



**MARSHALL, DENNEHEY, WARNER,
COLEMAN & GOGGIN**

Red Flag Rules Raise the Stakes on Identity Theft Prevention

Theodore J. Kobus III , Esquire

Safeguarding client data is not optional. It's the law.

On August 1, 2009, new federal regulations enforced by the FTC come into effect: the so-called Red Flag rules, which require businesses to take pro-active measures to detect and prevent identity theft involving client data. Financial institutions, which are not regulated by the FTC, have been subject to enforcement of the rules since November 1, 2008. The consequences of non-compliance are significant – civil penalties of up to \$2,500 per violation, which could quickly add up to painful amounts if a business has a large number of customer accounts and each account is considered a separate violation.

This bulletin provides an overview of the Red Flag rules. An appendix provides guidelines on implementing the systems needed to comply with the law.

Red Flag Rules

The Federal Trade Commission and other federal agencies have issued joint rules and guidelines to implement certain sections of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Known as the Red Flag rules, these rules and guidelines require various entities to develop procedures for detecting and preventing identity theft. Surprisingly, it appears that the rules apply not just to banks and other traditional financial institutions, but also to a tremendous number of unsuspecting businesses of all sizes.

As written, the rules apply to “financial institutions” and “creditors” with “covered accounts.” Without going into all the details of the definitions, a covered account is so broadly defined that just about any business that tracks transactions with customer-identifying information can be said to create “covered accounts.”

Obviously, “financial institutions” include banks, mortgage lenders, S&Ls and so forth. It is the definition of “creditor” that gives the Red Flag rules such broad application. In statements to clarify the meaning of the rules, the FTC noted that “any person that provides a product or service for which the consumer pays after delivery is a creditor.”¹

This extremely broad definition of “creditor” could apply to virtually any business that allows customers to defer payment and pay on credit. Simply accepting credit card payments does not make a business a “creditor” under the Red Flag Rules. But, professional service businesses that allow individual customers to defer payment over time, with or without financing charges will likely be viewed by the FTC as “creditors.” As noted in a recent FTC publication,² “if a company ... arranges for credit for its customers, or extends credit by selling customers goods or services and billing for them later, it is a ‘creditor’ under the laws.” Thus, the Red Flag rules are sweeping in their scope, going far beyond the traditional financial and banking industry entities.

The FTC has acted aggressively in the past with privacy issues, e.g., internet privacy statements in the early to mid 2000's related to the security of consumer credit card information. Thus, we expect the FTC to broadly apply its definition of “creditors,” sweeping all businesses offering open account payment terms into the purview of the Red Flag rules.

continued

What are the Red Flags?

FACTA defines a red flag as a pattern, practice or specific activity that indicates the possible existence of identity theft. The regulations provide guidance by listing five specific categories of red flags:

1. Alerts, notifications or other warnings received from consumer reporting agencies or service providers such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information, such as a suspicious address change;
4. The unusual use of, or other suspicious activity related to, a covered account;
5. Notice from customers, victims of identify theft or law enforcement authorities.

Compliance: What Do You Need To Do?

If the Red Flag rules apply to your business, you are required to implement a four-pronged identity theft prevention program for covered accounts.

Identify. You must identify and incorporate into your identity theft program any relevant patterns, practices, and activities that are “red flags” that could signal possible identity theft.

Detect. You must develop policies and procedures to detect red flags.

Respond. You must respond to any red flags that are detected, in order to prevent and mitigate identity theft. If red flags are detected, the guidelines recommend monitoring accounts for evidence of identity theft, contacting the customer, calling law enforcement and changing any security device that permits account access.

Update. You must update your ID theft program periodically to handle any changes in risks to customers from identity theft, or even risks to the soundness of the covered entity itself. Additionally, credit card issuers and users of consumer reports of all kinds, which include credit reports, have their own separate requirements, but these go beyond the scope of this bulletin.

Coordination with Industry and Profession-Specific Privacy and Security Rules

While the Red Flag rules apply broadly to “financial institutions” and “creditors” with “covered accounts,” there are other privacy-related laws, regulations and rules that apply to specific industries and professions. For example:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule applies to health care providers, health plans and health care clearinghouses and govern the handling of individually identifiable health information. They also can apply to advisors to those institutions, depending upon the circumstances.
- The Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLB Act) resulted in the issuance of the Privacy and Safeguards Rules by the FTC, which apply not only to traditional financial institutions such as banks and savings and loan associations, but also to non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. If your practice includes such services, you should review the rules and develop systems for compliance.
- Lawyers must also comply with professional ethics rules and regulations applicable to the handling of confidential client information.

This proliferating body of laws, regulations and rules underscores the importance of a coordinated approach to risk control. Businesses and professionals should designate an individual within their firm who is responsible for instituting and monitoring appropriate controls to ensure compliance with all privacy and data security requirements.

Summary

The Red Flag rules are one more sign that the landscape of privacy law is changing rapidly. The trend is clearly toward laws that require pro-active safeguards and that are broadly applicable to all industries.

The introduction of this bulletin noted that non-compliance with the Red Flag rules may result in civil penalties imposed by the Federal Trade Commission. However, it does not take a tremendous leap of logic to foresee plaintiff's attorneys using the Red Flag rules as a basis for the standard of care in a negligence action.

In short, those who ignore these rules do so at their peril.

Theodore J. Kobus III is a shareholder in Marshall, Dennehey, Warner, Coleman & Goggin's Philadelphia office. He chairs the firm's Technology, Media & Intellectual Property Practice Group.

* * *

Appendix – Protecting Your Clients from Identity Theft

Firms should consider the following guidelines for protecting their clients and complying with the Red Flag rules.

I. Identification of Red Flags for Your Identity Theft Program:

In addition to the broad categories of Red Flags listed above, Appendix A to the Red Flag rules³ includes 26 specific examples of potential red flags. Some of the more helpful guidance is as follows:

- A. Alerts, notifications or warnings from a consumer reporting agency:
 - 1. A fraud alert within a consumer report;
 - 2. A consumer reporting agency notes a credit freeze or address discrepancy;
 - 3. A recent increase in the volume of credit inquiries.

- B. Suspicious documents:
 - 1. ID documents that appear to be altered or forged;
 - 2. Photo ID is not consistent with the appearance of the customer;
 - 3. Information on the identification is not consistent with other information provided by the customer.

- C. Suspicious personal identifying information:
 - 1. The social security number is not issued or is listed on the Social Security Administration's Death Master File.
 - 2. The address does not match any address in the consumer report.
 - 3. The provided phone number is invalid or is associated with a pager or answering service.

- D. Suspicious activity related to a covered account:
 - 1. A covered account that has been inactive for a lengthy period of time is used.
 - 2. Mail to the customer is returned;
 - 3. An initial payment is not made, or an initial payment is made, but no subsequent payments.

II. Policies and Procedures to Detect Red Flags

Your compliance program should be in writing and should include the policies and procedures used by your company to detect red flags. Some examples are:

- Minimum information which must be contained in all applications for credit;
- A list of acceptable documentation for identity verification;
- Procedures to verify identification, such as check lists;
- Use of 3rd party verification tools.

continued

III. Responding to Red Flags

If red flags are detected, your compliance program should provide guidance on how to respond. Some of the possible responses are:

- Escalation of the issue to a manager;
- Instructing staff to not proceed with a transaction until the red flag is resolved;
- Requiring a satisfactory explanation for the red flag from the customer;
- Asking for additional identifying information;
- Notifying law enforcement;
- If applicable, changing passwords and/or security codes associated with an account.

IV. Updating the Program

Your compliance program should also include provisions for continually updating the program. These provisions could include:

- The committee or manager in charge of the program will review the program at least once each year;
- The program will be reviewed after any significant incident of identity theft;
- A formal report that will be prepared for any identity theft incidents that were not prevented by the policies and procedures in place at the time;
- Updates to the program should include any new methods of identity theft and/or any new methods of identity theft detection.

V. Costs

Obviously, the costs to implement and maintain a program in compliance with the Red Flag rules will vary greatly with the size, complexity and number of covered accounts handled by your company. Estimates have ranged from \$.32 to \$1.03 for each covered account.⁴ Also, there are many third-party providers willing to package and put in place a Red Flag compliance program. Their fees and services will vary widely.

Additional Resource: Current FTC guidance for businesses regarding compliance with the Rule can be found at the following web site: <http://www2.ftc.gov/bcp/edu/microsites/redflagrule/index.shtml>

¹ FTC Enforcement Policy Statement, <http://www.ftc.gov/os/2008/10/081022idtheftredflagrule.pdf>

² <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

³ 16 C.F.R., section 681, Identity Theft Rules, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr681_main_02.tpl

⁴ Security Update on Red Flag Compliance, <http://www.solutionary.com/pdfs/RedFlagSecurityCompliance.pdf>

