"RED FLAG" IDENTITY THEFT RULES MAY HAVE YOU SEEING RED: FTC EXTENDS COMPLIANCE DEADLINE BECAUSE MANY COMPANIES DID NOT KNOW THAT THESE RULES APPLY TO THEM

When companies outside the financial industry hear terms like "FACT Act,"[1] "FCRA,"[2] or "Identity Theft Red Flags," many understandably tune out, concluding that any associated regulations are inapplicable to them. However, the "Red Flag rules" recently adopted under the FACT Act can apply to *any company* that "provides a product or service for which the consumer pays after delivery."[3] *Given this extremely broad scope, the Red Flag rules will apply to a wide range of companies outside the financial arena, including telecommunications companies, cable operators, mobile telephone service providers, automobile dealers, franchisors, merchants, hospitals, and utility companies, among others.*

Under the key provisions of these rules, covered entities, including both "financial institutions" and "creditors," must implement a written program approved by their board of directors to detect, prevent, and mitigate identity theft ("Program"). This Program must be designed to identify and address so-called "Red Flags" that signal the possibility of an instance of identity theft. The requirements of the Red Flag rules are set forth in more detail below.

In light of the expansive coverage of the new Red Flag rules and the potentially significant enforcement penalties associated with noncompliance, *companies across all industries* should assess whether they qualify as a "covered entity" under the Red Flag rules and offer or maintain "covered accounts," in which case they are required to implement an identity theft prevention Program consistent with the FACT Act's requirements.

Deadline Extended. The new Red Flag rules went into effect on January 1, 2008, and require full compliance by November 1, 2008.[4] The Federal Trade Commission ("FTC"), however, recently suspended enforcement of the new rules until May 1, 2009 for nonfinancial companies.[5] The FTC has authority over enforcement of the Red Flag rules for most entities that fall under the "creditor" prong of the rules, and that is where there has been the most confusion over

---

1 *See* Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") (Public Law 108-159), 15 U.S.C. § 1681 *et seq.*

2 *See* Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*

3 *See* FTC Notice: Commission Determination to Forbear from Bringing Enforcement Actions against Certain Financial Institutions and Creditors until May 1, 2009 (*available at* http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf).

4 72 Fed. Reg. 63718. The text of the rules is available at www.occ.treas.gov/fr/fedregister/72fr63718.pdf.

5 The FTC extension of the compliance deadline applies only to companies outside the supervision of the federal bank regulatory agencies. For financial entities governed by the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, or the Office of Thrift Supervision, the November 1 deadline remains effective. *See* FTC Notice, *supra*. Hereinafter, these financial agencies and the FTC are referred to collectively as the "Agencies."

whether the Red Flag rules apply to a particular business.[6] The FTC believes that delaying its enforcement of the Red Flag rules by six months will allow nonfinancial entities -- which may not have even realized that they were covered by the rules -- to take the appropriate care and consideration in developing and implementing their required Programs.

Enforcement and Penalties. The Red Flag rules empower federal authorities to impose civil penalties against companies without adequate identity theft Programs in amounts up to $2,500 *per knowing violation*.[7] While the FTC has not elaborated on its method of calculating penalties, it is possible that the fine amount chosen could be assessed against a noncompliant company for *each* covered account it maintains. Companies with a significant number of accounts, therefore, could face significant civil penalties if they do not have an adequate Program. Although it lacks the authority to initiate random audits, the FTC has indicated that it might investigate a company's compliance based on consumer complaints or outside tips, or on other sources of industry information.[8]

1. Entities and Accounts Covered by the New Rules

1.1. *Covered Entities*

Under the FACT Act, "financial institutions" and "creditors" must comply with the new Red Flag rules. A "financial institution" is defined to include all banks, savings and loan associations, mutual savings banks, credit unions, and any other person that holds, directly or indirectly, a consumer "transaction account," such as a checking account, demand deposit, negotiable order of withdrawal account, savings deposit subject to automatic transfers, or share draft account. "Creditor" is defined broadly and includes (a) any entity that regularly extends, renews, or continues credit; (b) any entity that regularly arranges for the extension, renewal, or continuation of credit; or (c) any assignee of an original creditor that is involved in the decision to extend, renew, or continue credit.

Thus, as noted, the new Red Flag rules apply far beyond the financial industry, covering a wide variety of entities and industries that offer customers the ability to pay for goods or services *after* receipt of such goods or services.[9] The new rules explicitly include entities such as telecommunications companies, utility companies, and automobile dealers.[10]

---

6 *See* BNA Privacy & Security Law Report: *Identity Theft: FTC Won't Enforce Red Flags Until May '09; Banks Still Must Comply With Rules by Nov. 1*, 7 PVLR 1533 (October 2008).

7 *See* FCRA, § 621(a)(2)(A), 15 U.S.C. § 1681s. State authorities may also initiate enforcement proceedings if no federal action is pending; maximum fines in state proceedings are $1,000 for each willful or negligent violation. *See* FCRA, § 621(c).

8 Teleconference with Pavneet Singh, attorney in the FTC's Division of Privacy and Identity Protection, October 30, 2008.

9 *See* FTC Notice, *supra*. *See also* FTC Business Alert, "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft" (*available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm).

10 72 Fed. Reg. 63772 (Nov. 9, 2007).

1.2. *Covered Accounts*

Financial institutions and creditors that are subject to the new rules must develop and implement a written Program for all of their "covered accounts." A "covered account" is (a) a consumer account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions (*e.g.*, a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account); or (b) any other account 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.

The second prong is intended to cover certain *business* accounts; however, the risk-based nature of this prong allows each financial institution or creditor flexibility in determining which business accounts will be covered by its Program through a risk evaluation process. The Program must be designed to detect, prevent, and mitigate identity theft in connection with both (a) the opening of *new* covered accounts and (b) *existing* covered accounts.

The Agencies also recognized that a person may establish a relationship with a creditor, such as an automobile dealer or a telecommunications provider, primarily to obtain a product or service that is *not* financial in nature. To make clear that an "account" includes relationships with *creditors* that are *not* financial institutions, the definition is purposefully not tied to the provision of "financial" products and services.[11]

2. Key Definitions and Specific Program Requirements

The Program must contain "reasonable policies and procedures" to (a) identify relevant "Red Flags" for covered accounts and incorporate those Red Flags into the Program; (b) detect when the selected Red Flags are triggered; (c) respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and (d) ensure that the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.[12] Each of these four components and additional Program definitions are discussed below.

2.1. *Definitions*

"Red Flag" is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft."[13] "Identity theft" means "a fraud committed or attempted using the identifying information of another person without authority." "Identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any — (a) Name, social security number, date of birth,

[11] 72 Fed. Reg. 63718-25.

[12] 72 Fed. Reg. 63724.

[13] 72 Fed. Reg. 63723.

official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (b) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (c) Unique electronic identification number, address, or routing code; or (d) Telecommunication identifying information or access device (as defined in 18 U.S.C. § 1029(e))."

2.2. *Identifying Possible Red Flags*

The Agencies decided not to single out any specific Red Flags as mandatory for all financial institutions and creditors to address. Rather, the Agencies recognized that the final rules and guidelines cover a wide variety of entities that offer and maintain many different products and services, and must have the flexibility to be able to adapt to rapidly changing risks of identity theft. Therefore, the Red Flag rules contain a list of factors that a financial institution or creditor "should consider . . . as appropriate" in identifying relevant Red Flags. These factors include (a) the types of covered accounts it offers or maintains; (b) the methods it provides to open its covered accounts; (c) the methods it provides to access its covered accounts; and (d) its previous experiences with identity theft.[14]

A financial institution or creditor will not need to justify to an Agency its failure to include in the Program a specific Red Flag from the list of examples. However, a covered entity will have to account for the overall effectiveness of a Program, and that Program must be appropriate both as to its size and complexity and as to the nature and scope of its activities.[15]

2.3. *Detecting Red Flags*

A Program must contain policies and procedures to detect the Red Flags that a financial institution or creditor has incorporated into its Program. Notably, the Program's policies and procedures should address the detection of Red Flags in connection with (a) the *opening* of covered accounts, such as by obtaining identifying information about, and verifying the identity of, a person opening a covered account; and (b) *existing* covered accounts, such as by authenticating customers, monitoring transactions, and verifying the validity of change of address requests.[16]

2.4. *Responding to Red Flags*

The Program's policies and procedures should provide for appropriate responses to any detected Red Flags that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that might heighten the risk of identity theft, such as a data security incident that resulted in the

[14] 72 Fed. Reg. 63726-27, 63732, 63766 (OTS rules).

[15] 72 Fed. Reg. 63726-27, 63732, 63766-67 (OTS rules).

[16] 72 Fed. Reg. 63727-28.

unauthorized access to or loss of a customer's account records held by the financial institution or creditor, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor, or to a fraudulent website.

Appropriate responses may include, for example: (a) monitoring a covered account for evidence of identity theft; (b) contacting and notifying 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.[17]

2.5. *Updating the Program*

The Red Flag rules require "periodic" updating because the Agencies concluded that requiring financial institutions and creditors to "immediately and continuously" update their Programs would be overly burdensome. Factors that should cause a financial institution or creditor to update its Program include (a) its own experiences 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 it offers or maintains; and (e) changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.[18]

2.6. *Administering the Program*

(a) The Program must be approved by an institution's board of directors or a committee of the board. (*Note*: The board or an appropriate committee must approve only the *initial* written Program; thereafter, the board, a committee, or senior management may *update* the Program.)

(b) The board, an appropriate committee, or a designated senior management employee must be involved in the development, implementation, administration, and oversight of the Program.

(c) Those responsible for the Program should provide to the board or senior management a report (at least annually) that does the following: (1) shows the effectiveness of the Program in addressing the risk of identity theft in connection with new and existing covered accounts; (2) explains any "significant events" involving identity theft that have occurred and the management's response to them; (3) addresses service provider arrangements; and (4) provides recommendations for material changes to the Program based upon evolving risks and methods of identity theft.

---

[17] 72 Fed. Reg. 63728-29.

[18] 72 Fed. Reg. 63729-30.

(d) A covered entity must train "relevant staff" to effectively implement the Program. Staff members who have already been trained as a part of the antifraud prevention efforts of the financial institution or creditor do not need to be retrained except "as necessary."

(e) Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor must take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider, by contract, to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or take appropriate steps to prevent or mitigate identity theft.[19] These service provider provisions impose potentially unforeseen, but significant, burdens on companies. Notably, a business or organization that is not *itself* a covered entity but which serves as a service provider to a covered entity may still be required, via contract, to comply with these new rules if it has access to covered accounts in its role as a service provider.

3. Conclusion

Companies across all industries -- not just financial institutions -- must assess whether they fall under the Red Flag rules' very broad "creditor" definition and provide or maintain "covered accounts" and therefore must establish an identity theft prevention Program by the FTC's new May 1, 2009 deadline. In addition, service providers that are not themselves covered entities may nonetheless be indirectly subject to these rules through their contracts with covered entities.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Francis M. Buono (202-303-1104, fbuono@willkie.com), McLean Sieverding (202-303-1163, msieverding@willkie.com), Brien Bell (202-303-1164, bbell@willkie.com), or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, N.Y. 10019-6099 and has an office located at 1875 K Street, N.W., Washington, D.C. 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, D.C. telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

November 7, 2008

[19] 72 Fed. Reg. 63730-32.