

PRACTICE IDENTITY THEFT PREVENTION PROGRAM

PURPOSE

To establish an Identity Theft Prevention Program (Program) designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account, and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations (attached as Appendix 1 to this Program) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. This Program is limited to the scope defined above and is in addition to other programs or policies that the practice may have regarding legal requirements for proper handling and confidentiality of employee data, data security, client account information, access to practice records, and other security and privacy related programs or policies.

DEFINITIONS

Identify theft means fraud committed or attempted using the identifying information of another person without authority or consent.

A **covered account** means:

1. An account that a creditor offers or maintains, primarily for personal, family, or household purposes for a client that involves or is designed to permit multiple payments or transactions. Covered accounts include the extension of credit on an open account to clients; and
2. Any other account that a creditor offers or maintains for which there is a reasonably foreseeable risk to clients or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

THE PROGRAM

_____ (name practice) establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program includes reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to clients and to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

ADMINISTRATION OF PROGRAM

1. _____ (the practice governing body, an appropriate committee of the governing body, or a designated employee at the level of senior management) shall be responsible for the development, implementation, oversight and continued administration of the Program.
2. The practice shall train staff, as necessary, to effectively implement the Program; and
3. The practice shall exercise appropriate and effective oversight of service provider arrangements, where appropriate.

IDENTIFICATION OF RELEVANT RED FLAGS

1. The Program shall include relevant red flags from the following categories as appropriate:
 - a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - b. The presentation of suspicious documents related to covered accounts;
 - c. The presentation of suspicious personal identifying information related to covered accounts;
 - d. The unusual use of, or other suspicious activity related to a covered account; and
 - e. Notice from clients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:
 - a. The types of covered accounts offered or maintained;
 - b. The methods provided to open covered accounts;
 - c. The methods provided to access covered accounts; and
 - d. Its previous experience with identity theft.
3. The Program shall incorporate relevant red flags from sources such as:
 - a. Incidents of identity theft previously experienced;
 - b. Methods of identity theft that reflect changes in risk;
 - c. Applicable supervisory guidance, and
 - d. Supplement A to Appendix A of Part 681, referenced in Appendix 1 to this Program.

DETECTION OF RED FLAGS

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts by:

1. Obtaining identifying information about, verifying the identity of and authority of, a person opening a covered account;
2. Authenticating clients, monitoring transactions, and verifying the validity of change of address requests, or other changes, in the case of existing covered accounts; and

3. Verifying the authority of individuals having access to or using covered accounts, particularly in situations where the covered account relates to a corporation, partnership, limited liability company, or other legal entity, which is not an individual.

RESPONSE TO RED FLAGS

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;
2. Contact the client;
3. Change any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopen a covered account with a new account number;
5. Not open a new covered account;
6. Close an existing covered account;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.

UPDATING THE PROGRAM

The Program shall be updated periodically to reflect changes in risks to clients or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the organization offers or maintains;
5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

OVERSIGHT OF THE PROGRAM

1. Oversight of the Program shall include:
 - a. Assignment of specific responsibility for implementation of the Program;
 - b. Review of reports, if any, prepared by staff regarding compliance;
 - c. Approval of material changes to the Program as necessary to address changing risks of identity theft; and

- d. Preservation and retention of documentation of activities by responsible staff in a central location demonstrating compliance with the Program in case of audit, and to prepare required internal reports.
2. Reports shall be prepared as follows:
 - a. Staff responsible for development, implementation and administration of the Program shall report to _____ (the practice governing body, an appropriate committee of the governing body, or a designated employee at the level of senior management) at least annually on compliance by the organization with the Program.
 - b. The report shall address material matters related to the Program and evaluate issues such as:
 - i. The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - ii. Service provider agreements;
 - iii. Significant incidents involving identity theft or attempted identity theft and management's response; and
 - iv. Recommendations for material changes to the Program.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The practice shall take steps to ensure that the activity of any service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. Such service providers may include collection agencies or insurance companies.

DUTIES REGARDING ADDRESS DISCREPANCIES

The practice shall develop policies and procedures designed to enable the practice to form a reasonable belief that a credit report used by the practice, if any, relates to the consumer for whom it was requested if the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report. The practice may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the client;
2. Review of the practice records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the practice shall furnish the client's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The practice establishes a continuing relationship with the client; and
2. The practice regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.