Electronic Banking Law & Commerce REPORT

September 2008 ■ Volume 13 ■ Issue 7

Final Federal Rules Require Identity Theft Prevention Programs to Be Implemented in 2008 Part 2

BY JOHN L. NICHOLSON AND MEIGHAN E. O'REARDON

John L. Nicholson is a senior associate in the Global Sourcing group of Pillsbury Winthrop Shaw Pittman LLP. He can be reached at john.nicholson@pillsburylaw.com. Meighan E. O'Reardon is an attorney at the firm.

On November 1, 2008, many businesses will be expected to comply fully with new identity theft rules (the "Red Flag Rules") promulgated by six Federal financial regulators.[1] For background on these rules and requirements, please refer to *Part 1* of this article in the August 2008 issue of *Electronic Banking Law and Commerce Report*.[2] By now, most organizations subject to these requirements are actively developing and implementing their Identity Theft Prevention Programs. As organizations strive to meet the compliance deadlines, the following additional observations about the rules and current implementation efforts have been compiled.

Who Must Comply?

The Identity Theft Red Flag Rules do not apply just to financial organizations traditionally regulated by the Federal government. In fact, because the Federal Trade Commission is one of the six agencies issuing the Red Flag Rules, a broad cross-section of businesses must comply. Organizations subject to the regulations are described as *financial institutions*[3] and *creditors*. These terms include not only banks and credit unions but also organizations such as finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies. Under the

CONTINUED ON PAGE 4

Content HIGHLIGHTS

Complete Table of Contents listed on page 2.

THOMSON WEST

Table of CONTENTS

Electronic Banking Law & Commerce Report
West Legalworks
195 Broadway, 9th Floor
New York, NY 10007

One Year Subscription ■ 10 Issues ■ $490.00
(ISSN#: XXXX)

Please address all editorial, subscription, and other correspondence to the publishers at west.legalworksregistration@thomsonreuters.com

Red Flag Rules, "creditors" include any person/organization who regularly extends, renews or continues credit; any person/organization 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] Any business subject to the Red Flag Rules must develop a compliant Identity Theft Prevention Program ("Program").

Significantly, the Red Flag Rules apply to small merchants as well as large financial institutions. This means that organizations not traditionally regulated by Federal authorities may now be subject to Federal oversight. It is these smaller organizations that will likely face difficulties meeting the November deadline, since they may not have existing compliance programs in place or resources to leverage. Furthermore, in some extreme circumstances, these smaller organizations may not yet be aware that they must comply.

Within each organization, a variety of expertise is necessary to develop a Program. At a minimum, an organization's fraud, risk, information technology, compliance, business and legal functions should be involved. For some smaller organizations, these functions may not be performed by different people. The Federal regulators have acknowledged that implementing successful Programs and maintaining compliance will straddle multiple disciplines. In fact, examiners may even consider the level of cooperation among disciplines in their assessment of Programs.

What Constitutes a Covered Account?

Defining "covered accounts" has been one of the most challenging aspects of implementing the Identity Theft Prevention Programs. According to the Federal regulators, the definition of covered accounts has been a "fairly universal question."[5] Uncertainty exists because the guidance issued along with the Red Flag Rules ultimately leaves it to each institution to define those accounts that should be covered for their organization. According to the Regulation, a covered account includes personal accounts designed to permit multiple payments or transactions (*e.g.*, credit card accounts, mortgages, loans, etc.) and any account for which there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. It is the latter portion of this definition that has caused difficulty.

The Red Flag Rules require a risk assessment from each organization for its accounts, but there is little guidance as to how an organization should ultimately use the results in its determination of which accounts constitute covered accounts.[6] Defining the specific criteria for "covered accounts" should be an interactive process and involve analyzing how accounts are opened, how accounts are accessed, and the types of accounts most susceptible to identity theft. Organizations should be aware that the covered account factors listed in the Red Flag Rules are not exclusive. Perhaps the most important factor listed in the Red Flag Rules is each organization's past experience with identity theft. For example, if a reasonable analysis demonstrates that the potential harm to a customer from identity theft associated with specific business accounts is minimal, that may be a sufficient reason to exclude such accounts from the definition of "covered accounts." An organization making such a determination should confirm that the analysis is supported by the organization's auditors. Any category of accounts that have been subject to identity theft in the past (possibly even at a similar organization) will likely face greater scrutiny from examiners if not classified as covered accounts. Ultimately, the determination of what constitutes a covered account will be unique to each organization.

Enforcement and Liability for Non-Compliance

As of the November 1 deadline, organizations will have had one year to comply with the final Red Flag Rules and, as such, full compliance is expected on that date. However, the regulators have indicated that organizations that have made *reasonable* and *good faith efforts*, but who have failed to complete all required tasks, may receive some leniency. Organizations that have made minimal or no progress will likely face additional scrutiny.

Organizations should expect a graduated enforcement process. In instances where a Program is deficient or little to no progress has been made to comply with the Red Flag Rules, examiners may schedule additional on-site visits or require a rigid timeframe for implementation to be completed. Informal or formal penalties could ensue as a result of further and repeated lapses in compliance.

While sanctions and fines may be rare under the Red Flag Rules, the failure to comply with the Red Flag Rules could result in civil penalties due to certain provisions within the Fair Credit Reporting Act (FCRA).[7] The relevant liability provisions of the FCRA include fines and damages, including punitive damages and attorney's fees, for willful non-compliance or for negligent noncompliance with "any requirement imposed" under the FCRA (which now includes the Identity Theft Prevention Program requirement).[8] Any fines or sanctions that arise under the FCRA may only be enforced by the Federal Trade Commission (FTC) or the other federal financial regulators. This means that a private right of action in the courts has not been provided for anyone harmed by an organization that fails to comply with the Red Flag Rules.

Service Provider Compliance

The Red Flag Rules make special note of activities performed "in connection with one or more covered accounts" that are outsourced to third-party service providers.[9] In such instances, the organization has an obligation to ensure that its service providers are compliant with the Red Flag Rules. As part of current implementation efforts, organizations should review all applicable service provider contracts to determine whether existing contract language acknowledges compliance with this type of Federal requirement or if specific language must be addressed in an amendment. Frequently, service providers will attempt to pass on to their customers the cost of compliance with such new regulations. To the extent the service provider must comply with the Red Flag Rules solely because of the services provided to a specific customer, this is not an unreasonable position. However, where a service provider is required to comply by the nature of the provider's business, it is less reasonable for the service provider's customers to bear the cost of compliance. Such costs are simply additional costs of doing business that the service provider should recover over time in its pricing.

In addition to confirming that a service provider complies with the Red Flag Rules, an organization that is subject to the Red Flag Rules must maintain a copy of each applicable service providers' Program.

Required Activities versus Illustrative Examples

In addition to the final Red Flag Rules, the regulations include supplemental materials in the form of Guidelines and an Appendix. This arrangement has resulted in some confusion. The Guidelines are intended "to assist financial institutions and creditors in the formulation and maintenance of a Program."[10] While not binding, if an organization opts not to follow a particular guideline it must nonetheless have "reasonable policies and procedures to meet the specific requirements of the final rules."[11] Omitting specific guidelines from your Program will likely require some type of justification. The Appendix, unlike the Guidelines, is included merely to illustrate examples of "red flag" activity. Since these are just examples, a decision not to include one of the listed red flag activities in your Program will not require any type of justification.

Some commentators have noted that the interaction of the required activities and the nonbinding examples included with the Red Flag Rules creates a potential obligation to search lists of known criminals as part of the Program requirements.[12] The Red Flag Rules and associated Guidelines include a number of references to certain provisions of the USA Patriot Act. The requirement for the Red Flag Rules in the FACT Act cites these provisions and states that the Red Flag Guidelines must not be inconsistent with certain provisions of the USA Patriot Act requiring verification of the identity of persons opening new accounts.[13] The policies and procedures outlined in the referenced statutes set forth the minimum standards for financial institutions to verify

the identity of customers opening accounts.[14] Significantly, one of these minimum requirements includes "consulting lists of known or suspected terrorist or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list."[15]

This could imply that financial institutions and creditors should include checks of known identity thieves as part of their Program's procedures for opening accounts. Other than the referenced article, little attention has been paid to this reference to the USA Patriot Act. However, at a minimum organizations, particularly more sophisticated banks and financial institutions, should be aware that searching lists of known identity thieves and criminals may be an activity that should be addressed in their Program.

FFIEC Procedures Expected

As part of the evolution of the enforcement of the Red Flag Rules, the Federal Financial Institutions Examination Council[16] (FFIEC) is in the process of establishing the examination procedures for federal examiners who will be reviewing compliance with the Regulations. In an effort to establish consistency, the procedures are expected to be very similar for all entities regardless of which regulator is responsible for evaluating compliance. Currently, the final examination procedures are in the process of being approved by each regulatory agency and will be announced separately by each agency. At the time of this publication, the Department of Treasury, Office of Thrift Supervision (OTS) has released its examination procedures.

The OTS examination procedures, which are likely representative of the final procedures to be released by the other regulators, outline fifteen separate examination steps.[17] The first step in the OTS examination procedures will be a scoping process to assess how each organization's Program is organized. There will be six examination steps focused solely on Red Flag Program compliance that include assessing management oversight, the comprehensiveness of the Program, staff training, vendor management and interaction with findings under other regulations (e.g., the Bank Secrecy Act, Customer Identification Program and Customer Information Security Program). The remaining examination steps involve assessing each organization's compliance with the change of address and address discrepancy rules.

Organizations should watch for the release of their regulator's procedures and use the information provided to identify Program gaps and to understand the examiners' rationale. Federal officials have cautioned that organizations should not stall implementation efforts in anticipation of the procedures. The final examination procedures are expected to be high-level and brief, and will not be a roadmap for compliance.

NOTES

1. The Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Trade Commission and the Department of Treasury's Office of the Comptroller of the Currency and Office of Thrift Supervision.
2. John L. Nicholson and Meighan E. O'Reardon, "Final Federal Rules Require Identity Theft Prevention Programs to be Implemented in 2008: Part 1", *Electronic Banking Law and Commerce Report, Vol. 13, No. 6* (August 2008)
3. Financial institutions can be 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 belonging to a consumer. "Transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts. *See* Identity Theft Red Flags, Subpart J, § .90(b)(7) citing 15 U.S.C. 1681a(t).
4. *See* 15 U.S.C. § 1691(e).
5. Linda McGlasson, "Identity Theft Red Flags Progress Report: How Does Your Institution Stack Up?," BankInfo Security (May 6, 2008) available at www.bankinfosecurity.com/articles.php?art_id_=845 (last accessed June 4, 2008).
6. Identity Theft Red Flags, Subpart J, § .90(c).
7. Section 114 of the Fair and Accurate Credit Transactions (FACT) Act, which calls for the Red Flag Regulations, amends Section 615 of the FCRA. As a

result, the Identity Theft Program is subject to the various provisions of the FCRA.

8. 15 U.S.C. § 1681n(a), § 1681o.
9. Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, Appendix J, § VI(c).
10. Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, Appendix J.
11. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,720 (Nov. 9, 2007).
12. Tim Wilson, "Companies May Be Held Liable for Deals with Terrorists, ID Thieves," Dark Reading (April 23, 2008) available at http://www.darkreading.com/document.asp?doc_id=151872 (last accessed June 4, 2008).
13. The Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 114(3) (2003); 15 U.S.C. § 1681m(e)(3). *See also* Fed. Reg., Vol. 72, No. 217(II)(A)(1) at 63719.
14. 31 U.S.C. § 5318(l).
15. 31 U.S.C. § 5318(l)(2)(c).
16. The FFIEC is a formal interagency body with the power to prescribe uniform principles, standards and report formats for federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. For more information visit www.ffiec.gov (last accessed June 4, 2008).
17. Linda McGlasson, "ID Theft Red Flags Rule Examination Procedures Unveiled, OTS is First Agency to Detail How Examiners Will Measure Compliance After Nov. 1," BankInfoSecurity (August 11, 2008) available at www.bankinfosecurity.com/articles/php?art_id=933.