

# Red Flag Rules Deadline Approaching (Deadline has since been extended to May 1, 2009\*)

Source: ACA International, MAPbulletin - October 2008

*October 3, 2008*

Pursuant to regulations promulgated by the Federal Trade Commission (FTC) and other federal agencies, financial institutions and creditors will be required to create an Identity Theft Prevention Program (the "Program") to detect, prevent, and mitigate identity theft with respect to the opening of certain accounts or certain existing accounts. These regulations, often called the Red Flag Rules, became effective January 1, 2008, and mandatory compliance is required by November 1, 2008.

## ***Who Must Comply with the Red Flag Rules?***

The Red Flag Rules apply to financial institutions and creditors who offer or maintain one or more covered accounts, and specifically mandate these entities create and implement a Program.<sup>1</sup>

A **financial institution** is defined as 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 section 461(b) of Title 12) belonging to a consumer."<sup>2</sup>

Section 461(b), which falls under the Federal Reserve System regulations, defines a **transaction account** as 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.<sup>3</sup>

Traditional third-party debt collectors generally will not qualify as a financial institution under § 1681a(t) because they do not maintain transaction accounts whereas asset buyers may if they do hold such active accounts.

A **creditor** is defined as "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."<sup>4</sup> The term "credit" is defined as "the right granted by a creditor to a debtor to defer payment of debt or to incur

debts and defer its payment or to purchase property or services and defer payment therefore.”<sup>5</sup> Both definitions are adopted from the Equal Credit Opportunity Act (ECOA).

The FTC has stated that while accepting credit cards as a method of payment does not make the accepting entity a creditor, business such as finance companies, automobile dealers, utility companies, and telecommunication companies are creditors. Even non-profit and government entities who defer payment of goods and services are considered creditors.<sup>6</sup>

Unlike financial institutions, traditional third-party debt collectors and asset buyers may be required to develop and implement an identity theft prevention program. The guidance states a creditor could include third-party debt collectors if such parties assist in arranging for the extension, renewal, or continuation of credit.<sup>7</sup>

Similarly, an asset buyer participating in such activity could also be considered a creditor under the FCRA and regulations. However, the guidance does not provide examples of situations in which a third-party debt collector would be considered a creditor. As a result, it is crucial third-party debt collectors and asset buyers review their business practices to determine whether their interaction with clients makes them a creditor and obligates them to develop and implement a Program.

A **covered account** is an account that is offered primarily for personal, family, or household purposes that permits multiple payments or transactions as well as any other account the entity offers or maintains “for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.”<sup>8</sup> Because the definition of a covered account is extremely broad, any financial institution or creditor that reasonably foresees problems arising from identity theft should be prepared to create a written Program.

Although a collection agency or asset buyer may not be a creditor or financial institution, debt collectors may still be required to create and implement policies and procedures to detect, prevent, and mitigate identity theft, albeit by way of the creditor or financial institution because the Red Flag Rules require those entities provide for the Program’s continued administration and oversight. Among other things, the creditor or financial institution must take necessary steps to ensure service providers are complying with the Program.<sup>9</sup> Because the entity remains responsible for following the regulations, regardless of whether a service provider conducts certain operations for the entity, it is crucial the service provider understand the Program and incorporate the Program as necessary into its business practice.

Third-party debt collectors are likely service providers, and therefore, may be required by the entity to develop and implement policies and procedures mirroring the Program created by the entity. The guidance states if the entity “engages a service provider to perform an activity in connection with one or more covered accounts,” then the entity “should take steps to 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.”<sup>10</sup>

The guidance suggests, as an example, entities could require a service provider, by contract, to develop and implement policies and procedures to detect relevant Red Flags, report Red Flags to the entity, or undertake certain steps to prevent or mitigate identity theft.<sup>11</sup>

As a result, while a third-party debt collector or asset buyer may not be a creditor or financial institution, such businesses may still be required by their creditor or financial institution client to develop and enforce policies and procedures similar to those required of a Program under the regulations for any covered accounts.

### ***What Does the Identity Theft Prevention Program Require?***

The Red Flag Rules require responsible entities satisfy four elements in creating and implementing reasonable policies and procedures of an identity theft prevention program.

#### **1. Identify any specific activity, pattern, or practice indicating a possible existence of identity theft.**

Otherwise known as the Red Flags, the entity should consider four factors in determining what Red Flags it should incorporate into its Program:

- What types of covered accounts does the entity maintain or provide?
- What methods does the entity use in maintaining or providing covered accounts?
- What forms of access does the entity provide to consumer accounts?
- What experiences has the entity had with identity theft in the past?

The Red Flags are intended to alert the entity to any specific activity, pattern, or practice indicating the possible existence of identity theft. The guidance provides five categories from which Red Flags should be included in the Program:

- a. Alerts or warnings received from consumer reporting agencies or service providers;
- b. Presentation of suspicious documents;
- c. Presentation of any suspicious personal identifying information;
- d. Suspicious activity relating to a covered account; and
- e. Any notices received from identify theft victims, law enforcement authorities, or other parties containing information related to identity theft as to covered accounts.

The guidelines also provide a substantial list of examples of Red Flags that would fall under the above categories.

## **2. Detect Red Flags Incorporated in the Program**

The Program must have sufficient policies and procedures addressing the detection of those incorporated Red Flags. The guidelines provide two examples of such policies and procedures. First, acquiring identifying information about a person opening a covered account and verifying his or her identity. Second, identifying, monitoring, and verifying the validity of change of address requests for existing covered accounts.

## **3. Respond Appropriately to Any Red Flags Detected**

Once a Red Flag has been detected, the Program must define how the entity will respond. In responding to a Red Flag, the entity should determine whether the Red Flag detected a risk of identity theft and must have a reasonable basis to conclude there is no evidence of risk of identity theft.

The guidelines suggest an appropriate response should relate to the degree of risk detected by a Red Flag. The entity should also consider aggravating factors that may increase the degree of risk of identity theft, including loss of data security or notice that a party acting falsely as the entity acquired information from a customer of a covered account. The guidelines also provide nine examples of appropriate responses to Red Flags detected through the Program such as contacting the customer, reopening a covered account with a new account or identification number, or heightened monitoring of a covered account.

## **4. Update the Program Periodically**

The Program must be reviewed and updated periodically, and any updates should reflect changes in risks to customers and the entity from identify theft. This review not only includes considering changes in identity theft methods as well as the accounts the entity offers or maintains, but it also requires consideration of changes in business arrangements of the entity.

Additional information about the Red Flag Rules is available through [E-Compliance](#) on ACA's Web site, Document No. 1250.

### **ACA Hosting Red Flags Teleseminar**

ACA International is hosting a Web seminar on October 13, 2008, to provide greater detail about the Red Flag Rules and how they may apply to the collection industry. Please visit the [ACA International Online Calendar](#) to register.

<sup>1</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63772-74 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).

<sup>2</sup> 15 U.S.C. § 1681a(t) (2006).

<sup>3</sup> 12 U.S.C. § 461(b)(1)(C) (2006).

<sup>4</sup> 15 U.S.C. § 1681a(r)(5) (2006).

<sup>5</sup> 15 U.S.C. § 1691a(d) (2006).

<sup>6</sup> FTC Business Alert, June 2008, <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>.

<sup>7</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63722 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).

<sup>8</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63772 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).

<sup>9</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63773 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).

<sup>10</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63773-74 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).

<sup>11</sup> Identity Theft Red Flags Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63773-74 (Nov. 9, 2007) (to be codified at 16 C.F.R. pt. 681.2).