JONES DAY

NOVEMBER 2008

RED FLAG RULES REQUIRE COMPANIES TO TAKE IDENTITY THEFT SERIOUSLY

You may be surprised to learn that your business must comply with the new identity theft Red Flag Rules. Not only are credit card companies and financial institutions subject to these rules, but any company that regularly extends or merely arranges for the extension of credit is also subject to them. Thus, finance companies, mortgage brokers, automobile dealers, telecommunications companies, and utility companies, among others, will have to comply with the Red Flag Rules. If your company extends or arranges for the extension of credit, the Red Flag Rules require you to have an identity theft prevention program.

BACKGROUND

On December 4, 2003, the President signed into law the Fair and Accurate Credit Transactions Act ("FACTA"). FACTA was enacted by Congress to provide consumers with increased protection from identity theft. The regulations directed six agencies to jointly "establish and maintain guidelines . . . [that] identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft."[1] Accordingly, the six agencies published the final regulations on November 9, 2007, and those regulations became effective January 1, 2008,[2] with a mandatory compliance date of November 1, 2008.[3]

On October 22, 2008, one of the six agencies, the Federal Trade Commission ("FTC"), announced that it will suspend enforcement of the Red Flag Rules until May 1, 2009, to give creditors and financial institutions additional time in which to develop and implement written identity theft prevention programs. The FTC's delay in enforcement, however, does not affect the other federal agencies' enforcement of the original November 1, 2008, compliance deadline for financial institutions subject to their oversight. But for most creditors, the FTC's delay in enforcement will give them much-needed time to become compliant with the Red Flag Rules.

The final regulations contain three parts. First, they require covered entities to create a written identity theft program designed to detect, prevent, and

mitigate identity theft in connection with certain covered accounts (the "Red Flag Rules" or the "Rules"). Second, the regulations require users of consumer reports to adopt policies for verifying identity when they receive a notice of address discrepancy from a consumer reporting agency. Third, the regulations impose requirements on debit and credit card issuers to implement procedures to assess the validity of address changes under certain circumstances. This *Commentary* focuses on only the Red Flag Rules portion of the regulations.

COVERED ENTITIES

The Red Flag Rules cover financial institutions and creditors that offer or maintain covered accounts. The breadth of the Rules comes from the broad definition of "creditors." The term "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."[4] Consequently, many entities involved in the process of extending or maintaining credit must comply with the Red Flag Rules despite the fact that they do not extend credit themselves. For example, a retailer that takes applications for a third-party credit card or the car dealer that partners with a local bank branch to facilitate car loans will likely be subject to the Rules. Similarly, where nonprofit and government entities, such as many hospitals, defer payment for goods and services, they too will be considered creditors.

In addition to creditors, financial institutions are also required to comply with the Red Flag Rules. For purposes of the Rules, "financial institution" means a bank, savings and loan association, mutual savings bank, credit union, or any other person who, directly or indirectly, holds a transaction account belonging to a consumer.[5]

Under the Red Flag Rules, only those creditors and financial institutions that offer or maintain covered accounts are required to develop and implement an identity theft prevention program. A "covered account" is "(i) [a]n 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 . . . and (ii) any other account . . . for which there is a reasonably foreseeable risk to customers . . . from identity theft . . . ."[6] Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, and checking and savings accounts. In determining whether the Red Flag Rules apply, a company should consider the types of accounts it offers, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft.[7] Additionally, the company should periodically perform a reassessment of all of its accounts to determine whether they are covered accounts that trigger the application of the Rules.

DESIGNING A PROGRAM

Companies subject to the Red Flag Rules must design 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.[8] The Rules do not specify the contents of the program that must be adopted. An Appendix to the Rules contains Guidelines to assist companies in creating and maintaining their programs. The Rules require that the Guidelines be considered, but companies are free to tailor their programs as they see fit. The Rules give companies a great deal of flexibility, requiring merely that a company design and implement a program that is appropriate to the size and complexity of the company and the nature and scope of its activities.

The Red Flag Rules do require identity theft prevention programs to include "reasonable policies and procedures" to identify relevant red flags and incorporate them into the program, to detect those red flags, to respond appropriately when red flags are detected, and to ensure that the program is updated periodically. Each of these elements is discussed below.

Identify Relevant Red Flags. The first step in creating an identity theft prevention program, as required by the Red Flag Rules, is to determine which red flags are relevant to the company and to incorporate those red flags into its

program.[9] "Red flags" are patterns, practices, or specific activities that indicate the possible existence of identity theft in connection with a covered account. The company should examine the covered accounts it currently offers or maintains and identify potential sources of red flags. A Supplement to the Rules sets forth 26 examples of potential red flags. While not all 26 of the example red flags must be incorporated, the company should seriously consider each example and have legitimate reasons for not incorporating any of them in the final written program. The company also should take into account its previous experience with identity theft in determining the appropriate red flags for its program. Red flags may include the following:

- An application that appears to have been forged, altered, or destroyed and reassembled.
- A consumer report that includes a fraud alert, credit freeze, or address discrepancy.
- A change-of-address notice that is followed shortly by a request for a new credit card, bank card, or cell phone.
- A Social Security number supplied by an applicant that is the same as that submitted by another person opening an account.
- An address or telephone number supplied by an applicant that is the same or similar to the account number or telephone number submitted by an unusually large number of other persons.
- Notification of the financial institution or creditor that the customer is not receiving account statements.
- Use of an account that has been inactive for a reasonably lengthy period of time.

Detect Red Flags. The company should implement procedures to detect the identified red flags. The company should be sure to verify the identity of persons opening new covered accounts and should authenticate customers with existing covered accounts.[10] For guidance, the company can refer to the verification procedures set forth in the Customer Identification Program rules that apply to financial institutions.[11]

Establish Response Procedures. The company should develop appropriate policies and procedures to respond to any red flags that are detected. The responses, which should be commensurate with the degree of risk posed, may include monitoring an account, contacting the customer, changing passwords, or notifying law enforcement. In some situations, it may be appropriate to determine that no response is necessary.[12]

Ensure That the Program Is Updated Periodically. It is important for the company to periodically update its program to reflect changes in risks. The company must remain up to date with changes in identity theft, and as necessary, it must incorporate new methods of combating identity theft. Additionally, the company should be aware that risks may change when it alters its business arrangements or modifies the types of accounts it offers.[13]

METHODS FOR ADMINISTERING THE PROGRAM

Approval of the initial written program must be obtained from the company's board of directors or an appropriate committee thereof.[14] Oversight of the implementation and administration of the program must be done by the board, a board committee, or a designated employee at the level of senior management.[15] This oversight also includes reviewing reports and approving material changes to the program.[16] If the company has any arrangements with service providers, it must exercise oversight of those providers.[17] This can be done, for example, by requiring service providers to have their own Red Flag programs or by requiring them to follow the company's program.

CONSEQUENCES OF NONCOMPLIANCE

Failure to comply with the Red Flag Rules can result in various penalties. Consequences may include a civil money penalty for each violation, regulatory enforcement action, and negative publicity.[18] Although the Rules do not allow for any private legal action in the event of a violation,[19] there is the potential for private-plaintiff lawsuits under other laws because a violation of federal rules may itself be a violation of state laws. These state laws may permit actions by consumers or state

attorneys general. In any event, it is likely that, over time, the Red Flag Rules will become a de facto standard of care applied to determine whether a company has negligently allowed a customer's identity to be stolen.

CONCLUSION

In general, the new Red Flag Rules require companies with covered accounts to take reasonable measures to ensure the safety of sensitive consumer information. The Rules are intended to detect, prevent, and mitigate the risk of identity theft, but they do not require companies to adopt any particular policy or procedure. Rather, companies can scale their programs to match the size, complexity, and nature of their businesses. The process a company follows in adopting its identity theft prevention program will go a long way toward establishing that the program is reasonable. At a minimum, the company should be capable of justifying the policies and procedures it adopts by demonstrating that it has seriously considered the pertinent risks and has attempted to minimize them.

LAWYER CONTACT

For further information, please contact your principal Firm representative or the lawyer listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

This Commentary *was prepared with assistance from Corey Dickey, a summer associate in the Columbus Office.*

ENDNOTES

1. 15 U.S.C. § 1681m(e)(1)(A) & (2)(A). The six agencies responsible for issuing the joint guidelines are as follows: (1) the Office of the Comptroller of the Currency, Treasury; (2) the Board of Governors of the Federal Reserve System; (3) the Federal Deposit Insurance Corporation; (4) the Office of Thrift Supervision, Treasury; (5) the National Credit Union Administration; and (6) the Federal Trade Commission.
2. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transaction Act of 2003; Final Rule, 72 Fed. Reg. 63718 (to be codified at 12 C.F.R. pts. 41, 222, 333, 364, 571, and 717 and 16 C.F.R. pt. 681). Note that each of the six agencies will codify the regulations at different parts. For simplicity, all future general references to the regulations will be cited to the Office of the Comptroller of the Currency's codification at pt. 41.
3. *Id.*
4. 15 U.S.C. § 1691a(e).
5. 15 U.S.C. § 1681a(t).
6. 72 Fed. Reg. 63718, 63753–63754 (to be codified at 12 C.F.R. 41.90(b)(3)(i) and (ii)).
7 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(c)(1) through (3)); Appendix J to Part 41 II(a)(1) through (4).
8. 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(d)(1)).
9. 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(d)(2)(i)).
10. Appendix J to Part 41 III(a) and (b).
11. 31 U.S.C. 5318(l) (31 C.F.R. 103.121).
12. Appendix J to Part 41 IV(a), (b), (c), (h), and (i).
13. Appendix J to Part 41 V(d) and (e).
14. 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(e)(1)).
15. 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(e)(2)).
16. Appendix J to Part 41 VI(a)(2) and (3).
17. Appendix J to Part 41 VI(c).
18. Press Release, Reuters, "Compliance Coach Identifies 23 New Identity Theft Red Flags Based on Recent Cases" (May 5, 2008) (http://www.reuters.com/article/pressRelease/idUS97072+05-May-2008+BW20080505) (last visited November 11, 2008).
19. Plaintiffs have attempted to bring private actions under the Fair Credit Reporting Act (15 U.S.C. § 1681m) because of an apparent drafting error in § 1681m(h)(8). Courts have differed on the interpretation of the drafting error. Most recently, the United States Court of Appeals for the Seventh Circuit refused to permit such actions, ruling that the newly added § 1681m(h)(8) was designed to preclude private enforcement of the entirety of § 1681m, not just § 1681m(h). *Perry v. First National Bank*, 459 F.3d 816 (7th Cir. 2006). *But see Barnette v. Brook Road, Inc.*, 429 F. Supp. 2d 741 (E.D. Va. 2006).