

**DISCLAIMER:** This document has not been approved, disapproved, or otherwise acted upon by any senior technical committees of, and does not represent an official position of the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services on this Web site. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

## **A CPA's GUIDE TO CREATING AN IDENTITY THEFT PREVENTION PROGRAM**

The Federal Trade Commission (FTC) has enacted the Red Flags Rule (rule), which affects all CPA firms. The Red Flags Rule requires not only CPA firms, but many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs or “red flags” of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts. By identifying red flags in advance, a firm will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into a costly episode of identity theft.

The rule was enacted to deter identity theft and is mandated by the Fair and Accurate Credit Transactions Act of 2003. It requires financial institutions and creditors to implement programs to detect, prevent, and mitigate identity theft.

Under the rule, the definition of *creditor* includes businesses or organizations that regularly provide goods or services first and allow customers to pay later. According to the [FTC's FAQs](#), examples of groups that may fall within this definition are utilities, health care providers, lawyers, **accountants**, and other professionals.

Compliance with this rule requires CPAs to protect the identities of their clients. You must have a written policy with procedures that are designed to prevent, detect, and mitigate identity theft—the Identity Theft Prevention Program (program). This program must be properly designed, documented, regularly updated, and must be approved and reviewed by the management of the firm. Training must be provided to your employees to comply with the program. If any business operations have been outsourced that might be susceptible to identity theft, you are required to ensure that the service provider has an adequate Red Flags program in place.

The four basic steps to designing a program to comply with the rule are as follows:

1. Identify relevant red flags
2. Detect red flags
3. Prevent and mitigate identity theft
4. Update the program periodically

The program must spell out how it will be administered and should be appropriate to the size and nature of your operations.

The following are step-by-step procedures for developing an identity theft prevention program.

### **Step One: Identify Relevant Red Flags**

The program must include reasonable policies and procedures to identify the red flags of identity theft you may run across in the day-to-day operations of your firm. Red flags are suspicious patterns, practices, or activities that indicate the possibility of identity theft. (Review the list of the 26 Red Flags identified by the FTC in [supplement A](#) to the rule and identify those that are

relevant to your practice.) You should review your files, which may identify other red flags not on the list that are relevant to your practice.

### **Step Two: Detect Red Flags**

Once you have identified and documented those red flags relevant to your practice, you must develop and document those procedures required to address those red flags if encountered.

For example, you may spot a red flag when you verify a client's identity, monitor transactions, or verify requests for changes of address. Some red flags may seem harmless on their own but may signal identity theft when paired with other events such as a change of address coupled with the use of an address associated with fraudulent accounts.

### **Step Three: Prevent and Mitigate Identity Theft**

The program must include appropriate responses to your red flags in order to prevent and mitigate identity theft. These responses could include monitoring an account, closing an account, refusing to open a new account, contacting the client when a red flag is spotted, or a combination of these. Sometimes no response may be proper. In other cases, certain events— such as a recent data breach, a phishing fraud that targeted your firm, or another suspicious activity—may raise the risk of identity theft and require specific preventive actions.

### **Step Four: Update the Program Periodically**

Because identity theft threats change, the program must describe how it will be updated to ensure new risks and trends are being identified.

#### *Administering the Program*

The program must describe how it will be administered and maintained. The program must be approved by the firm's management. The manager must approve any material changes to the program. The program should provide for training, where appropriate, and provide a way to monitor the work of any service providers. The key is to maintain oversight of the program, keep it relevant and current, and ensure that all necessary members of your firm are on board.

#### *Responsibility for the Program*

The manager is responsible for implementing and administering the identity theft prevention program. An office manager, associate, or other senior staff member can be the designated program administrator, but the manager owner retains oversight and approval of any revisions to the program.

#### *Program Administrator Duties*

The program administrator must be notified immediately when any red flags are detected and is required to oversee the response. The identification of and response to red flags must be documented in a log.

#### *Training*

Members of the firm should be trained to recognize, report, and respond (where appropriate) to red flags encountered by the firm. The training program should provide the following:

- The purpose
- Identification of red flags
- Proper procedures for reporting and responding to red flags

All members of the firm should receive a copy of the program and need to sign a form acknowledging that they have read and are complying with the program. Copies of these signed forms are required to be retained by the firm.

#### *Service Providers*

You need to take into consideration the firm's arrangements with payroll service providers, credit card companies and credit organizations, or any other providers that may store the personal information of staff or clients. Review your agreements with these providers to make sure they positively state that they protect against identity theft. If the agreement does not specifically state this, you need to verify their protection against identity theft. You may choose to ask for a new agreement including such a statement, or you may opt to refuse to do business with them.

#### *Reviewing and Evaluating the Program*

Periodic review and evaluation of the firm's written identity theft prevention program is required. The program must be reviewed and modified as needed annually or more frequently if necessary.

#### *Penalties for Noncompliance*

The FTC can seek both monetary civil penalties and injunctive relief for violations of the Red Flags Rule. If a complaint seeks civil penalties, the U.S. Department of Justice typically files the lawsuit in federal court on behalf of the FTC. Currently, the law sets \$3,500 as the maximum civil penalty per violation. Each instance in which the company has violated the rule is a separate violation. Injunctive relief in cases like this often requires the parties being sued to comply with the law in the future, as well as provide reports, retain documents, and take other steps to ensure compliance with both the rule and the court order. Failure to comply with the court order could subject the parties to further penalties and injunctive relief.

**DISCLAIMER:** This document has not been approved, disapproved, or otherwise acted upon by any senior technical committees of, and does not represent an official position of the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services on this Web site. If legal advice or other expert assistance is required, the services of a competent professional should be sought.