

**Authors**

**Gregory T. Casamento**  
212-812-8325  
[gcasamento@lockelord.com](mailto:gcasamento@lockelord.com)

**Patrick J. Hatfield**  
404-870-4643  
[phatfield@lockelord.com](mailto:phatfield@lockelord.com)

**Vita E. Zeltser**  
404-870-4666  
[vzeltser@lockelord.com](mailto:vzeltser@lockelord.com)

[www.lockelord.com](http://www.lockelord.com)

This *Client Alert* is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. Readers should obtain legal advice specific to their enterprise and circumstances in connection with each of the topics addressed.

If you would like to be removed from our mailing list, please contact us at either [unsubscribe@lockelord.com](mailto:unsubscribe@lockelord.com) or Locke Lord Bissell & Liddell LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive *Client Alerts*.

Attorney Advertising

© 2009 Locke Lord Bissell & Liddell LLP

## The Red Flags Waive for Thee!

### *Extended Red Flags Rule Compliance Deadline is August 1, 2009*

The Federal Trade Commission (“FTC”) mandatory compliance deadline for the Red Flags Rule (the “Rule”), as most recently extended, is **August 1, 2009**. The extension, announced on the eve of the prior May 1, 2009 compliance date (which itself represented a six-month extension of the original enforcement date), was intended to give more time to entities who are still unaware that they are subject to the Rule another chance to become compliant. In the weeks leading up to the current mandatory compliance date, the FTC has issued additional guidance for compliance for businesses with a low risk of identity theft. The FTC published a Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft, which can be found at the FTC website, providing guidance for businesses in which employees know the customers personally, provide services at customers’ homes, have never experienced identity theft, or businesses that are in a line of work where identity theft is uncommon. The FTC has also published articles geared toward healthcare providers, franchisors, telecom and utility companies, and companies offering services in and around the home. All of these can also be found on the FTC website.

The following provides an overview of the Rule and a brief test to determine if a company is within the Rule’s scope, a detailed analysis regarding applicability, and an overview of compliance requirements. Companies subject to the Rule must take action at the board of directors level prior to August 1, 2009.

Companies across all industries should carefully examine the Rule because of the surprising breadth of the Rule’s scope. The FTC’s second extension of the mandatory enforcement deadline demonstrates the FTC’s belief that many were still unaware that they are covered by the Rule.

### Overview

#### Red Flags Rule

To detect, prevent, and mitigate identity theft, the FTC issued the Rule requiring financial institutions and creditors to establish identity theft prevention programs. This Rule stems from Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”), which was added to the Fair Credit Reporting Act (“FCRA”) as Section 615(e) (codified as 15 USC

1681m(e)). The definitions of financial institutions and creditors are surprisingly broad. Companies who may not view themselves as financial institutions or creditors within the general meaning of those terms may nonetheless be subject to the Rule.

Generally, entities subject to the Rule are required to adopt a written program to designate a senior management-level employee to administer the program, to train staff to comply with the terms of the program, and to report, at least annually, to the board of directors regarding compliance with the program. The Rule specifies what the program should address. Further, the program must be adopted by a company’s board of directors, a committee of the board, or a designated senior management-level person if the company does not have a board of directors.

### Test for Compliance With Red Flags Rule

To determine whether a company is subject to the Rule, we offer the following guide:

1. Are you subject to the FTC’s enforcement authority?

If Yes, proceed to #2; if No, you are not within the scope of the Rule.

2. Are you either:

- a. A “financial institution,” which means 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 § 461 (b) of title 12) 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.

or

- b. A “creditor” which is “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. § 1691a(e)), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies. (16 C.F.R. § 681.2(b)(5)).

If you are either a “financial institution” or a “creditor”, proceed to #3; if you are neither, you are not within the scope of the Rule.

- 3. Do you have a “covered account,” which is an account a financial institution or creditor offers or maintains primarily for personal, family, or household purpose, that involves or is designated to permit multiple payments or transactions (such as a loan or utility account), and 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 creditors from identity theft, including financial, operational, compliance, reputation, or litigation risk. (16 C.F.R. § 681.2(b)(3))

If you are either a “financial institution” or a “creditor” and you have one or more “covered accounts, you are within the scope of the Rule.

### Applicability of Red Flags Rule

#### FCRA Requirements

Generally, FCRA requires certain entities to implement identity theft prevention programs covering accounts susceptible to identity theft. Section 615(e)(1) of FCRA (codified as 15 U.S.C. § 1681m(e)), as amended by FACT Act, states:

The Federal banking agencies, the National Credit Union Administration, and the [Federal Trade] Commission shall jointly, with respect to the entities that are subject to their respective enforcement authority under section [§ 621 of FCRA (codified as 15 U.S.C. § 1681s)] of this title—

- (A) establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary;
- (B) prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to subparagraph (A), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers;... (emphasis added).

The above-referenced FCRA Section 621 (codified as 15 U.S.C. § 1681s) provides in relevant part in Subsection 621(a)(1) (codified as 15 U.S.C. § 1681s(a)(1)) as follows:

Enforcement by Federal Trade Commission. Compliance with the requirements imposed under this subchapter shall be enforced under the Federal Trade Commission Act [15 U.S.C. § 41 et seq.] by the Federal Trade Commission with respect to consumer reporting agencies and all other persons subject thereto, except to the extent that enforcement of the requirements imposed under this subchapter is specifically committed to some other government agency under subsection (b) hereof... (emphasis added).

The above-referenced “subsection (b)” lists a variety of federal regulatory agencies, several of which have promulgated their own versions of the Rule. Discussion of these other agencies’ rules is beyond the scope of this alert.

### Red Flags Rule Compliance Requirements

#### Compliance With Red Flags Rule

Each company that must comply with the Rule must periodically determine whether it offers or maintains “covered accounts.” To the extent it maintains one or more covered accounts, each company must establish a written identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be appropriate in size, scope, and complexity to the size of the company and to the nature of its activities.

The identity theft prevention program must identify “red flags” for the covered accounts – namely, the pattern, practice, or special activity that may indicate the possible existence of identity theft, detect the red flags that have been incorporated into the identity theft prevention program, respond to red flags when they are detected, and periodically update the identity theft prevention program to reflect changes in risk to customers. To identify relevant red flags for covered accounts, a company must determine what types of covered accounts it offers and maintains and how those accounts are opened and accessed, in addition to the company’s previous experiences with identity theft. The identity theft prevention policy should include red flags from the categories listed in the Rule (i.e., receiving alerts, notifications or warnings from a consumer reporting agency, receiving suspicious documents or suspicious personal identification information, unusual use of or suspicious activity related to the covered account, and notice from customers, victims of identity theft, law enforcement or the like regarding possible identity theft in connection with a covered account).

Further, the identity theft prevention program must provide for steps to detect red flags and prevent illegal activities – for example, verifying the identity of a person opening a covered account, monitoring transactions, and verifying the validity of change of address request for covered accounts. The program, including the red flags determined to be relevant, should be updated periodically

**Offices**

Atlanta  
Austin  
Boston  
Chicago  
Dallas  
Houston  
London  
Los Angeles  
New Orleans  
New York  
Sacramento  
San Francisco  
Washington DC

**The Red Flags Waive for Thee!**

*Extended Red Flags Rule Compliance Deadline is August 1, 2009* (cont'd.)

to reflect changed circumstances such as, for example, the experiences of the company, changes in methods of identity theft, detection, prevention, and mitigation, changes in types of accounts that the company offers or maintains, and changes in the company's business arrangements.

As noted above, the initial written identity theft prevention program must be approved either by the board of directors or an appropriate committee of the board of directors, and must involve the board, one of its committees, or a designated senior management-level employee to oversee, develop, implement, and administer the program, and to train staff and oversee service providers to ensure their compliance with the program.

**Administering the Identity Theft Prevention Program Required by the Red Flags Rule****Oversight of the Program**

The board of directors, an appropriate committee of the board, or a designated senior management-level employee should assign specific responsibility for the program's implementation, review reports prepared by staff regarding compliance with the Rule, and approve changes to the program necessary to address the changing identity theft risks.

**Periodic Reports to Board of Directors**

Staff responsible for development, implementation, and administration of the program should report to the board of directors, an appropriate committee of the board, or a designated senior management-level employee at least annually on compliance with the Rule. The reports should evaluate the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the identity theft prevention program.

**Monitoring Third-Party Service Providers for Compliance**

If a company engages a third-party service provider to perform an activity in connection with covered accounts, the company should 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.

**Conclusion**

The Rule has a surprisingly broad scope and requires compliance even by entities deemed to be at low risk for identity theft. Therefore, companies that have not done so already are encouraged to determine if they are compliant. The burden to comply with the Rule may not be that great for companies. The cost of non-compliance could, however, be significant.

**About the Authors**

Gregory T. Casamento is a partner in Locke Lord Bissell & Liddell's New York office. He focuses his practice on business, commercial, insurance and intellectual property litigation and technology transactions. Mr. Casamento has significant experience litigating trademark infringement claims, technology, contract and restrictive covenant disputes, and insurance issues for his clients before both State and Federal Courts. His experience also includes advising clients on e-Matters issues, including, e-signature, e-discovery, e-admissibility and e-records management.

Patrick J. Hatfield is a partner in the corporate department in the Atlanta office and co-chairs the Firm's Technology Transactions Group. Throughout his legal career, Mr. Hatfield has focused on financial services, intellectual property and technology, gaining valuable experience as in-house counsel, including 10 years as senior counsel and vice president to a leading provider of IT and outsourcing services to the global financial services industry (NYSE:PMS) now part of Computer Sciences Corporation. Mr. Hatfield has handled a wide range of IT, outsourcing, acquisition and joint venture arrangements in the global financial services industry. His experience includes handling licensing, outsourcing and mergers & acquisitions transactions in the United States, Europe, South Africa, Australia, and Asia.

Vita E. Zeltser is an associate in Locke Lord Bissell & Liddell's corporate department, focusing on general corporate and corporate governance matters, information technology, e-commerce, privacy, and information security.