Red Flags Rule Identity Theft Prevention Program Master Policy

by Dana B. Rosenfeld, Alysa Z. Hutnik, and Carmen Tracy, Kelley Drye & Warren LLP

Maintained • USA (National/Federal)

Related Content

A master policy setting up the framework for developing, implementing, updating, and administering a written identity theft prevention program required by the Federal Trade Commission's (FTC) Red Flags Rule. This Standard Document has integrated notes with important explanatory and drafting tips.

Red Flags Rule Identity Theft Prevention Program
Master Policy

Note: *Read This Before Using Document*

Definitions

- "**Covered Account**" means:
  - an account that [COMPANY] offers or maintains, primarily for personal, family, or household purposes, and which involves or is designed to permit multiple payments or transactions; or
  - any other account that [COMPANY] offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of [COMPANY] from Identity Theft.

Note: *Covered Account*

- "**Red Flag**" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
- "**Identity Theft**" means a fraud committed or attempted using the Identifying Information of another person without authorization.
- "**Identifying Information**" includes any name or number that may be used, alone or with other information, to identify a specific person, including:
  - Name, Social Security number, date of birth, government-issued identification number, alien registration number, government passport number, employer, or taxpayer identification number;
  - Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
  - Unique electronic identification number, address, or routing code; or
  - Telecommunications identifying information or access device.
- "**Service Provider**" means a person or business that provides a service directly to [COMPANY] involving Covered Accounts.

Purpose

The purpose of [COMPANY]'s Identity Theft Prevention Program is to ensure that [COMPANY] has in place reasonable policies and procedures that are designed to detect, prevent, and mitigate Identity Theft in connection with the opening of a Covered Account or any existing Covered Account, in

compliance with the Federal Trade Commission's (FTC) Red Flags Rule found at 16 C.F.R. Part 681.

These policies and procedures should be designed to accomplish the following objectives:

- Identify relevant Red Flags for the Covered Accounts that [COMPANY] offers or maintains, and incorporate those Red Flags into the Identity Theft Prevention Program.
- Detect Red Flags that have been incorporated in the Identity Theft Prevention Program.
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft.
- Ensure that the Identity Theft Prevention Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of [COMPANY] from Identity Theft.
- Establish the framework to be used and principles to guide the development and implementation of, and updates to, [COMPANY]'s Identity Theft Prevention Program, and the key roles in administering and in preparing the annual report on the program.
- Track and document [COMPANY]'s Identity Theft prevention, detection, and mitigation activities.

Note: ***Purpose***

Scope

What: This Master Policy applies to all of [COMPANY]'s administrative, technical, and physical policies, procedures, and practices concerning the opening and maintenance of Covered Accounts that relate to the prevention, detection, and mitigation of Identity Theft.

Who: The development, implementation, maintenance, and execution of the Identity Theft Prevention Program are the joint responsibility of [MAIN RESPONSIBLE GROUP AT COMPANY] [and a cross-functional FACTA Red Flags core team, including representatives from information technology (IT), information security, legal, marketing, and product development], and each employee who has duties under the applicable policies, procedures, and practices relating to Covered Accounts. Employees are expected to cooperate fully with any Red Flags assessment being conducted as part of the Identity Theft Prevention Program in departments or divisions for which they are accountable. Employees are further expected to work with the [MAIN RESPONSIBLE GROUP AT COMPANY] [and the cross-functional FACTA Red Flags core team] to develop any required Identify Theft prevention, detection, or mitigation plans.

Note: ***Scope***

Guidelines for Identifying Red Flags

In designing and updating the Identity Theft Prevention Program, consideration should be given to:

- The types of Covered Accounts offered or maintained by [COMPANY];
- The methods used to open Covered Accounts;
- The methods provided to access Covered Accounts; and
- [COMPANY]'s previous experiences with Identity Theft.

Further, when incorporating Red Flags into the Identity Theft Prevention Program, consideration should be given to:

- Identity Theft incidents that [COMPANY] has incurred or has identified as a potential risk;
- Applicable supervisory guidance, notifications, alerts, or warnings issued by the FTC, the national credit reporting agencies, law enforcement, or others as applicable;
- The presentation of suspicious documents;
- The presentation of suspicious personal Identifying Information;
- The unusual use of, or other suspicious activity related to, a Covered Account;
- Notice from customers, victims of Identity Theft, law enforcement authorities, consumer reporting agencies, or other persons regarding possible Identity Theft in connection with Covered Accounts; and

- Those Red Flags that are relevant to [COMPANY], which have been identified by the FTC in 16 C.F.R. Part 681, Supplement A to Appendix A[, a copy of which is attached].

All identified Red Flags deemed relevant to [COMPANY] should be documented in the Red Flags Tracking Spreadsheet (referenced at the end of this policy).

Note: *Guidelines for Identifying Red Flags*

Guidelines for Detecting Red Flags

The policies, procedures, and practices of the Identity Theft Prevention Program must address the relevant Red Flags that [COMPANY] may detect in connection with opening Covered Accounts or activity related to existing Covered Accounts. These include, but are not limited to:

- Obtaining Identifying Information about, and verifying the identity of, a person opening a Covered Account; and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests for existing Covered Accounts.

Note: *Guidelines for Detecting Red Flags*

Guidelines for Preventing and Mitigating Identity Theft

The policies, procedures, and practices of the Identity Theft Prevention Program should provide for responses to the detected Red Flags that are appropriate when balanced against the degree of risk posed. In determining an appropriate response, consideration should be given to any aggravating factors that may increase the risk of Identity Theft, such as a data breach or phishing or pretexting occurrence (for example, where a bad actor convinces an employee to provide sensitive customer information).

Processes identified as a means of preventing and mitigating Identity Theft in relation to identified Red Flags should be documented in writing in the Red Flags Tracking Spreadsheet (referenced at the end of this policy) and in any written policies or procedures, as needed.

Note: *Guidelines for Preventing and Mitigating Identity Theft*

Service Provider Arrangements

When [COMPANY] engages a service provider to perform an activity in connection with Covered Accounts, steps must be taken to help confirm that the service provider's activity is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. These steps include requiring the service provider by written contract to:

- Have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities using the same standards [COMPANY] would take if performing the tasks itself; and
- To either report any identified Red Flags to [COMPANY], or take appropriate steps to prevent or mitigate Identity Theft.

[GROUP IN CHARGE OF SERVICE PROVIDER ARRANGEMENTS] is responsible for identifying all applicable service provider arrangements and confirming that they meet these requirements.

Note: *Service Provider Arrangements*

Updating the Identity Theft Prevention Program

The [MAIN RESPONSIBLE GROUP AT COMPANY] [and the cross-functional FACTA Red Flags core team] shall periodically (but no less than annually, and preferably at least each quarter and prior to any significant change in pertinent business processes or systems) determine whether the Identity Theft Prevention Program requires modification. As part of this determination, consideration should be given to changes in the following activities or processes:

- The types of accounts [COMPANY] offers or maintains;
- Methods [COMPANY] uses to open or access Covered Accounts;
- [COMPANY]’s previous experiences with Identity Theft;
- [COMPANY]’s methods to detect, prevent, and mitigate Identity Theft; and

- [COMPANY]’s business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Any recommended changes to the Identity Theft Prevention Program, and the reasons and plans for making such changes, should be documented in the Red Flags Tracking Spreadsheet (referenced at the end of this policy).

Note: ***Updating the Identity Theft Prevention Program***

Approval and Administration of the Identity Theft Prevention Program

[COMPANY]'s Board of Directors or an appropriate committee of the Board of Directors must approve the initial written Identity Theft Prevention Program. Thereafter, the Identity Theft Prevention Program will be a dynamic program that is updated as appropriate. The Board of Directors, an appropriate committee thereof, or a designated employee at the level of senior management shall be involved in the oversight, development, implementation, and administration of the Identity Theft Prevention Program.

As part of these oversight obligations, the Board of Directors, an appropriate committee thereof or a designated employee at the level of senior management shall:

- Assign specific responsibility for the Identity Theft Prevention Program's implementation;
- Review reports prepared by personnel regarding compliance with the Red Flags Identity Theft Prevention Program requirements;
- Approve material changes to the Identity Theft Prevention Program as necessary to address changing Identity Theft risks; and
- Confirm there is appropriate and effective oversight of service provider arrangements.

In addition, [COMPANY] shall train its personnel, as necessary, to effectively implement the Identity Theft Prevention Program.

Note: ***Approval and Administration of the Identity Theft Prevention Program***

Annual Compliance Report

Designated personnel responsible for the development, implementation, and administration of the Identity Theft Prevention Program must report to the Board of Directors, an appropriate committee thereof or a designated employee at the level of senior management, at least annually, on [COMPANY]’s compliance with the Identity Theft Prevention Program requirements. The annual report must address:

- The effectiveness of [COMPANY]'s 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, that is, a written review of what [COMPANY] has put in place, and how effective these policies and procedures have been in detecting, preventing, and mitigating Identity Theft risks over the past year;
- Service provider arrangements;
- Significant incidents involving Identity Theft from the past year (if any), and management's response to such incidents; and
- Recommendations for any material changes to the Identity Theft Prevention Program.

Note: ***Annual Compliance Report***

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

- Version 1 approved on [DATE].

Supporting Documents

- Red Flags Tracking Spreadsheet [OR OTHER DOCUMENT]
- [16 C.F.R. Part 681, Appendix A]
- [POLICY AND PROCEDURE DOCUMENTS THAT RELATE TO THIS MASTER POLICY, INCLUDING A CURRENT LIST OF RELEVANT RED FLAGS AND POLICIES THAT ADDRESS HOW TO RESOLVE IDENTIFIED RED FLAGS]

Note: ***Supporting Documents***

PRODUCTS

PLC US Corporate and Securities, PLC US Finance, PLC US Financial Services, PLC US Intellectual Property and Technology, PLC US Law Department