

**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.

**Sample  
Identity Theft Prevention Program  
Effective November 1, 2009**

The obligation to develop a written Red Flags Rule Identity Theft Prevention Program (Program) is not a “one-size-fits-all” requirement. **You must customize this template to fit your particular firm’s situation.** If any of the language does not adequately address your firm’s business situation, you will need to prepare your own language. You are responsible for ensuring that the program fits your firm’s business and that you implement the Program. The language in this template is designed to be a starting point and to walk you through developing your firm’s Program. Following this template does not guarantee compliance, or create any safe harbor, with the Federal Trade Commission’s Rule.

I.	INTRODUCTION AND OVERVIEW .....	2
A.	Firm Policy .....	2
II.	PROGRAM ADOPTION AND DEFINITIONS.....	2
A.	Program Adoption .....	2
B.	Red Flags Rule Definitions Used in This Program .....	2
III.	IDENTIFICATION OF RED FLAGS.....	3
A.	Alerts, Notifications, and Warnings From a Credit Reporting Company .....	3
B.	Suspicious Documents .....	3
C.	Suspicious Personal Identifying Information .....	3
D.	Suspicious Account Activity or Unusual Use of Account .....	4
E.	Alerts From Others.....	4
IV.	DETECTING RED FLAGS .....	4
A.	New Accounts .....	4
B.	Existing Accounts.....	5
C.	Consumer (“Credit”) Report Requests .....	5
V.	RESPONDING TO RED FLAGS TO MITIGATE IDENTITY THEFT .....	5
A.	Prevent and Mitigate .....	5
B.	Protect Personal Information.....	6
VI.	PROGRAM ADMINISTRATION .....	6
A.	Oversight .....	6
B.	Program Updates .....	6
C.	Staff Training and Reports .....	7
D.	Service Provider Arrangements.....	7
VII.	APPROVAL .....	7
VIII.	APPENDIX A.....	8

## **I. INTRODUCTION AND OVERVIEW**

### **A. Firm Policy**

[FIRM NAME]'s policy is to protect our clients and their accounts from identity theft and to comply with the Federal Trade Commission's (FTC) Red Flags Rule. We will do this by developing and implementing this written Identity Theft Prevention Program (Program), which is appropriate to our firm's size and complexity, and the nature and scope of our activities. This Program addresses 1) identifying relevant identity theft Red Flags, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our Program periodically to reflect changes in risks.

Our identity theft policies, procedures, and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Based on the definitions used in these regulations, there are several areas at [FIRM NAME] where this Program applies, including client payments. This Program may also apply to any other business functions of [FIRM NAME], which allow clients to defer payment for product or services.

## **II. PROGRAM ADOPTION AND DEFINITIONS**

### **A. Program Adoption**

[FIRM NAME] developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of [FIRM NAME] Management. After consideration of the size and complexity of our operations and account systems, and the nature and the scope of our activities, we have determined that this Program was appropriate for [FIRM NAME], and therefore approved this Program on [DATE].

### **B. Red Flags Rule Definitions Used in This Program**

**Account:** a continuing relationship with a creditor to obtain a product or service that includes deferred payments for services or property.

**Covered account:** (1) an account offered or maintained by [FIRM NAME] primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions; and (2) any other account offered or maintained by [FIRM NAME] for which identity theft is a reasonably foreseeable risk that may impact [FIRM NAME]'s clients or the safety and soundness of [FIRM NAME], including financial, operational, compliance, reputation, or litigation risks. An [FIRM NAME] example of a "covered account" is a client billing account.

If the covered account is provisioned by or processed by a third party, then the guidance regarding third parties may apply (see Section VI).

**Credit:** the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

**Creditor:** any person or business who arranges for the extension, renewal, or continuation of credit with a covered account.

**Identity Theft:** fraud committed or attempted using the identifying information of another person without authority.

**Identifying Information:** any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.

**Red Flag:** a pattern, practice, or specific activity that indicates the possible existence of identity theft.

### **III. IDENTIFICATION OF RED FLAGS**

To identify relevant Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) its previous experience with identity theft. We considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation:

#### **A. Alerts, Notifications, and Warnings From a Credit Reporting Company**

##### **Red Flags**

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an individual;
3. Notice or report from a credit agency of an active duty alert for an individual;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an individual's usual pattern or activity.

#### **B. Suspicious Documents**

##### **Red Flags**

6. Identification document or card that appears to be forged, altered, or inauthentic;
7. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
8. Other documents with information that is not consistent with existing personal information (such as if a person's signature does not match between different documents, or does not match signature on file); and
9. Application that appears to have been altered or forged.

#### **C. Suspicious Personal Identifying Information**

##### **Red Flags**

10. Identifying information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
11. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
12. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
13. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number);
14. Social security number presented that is the same as one given by another individual;
15. An address or phone number presented that is the same as that of another person;
16. A person fails to provide complete personal identifying information on an application when reminded to do so;
17. A person's identifying information is not consistent with the information that is on file for the individual.

D. Suspicious Account Activity or Unusual Use of Account

**Red Flags**

18. Change of address for an account followed by a request to change the individual's name;
19. Payments stop on an otherwise consistently up-to-date account;
20. Account used in a way that is not consistent with prior use;
21. Mail sent to the account holder is repeatedly returned as undeliverable;
22. Notice to the firm that the individual is not receiving mail sent by the firm;
23. Notice to the firm that an account has unauthorized activity;
24. Breach in the firm's computer system security; and
25. Unauthorized access to or use of individual account information.

E. Alerts From Others

**Red Flag**

26. Notice to the firm from an individual, identity theft victim, law enforcement, or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

We understand that some of these categories and examples may not be relevant to our firm, and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant Red Flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of Red Flags, we have identified our firm's Red Flags, which are contained in the first column of Appendix A, "Red Flag Identification and Detection Grid."

**IV. DETECTING RED FLAGS**

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new covered account**, [FIRM NAME] personnel will take steps to obtain and verify the identity of the

person opening the account. Each business unit responsible for offering covered accounts is expected to document the steps they will take, considering methods such as:

1. Requiring certain identifying information such as name, date of birth, address, driver's license, or other identification, and, where feasible, to compare with existing file information for the individual;
2. Verifying the identity (for instance, examine the picture on a government-issued ID card); and
3. Independently contacting the purported individual, using contact information already on file in [FIRM NAME] systems.

#### B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing covered account**, [FIRM NAME] personnel will take steps to monitor transactions with an account. Each business unit responsible for monitoring covered accounts is expected to document the steps they will take, considering methods such as:

1. If an individual is requesting information in person, or via telephone, fax, or email, then verifying the identification of the individual prior to providing the information;
2. Verifying the validity of requests to change billing addresses, and/or confirming changes, such as sending a change confirmation to email address on file; and
3. Verifying changes in banking information given for billing and payment purposes, such as contacting the individual via information already on file, prior to making any changes.

#### C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for which a credit or background report is sought, [FIRM NAME] personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time of the request for the credit report is made to the consumer reporting agency; and
2. In the event that the notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the firm has reasonably confirmed is accurate.

### V. **RESPONDING TO RED FLAGS TO MITIGATE IDENTITY THEFT**

In the event [FIRM NAME] personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, after consulting with department management and depending on the degree of identity theft risk posed by the Red Flag:

#### A. Prevent and Mitigate

1. Contact the affected individual, using information already on file;
2. Change any passwords or other security devices that permit access to accounts;
3. Continue to monitor an account for evidence of identity theft;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;

7. Notify the Program Administrator to have the incident logged, and for additional assistance if needed;
8. Determine that no response is warranted under the particular circumstances.

#### B. Protect Personal Information

In order to further prevent the likelihood of identity theft occurring with respect to [FIRM NAME] accounts, [FIRM NAME] staff will adhere to [FIRM NAME]'s policies and practices regarding protection of personal information by:

1. Collecting only the personal information that is needed for firm purposes;
2. Retaining personal information for only the time period legally required and/or necessary for firm purposes;
3. Protecting personal information collected, used, disclosed, and retained;
4. Ensuring additional protection methods on sensitive personal information that is retained;
5. Restricting access to personal information only to individuals who have a business need to access information;
6. Disposing of personal information appropriately;
7. Instilling awareness and training employees on the proper handling of personal information;
8. Understanding the requirements of applicable data privacy protection laws and regulations;
9. Conducting regular risk assessments to identify where and how the firm stores or transmits personal information;
10. Developing, reviewing, and assessing the information security management program, policies, and procedures to ensure they are current and effectively communicated throughout the firm.

## VI. PROGRAM ADMINISTRATION

#### A. Oversight

Responsibility for developing, implementing, and updating this Program lies with the Program Committee, under the sponsorship and oversight of the Executive Committee, and comprised of representatives of Human Resources, Internal Technology, Marketing, and Finance working in consultation with key business process owners, such as Client Billing Services.

The Committee will be responsible for the Program administration, for ensuring appropriate training of [FIRM NAME] staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program. The Committee will annually report to [FIRM NAME]'s Management.

#### B. Program Updates

This Program will be periodically reviewed and updated to reflect changes in risks to individuals and the soundness of [FIRM NAME]'s Program to protect individuals from identity theft. At least annually, the firm will consider its experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts it maintains, and changes in the firm's business arrangements with other entities. After considering these factors, the Program

Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Committee will recommend updates to the Program, pending management approval.

**C. Staff Training and Reports**

[FIRM NAME] staff responsible for implementing the Program shall be trained in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Areas with covered accounts will review the Program at least annually, incorporating any Program updates in their processes. New employees are expected to be trained prior to any involvement with covered accounts. Staff is expected to report any suspicious activity to the Program Administrator; this will automatically create a record in the reporting system. The Program Committee will prepare an annual review of the Program, including compliance and effectiveness.

**D. Service Provider Arrangements**

In the event [FIRM NAME] engages a service provider to perform an activity in connection with one or more covered accounts, [FIRM NAME] will take steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. This may include a review of the service provider's Red Flag Identity Theft Program, or contract language with regard to policies and procedures. Additionally, [FIRM NAME] and the service provider should have a mutually agreeable means for notification in the event the service provider identifies a Red Flag situation.

**VII. APPROVAL**

I approve this Identity Theft Prevention Program as reasonably designed to enable [FIRM NAME] to detect, prevent, and mitigate identity theft.

Signed: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**VIII. APPENDIX A**

**Red Flag Identification and Detection Grid**

This grid provides Federal Trade Commission categories and examples of potential Red Flags.<sup>1</sup> Please note these examples are not exhaustive nor a mandatory checklist, but a way to help a firm think through relevant Red Flags in the context of its business. Some examples may not be relevant to the firm, while others may be relevant when combined or considered with other indicators of identity theft. You may modify the cells in the table below as described in Section III, Identification of Red Flags, and Section IV, Detecting Red Flags. If any categories and examples under them do not apply to the firm, delete the rows containing them. Likewise, add rows for any not on the list that you need to add based on your risk factor and sources assessment. For example, if the firm does not use consumer credit reports, it should delete the “Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency” and the rows of Red Flag examples 1 through 4 under it. If the firm chooses to use this template as a guide, it must adapt it to reflect the firm's business situation. Without such analysis and modification, the firm's Program will not comply with regulatory requirements.

<b>Red Flag</b>	<b>Detecting the Red Flag</b>
<b>Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency</b>	
1. A fraud or active duty alert is included on a consumer credit report.	We will verify that the fraud or active duty alert covers an applicant or client and review the allegations in the alert. [In addition, <i>describe any other steps the firm takes</i> ].
2. A notice of credit freeze is given in response to a request for a consumer credit report.	We will verify that the credit freeze covers an applicant or client and review the freeze. [In addition, <i>describe any other steps the firm takes</i> ].
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	We will verify that the notice of address or other discrepancy covers an applicant or client and review the address discrepancy. [In addition, <i>describe any other steps the firm takes</i> ].
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	We will verify that the consumer credit report covers an applicant or client, and review the degree of inconsistency with prior history. [In addition, <i>describe any other steps the firm takes</i> ].
<i>Insert other Red Flags in this category based on the firm's own experience or its knowledge of likely new methods of identity theft.</i>	<i>Insert how the firm would detect these Red Flags you have identified.</i>
<b>Category: Suspicious Documents</b>	
5. Identification presented looks altered or forged.	Our staff who deal with clients and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged. [In addition, <i>describe any other steps the firm takes</i> ].

<sup>1</sup> This grid is reprinted from the *FTC FACT Act Red Flags Rule Template* provided by the Financial Industry Regulatory Authority (FINRA).

6. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with clients and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it. [In addition, <i>describe any other steps the firm takes</i> ].
7. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with clients and their supervisors will ensure that the identification and the statements of the person presenting it are consistent. [In addition, <i>describe any other steps the firm takes</i> ].
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card, or a recent check.	Our staff who deal with clients and their supervisors will ensure that the identification presented and other information we have on file from the account, such as [ <i>describe the information</i> ] are consistent. [In addition, <i>describe any other steps the firm takes</i> ].
9. The application looks like it has been altered, forged, or torn up and reassembled.	Our staff who deal with clients and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled. [In addition, <i>describe any other steps the firm takes</i> ].
<i>Insert other Red Flags in this category based on the firm's own experience or its knowledge of likely new methods of identity theft.</i>	<i>Insert how the firm would detect these Red Flags you have identified.</i>
<b>Category: Suspicious Personal Identifying Information</b>	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	Our staff will check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match. [In addition, <i>describe any other steps the firm takes</i> ].
11. Inconsistencies exist in the information that the client gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	Our staff will check personal identifying information presented to us to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables [ <i>or describe other internal consistency tests made</i> ].
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent. [In addition, <i>describe any other steps the firm takes</i> ].
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff will validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services. [In addition, <i>describe any other steps the firm takes</i> ].
14. The SSN presented was used by someone else opening an account or other clients.	Our staff will compare the SSNs presented to see if they were given by others opening accounts or other clients. [In addition, <i>describe any other steps the firm takes</i> ].
15. The address or telephone number presented has been used by many other people opening	Our staff will compare address and telephone number information to see if they were used by other applicants

accounts or other clients.	and clients. [In addition, <i>describe any other steps the firm takes</i> ].
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff will track when applicants or clients have not responded to requests for required information and will follow up with the applicants or clients to determine why they have not responded. [In addition, <i>describe any other steps the firm takes</i> ].
17. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file. [In addition, <i>describe any other steps the firm takes</i> ].
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	Our staff will authenticate identities for existing clients by asking challenge questions that have been prearranged with the client and for applicants or clients by asking questions that require information beyond what is readily available from a wallet or a consumer credit report. [In addition, <i>describe any other steps the firm takes</i> ].
<i>Insert other Red Flags in this category based on the firm's own experience or its knowledge of likely new methods of identity theft.</i>	<i>Insert how you would detect these Red Flags you have identified.</i>
<b>Category: Suspicious Account Activity</b>	
19. Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	We will verify change of address requests by sending a notice of the change to both the new and old addresses so the client will learn of any unauthorized changes and can notify us. [In addition, <i>describe any other steps the firm takes</i> ].
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.	We will review new account activity to ensure that first and subsequent payments are made, and that credit is primarily used for other than cash advances and securities easily converted into cash. [In addition, <i>describe any other steps the firm takes</i> ].
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	We will review our accounts on at least a monthly basis and check for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or a big change in spending or electronic fund transfers. [In addition, <i>describe any other steps the firm takes</i> ].
22. An account that is inactive for a long time is suddenly used again.	We will review our accounts on at least a monthly basis to see if long inactive accounts become very active. [In addition, <i>describe any other steps the firm takes</i> ].
23. Mail our firm sends to a client is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account and immediately check the account's activity. [In addition, <i>describe any other steps the firm takes</i> ].
24. We learn that a client is not getting his or her paper account statements.	We will record on the account any report that the client is not receiving paper statements and immediately investigate them. [In addition, <i>describe any other steps the firm takes</i> ].
25. We are notified that there are unauthorized charges or transactions to the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report. [In addition, <i>describe any other steps the firm takes</i> ].
<i>Insert other Red Flags in this category based on the firm's own experience or its knowledge</i>	<i>Insert how you would detect these Red Flags you have identified.</i>

<i>of likely new methods of identity theft.</i>	
<b>Category: Notice From Other Sources</b>	
26. We are told that an account has been opened or used fraudulently by a client, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report. [In addition, <i>describe any other steps the firm takes</i> ].
We learn that unauthorized access to the client’s personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the client to learn the details of the unauthorized access to determine if other steps are warranted. [In addition, <i>describe any other steps the firm takes</i> ].
<i>Insert other Red Flags in this category based on the firm’s own experience or its knowledge of likely new methods of identity theft.</i>	<i>Insert how the firm would detect these Red Flags you have identified.</i>

**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.