the Red Flags Rule is a proper cure, or an overbroad and burdensome edict with unintended consequences. While the debate continues, it is nevertheless imperative for every business to evaluate the Rule's applicability and, if necessary, implement a compliant Program to avoid sanctions.