



HIRSCH  
ROBERTS  
WEINSTEIN LLP

ATTORNEYS AT LAW

## **AN OVERVIEW OF THE FEDERAL TRADE COMMISSION'S IDENTITY THEFT "RED FLAGS RULES"**

In 2009 Massachusetts businesses must come into compliance with two new laws designed to combat and address identity theft: the Federal Trade Commission (FTC) Red Flags Rules and the Massachusetts Data Security Regulations. As explained in a previous HRW Overview,<sup>1</sup> the Massachusetts regulations require all Massachusetts businesses to take specific steps to protect residents' "Personal Information." The FTC Red Flags Rules, which begin where state data security laws leave off, require businesses to implement certain procedures for detecting and responding to identity theft. The FTC will begin enforcing these rules on August 1, 2009. This document is intended to give a brief overview of the FTC Red Flags Rules, 16 CFR § 681.2, and outline the action items Massachusetts businesses should take to be in compliance by August 1, 2009.<sup>2</sup>

### **Introduction**

The Red Flags Rules require every business that provides goods or services for which a consumer pays after delivery to implement a written identity theft prevention program to identify, detect, and respond to warning signs – "red flags" – that someone has opened or is trying to open an account using someone else's identity or that someone is misusing another's existing account as their own.<sup>3</sup>

The required program must be tailored to the actual day-to-day operations of the business, and its complexity will depend on the risk of identity theft in that business. For businesses that know their clients personally and do not process third-party transactions, the program can be simple since the risk of identity theft is small. For other businesses, such as those that provide medical services on an emergency basis or that offer installment sales agreements or that provide professional services to people not otherwise known to them or that permit remote access to accounts, the risk is greater, and the program must accordingly be more detailed.

---

<sup>1</sup> HRW's Overview of the Massachusetts Data Security Regulations can be found at [www.hrwlawyers.com](http://www.hrwlawyers.com).

<sup>2</sup> This document is for educational purposes only and should not be relied on as legal advice. You are encouraged to consult with counsel before making any decisions concerning the issues discussed in this document.

<sup>3</sup> A red flag is any type of indication that the person is trying to open or use an account to obtain goods or services and have them billed to someone else. A red flag may be something as simple as the presentation of an identification card that is obviously altered or a customer reporting that the goods or services for which he or she was billed were not received by him or her. Or it may be something more difficult to detect, such as a new account used in a manner commonly associated with known patterns of fraud or in a manner that differs from established patterns of activity on the account

Because businesses have an interest in ensuring that the customers and clients to whom they provide goods and services are who they say they are, most businesses will already have in place at least some informal procedures for ensuring the identity of their customers and clients. The Rules require that these procedures be institutionalized in a written program and that the business systematically identify all the red flags it may encounter and how it will address them.

## **Coverage**

Although the governing statute was designed to prevent identity theft in connection with lenders such as banks, finance and credit card companies, utility companies, and telecommunications companies – all of which extend credit to people with whom they have no in-person contact – the Red Flags Rules apply to all businesses that permit customers or clients to receive services before paying for them. Specifically, the Rules apply to “financial institutions” and “creditors.” A “creditor” is any entity that regularly permits deferred payments for goods or services. The FTC has explained that “any person that provides a product or service for which the consumer pays after delivery is a creditor” under the Rules.<sup>4</sup>

## **Scope**

The Red Flags Rules apply only to client accounts. Unlike the Massachusetts Data Security Regulations, the Rules do not apply to employee information since the focus is on preventing the wrongful opening and use of accounts, not the safeguarding of information. As such, the Rules focus on

- (1) ways someone could open an account under someone else’s identity,
- (2) the means of detecting such wrongful actions, and
- (3) actions to be taken when “red flags” go up that such wrongful actions might be occurring.

## **Requirements**

The Red Flags Rules set out five requirements that every business that has "covered accounts" must meet:

- (1) Identify all covered accounts. “Covered accounts” are any accounts through which a client or customer is extended any type of credit that are used mostly for personal, family, or household purposes that involve multiple payment or transactions or any accounts for which there is a foreseeable risk of identity theft.
- (2) Create and implement a written program that has policies and procedures to
  - (a) Identify all “red flags” associated with all covered accounts.
  - (b) Detect red flags.
  - (c) Respond to red flags.
  - (d) Ensure the program is updated at least annually.
- (3) Administer the program, including obtaining board approval and reporting annually.
- (4) Train employees on the program periodically.
- (5) Exercise appropriate and effective oversight of service provider arrangements.

---

<sup>4</sup> [www.ftc.gov/os/2008/10/081002idthftredflasrule.pdf](http://www.ftc.gov/os/2008/10/081002idthftredflasrule.pdf)

The Red Flags Rules do not set specific requirements for safeguarding information as the Massachusetts Data Security Regulations do, but they are quite specific as to the types of Red Flags that need to be considered. The Rules require that as part of the identification of red flags, businesses consider (a) certain risk factors for identity theft,<sup>5</sup> (b) various sources of red flags,<sup>6</sup> and (c) 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 identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

The FTC has further listed twenty-six examples under these categories, which can be found in Supplement A to Appendix A of the Red Flags Rules (available at [www.hrwlawyers.com](http://www.hrwlawyers.com) as “Guidelines to FTC Red Flags Rules”).

### **Penalties**

Although businesses will incur costs to implement the Red Flags Rules, the cost of noncompliance may be higher: \$2,500 per violation.

### **Next Steps**

Follow the “To Do” List attached to this Overview. Start soon so that your Program is in place before the August 1, 2009, deadline.

### **For More Information**

Contact any of the following members of HRW’s Data Security Team:

- Andrea C. Kramer, 617-348-4380, [akramer@hrwlawyers.com](mailto:akramer@hrwlawyers.com)
- C. Max Perlman, 617-348-4326, [max@hrwlawyers.com](mailto:max@hrwlawyers.com)
- Erin D. Reed, 617-348-4385, [ereed@hrwlawyers.com](mailto:ereed@hrwlawyers.com)
- David B. Wilson, 617-348-4314, [dwilson@hrwlawyers.com](mailto:dwilson@hrwlawyers.com)

---

<sup>5</sup> The Red Flags Rules list the following risk factors to be considered:

- (1) The types of covered accounts it offers or maintains.
- (2) The methods it provides to open its covered accounts.
- (3) The methods it provides to access its covered accounts.
- (4) Its previous experiences with identity theft.

<sup>6</sup> The Red Flags Rules list the following sources of red flags as ones to be considered:

- (1) Incidents of identity theft that the financial institution or creditor has experienced.
- (2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.
- (3) Applicable supervisory guidance.

## “To Do” List - By August 1, 2009

- Assemble an internal data security team, just as was recommended in connection with the Massachusetts Data Security Regulations. It can be the same team. In fact, having the same team may help the organization fashion one program that complies with both regulatory regimes, thereby reducing the chance of conflict between the programs and the time spent complying and training for both programs. Ideally, this team would include Operations, Human Resources, Information Technology, Accounting/Billing, Sales, and Legal.
- Educate the data security team on the requirements and details of the new rules.
- Identify the accounts that are subject to the Rules.
- List all the ways in which someone could open an account with your business using someone else’s identity or could misuse someone else’s existing account to obtain goods or services for themselves. In making the list, consider any incidents of identity theft your business has experienced.
- List all the red flags your business might encounter and how they would be detected. As part of this process, go through the Guidelines to the FTC Red Flags Rules, available at [www.hrwlawyers.com](http://www.hrwlawyers.com). Add other red flags that are particular to your business.
- Determine the steps that will be taken to respond to any red flags that are detected. Appropriate responses may include the following:
  - (a) Monitoring a covered account for evidence of identity theft.
  - (b) Contacting 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.
  - (i) Determining that no response is warranted under the particular circumstances.
- Document (or formalize the lists of) the red flags, the detection methods, and the responses to red flags identified in the previous steps. This will be the required written Identity Theft Prevention Program.
- Determine whether your business uses any service providers who might detect any red flags, such as a collection agency or a billing company. If so, document how the service provider will be supervised and add this to the program.
- Have the board of directors approve the program.
- Designate a senior employee to administer the program.
- Train the appropriate personnel on the program.