DOCUMENTS

Red Flags Rule Identity Theft Prevention Program Master Policy

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 Red Flags Rule. This Standard Document has integrated notes with important explanatory and drafting tips. It can be used as a stand-alone document or as part of an existing compliance policy.

Dana B. Rosenfeld, Alysa Zeltzer Hutnik & Christopher M. Loeffler, Kelley Drye & Warren LLP

DRAFTING NOTE

GENERAL

LEGAL ISSUES

The Red Flags Rule, issued by the Federal Trade Commission (FTC) (jointly with the federal bank regulatory agencies), implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). It requires "financial institutions" and "creditors" with "covered accounts" (as defined in the Red Flags Rule) to develop a written program that identifies and detects the relevant warning signs, or "red flags," of identity theft (see the FTC's *Red Flags Rule, 16 C.F.R. § 681.1*). Red flags can include, for example:

- Unusual account activity.
- Fraud alerts on a consumer report.
- Attempted use of suspicious account application documents.

The Red Flags Rule's definition of "creditor" is broad and includes any entity that regularly extends or renews credit and includes all entities that regularly permit deferred payment for goods or services. For financial institutions and creditors subject to the FTC's jurisdiction, compliance with the rule currently is required by June 1, 2010 (the rule has been in effect since November 1, 2008 for institutions subject to the oversight of the federal bank regulatory agencies).

The written identity theft prevention program must include "reasonable policies and procedures" appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities to:

- Identify relevant red flags for the covered entity.
- Detect red flags.
- Respond to red flags.
- Ensure the program is updated periodically.

The FTC's Red Flags Rule also requires that:

- The program include certain administrative components, such as approval of the program by the covered entity's board of directors.
- Each covered entity considers the guidelines in *16 C.F.R. § 681, Appendix A* and include in its program those guidelines that are appropriate.

The FTC provides further information on its website (see *ftc.gov*).

DRAFTING ISSUES

This master policy sets out the framework for developing, implementing, updating and administrating a written identity theft prevention program for financial institutions and creditors that come under the jurisdiction of the FTC. It anticipates that the specific policies and procedures appropriate to the size and complexity of the covered entity's business will necessarily be developed and implemented in accordance with the master policy.

This master policy can be drafted as a comprehensive, stand-alone document or as a section of an existing compliance policy or data privacy and security policy. Companies should ensure that employees have been trained on and agree to follow the policy as appropriate. This might include, for example, incorporating an acknowledgement section in the policy or as part of a larger policy or handbook confirming the employee's receipt and understanding of the policy requirements, requiring web training and completion confirmation and/or performing random audits of policy effectiveness to determine whether further steps are needed to ensure compliance.

DEFINITIONS

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

DRAFTING NOTE

COVERED ACCOUNT

The Red Flags Rule defines a "covered account" as:

- An account used mostly for personal, family or household purposes that involves multiple payments or transactions. Examples include:
  - credit card accounts;
  - mortgage accounts;
  - cell phone accounts; and
  - utility accounts.
- Any other account for which there is a "reasonably foreseeable risk of identity theft."

(*16 C.F.R. § 681.1(b)(3).*)

The definition of "covered accounts" in the master policy should be appropriately tailored to reflect the types of covered accounts the covered entity maintains.

- **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 authority. Identifying information includes any name or number that may be used 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, or telecommunications identifying information or access device.
- **Service Provider** means a person or business that provides a service directly to [COMPANY NAME] involving Covered Accounts.

PURPOSE

The purpose of [COMPANY NAME]'s Identity Theft Prevention Program is to ensure that [COMPANY NAME] 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 Red Flags Rule, 16 C.F.R. § 681.1.

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

- Identify relevant Red Flags for the Covered Accounts that [COMPANY NAME] 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 the Company from identity theft;
- Establish the framework to be used and principles that guide the development, implementation and updates to [COMPANY NAME]'s Identity Theft Prevention Program, as well as the key roles in administering and in preparing the annual report on the program; and
- Track and document appropriate identity theft prevention, detection and mitigation activities.

DRAFTING NOTE

PURPOSE

This paragraph describes the purpose of the policy. It is helpful to provide context for the policy and to reinforce the culture of awareness necessary for an effective identity theft prevention program.

SCOPE

What: This Master Policy applies to all of [COMPANY NAME]'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, updates and execution of the Identity Theft Prevention Program are the joint responsibility of [IDENTIFY MAIN RESPONSIBLE GROUP AT COMPANY] [and representatives of the cross-functional FACTA Red Flags core team], as well as each employee with responsibilities under 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 will be held accountable. Employees are further expected to work with the [IDENTIFY MAIN RESPONSIBLE GROUP AT COMPANY] [and the cross-functional FACTA Red Flags core team] in the development of any required identify theft prevention, detection or mitigation plans.

DRAFTING NOTE

SCOPE

This paragraph sets out the activities of the covered entity to which the master policy applies. It also identifies the business groups and employees responsible for the program. All employees that have responsibilities in connection with the identity theft prevention program or under any applicable policies, procedures or practices relating to covered accounts should receive a copy of the master policy.

This section should be revised to identify the main group at the covered entity responsible for development, implementation and administration of the identity theft prevention program, and, if applicable, the covered entity's Red Flags Rule core team.

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 NAME];
- The methods used to open Covered Accounts;
- The methods provided to access Covered Accounts; and
- [COMPANY NAME]'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 NAME] 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 or other persons regarding possible identity theft in connection with Covered Accounts; and

- Those Red Flags that are relevant to [COMPANY NAME], which have been identified by the FTC in 16 C.F.R. Part 681, Supplement A to Appendix A, [available by clicking here [INSERT LINK HERE TO ELECTRONIC VERSION OF RULE]/a copy of which is attached].

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

DRAFTING NOTE

GUIDELINES FOR IDENTIFYING RED FLAGS

When assessing the relevant red flags, the Red Flags Rule requires the covered entity to consider the nature of its business and the type of identity theft to which its customers may be subject. The written identity theft program should also include any relevant red flags identified by the FTC in Supplement A to Appendix A of 16 C.F.R. § 681, which are grouped into five categories:

- 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 or other persons regarding possible identity theft in connection with covered accounts.

The red flags identified by the covered entity should be listed on a spreadsheet or other document and attached to the master policy (for example, see below *Guidelines for Detecting Red Flags and Supporting Documents*). The rule requires that the covered entity continuously update the list of red flags, and this should be made part of the update process outlined below in *Updating the Identity Theft Prevention Program*.

GUIDELINES FOR DETECTING RED FLAGS

The policies, procedures and/or practices of the Identity Theft Prevention Program must address the detection of Red Flags 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.

DRAFTING NOTE

GUIDELINES FOR DETECTING RED FLAGS

The Red Flags Rule requires that the program include "reasonable policies and procedures" for detecting red flags. The Red Flags Rule guidelines suggest that for new covered accounts, these procedures would include controls for obtaining and verifying the identity of persons opening a new covered account. For existing covered accounts, covered entities should include controls for:

- Authenticating customers.
- Monitoring change of address requests.
- Verifying the validity of change of address requests.

(*16 C.F.R. Part 681, Appendix A.*)

GUIDELINES FOR PREVENTING AND MITIGATING IDENTITY THEFT

The policies, procedures and/or practices of the Identity Theft Prevention Program should provide for responses to the Red Flags detected 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/pretexting" occurrence. 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.

DRAFTING NOTE

GUIDELINES FOR PREVENTING AND MITIGATING IDENTITY THEFT

Under the Red Flags Rule, covered companies must implement "reasonable policies and procedures" to appropriately respond to any detected red flags. The appropriate response should take into account the level of risk posed by the particular red flag, and may include, for example, one or more of the following:

- Monitoring a covered account for identity theft.
- Contacting the customer.
- Changing passwords and security codes or other security devices that permit access to a customer's account.
- Reopening a covered account with a new account number.

- Not opening a covered account.
- Closing an existing account.
- Not attempting to collect on a covered account or not selling a covered account to a debt collector.
- Notifying law enforcement.
- Determining that no response is warranted under the particular circumstances.

(*16 C.F.R. Part 681, Appendix A.*)

The covered entity must also take into account any responses legally required under other laws or regulations.

This policy contemplates that the appropriate responses determined by the covered entity will be documented in writing and included in a tracking spreadsheet to be attached to the policy (see below *Supporting Documents*).

SERVICE PROVIDER ARRANGEMENTS

When [COMPANY NAME] 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; and
- To either report any identified Red Flags to [COMPANY NAME], or take appropriate steps to prevent or mitigate identity theft.

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

DRAFTING NOTE

SERVICE PROVIDER ARRANGEMENTS

The Red Flags Rule requires that covered entities "exercise appropriate and effective oversight of service provider arrangements" (*16 C.F.R. § 681(e)(4)*). As described in this paragraph, this oversight could include contractually requiring service providers to have appropriate procedures in place to detect red flags and report them to the covered entity. This paragraph also serves to identify the covered entity's business group or team responsible for this oversight.

UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The [IDENTIFY MAIN RESPONSIBLE GROUP AT COMPANY] [and the cross-functional FACTA Red Flags core team] shall periodically (but no less than annually,

and preferably each quarter) 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 NAME] offers or maintains;
- Methods [COMPANY NAME] uses to open or access Covered Accounts;
- [COMPANY NAME]'s previous experiences with identity theft;
- [COMPANY NAME]'s methods to detect, prevent and mitigate identity theft; and
- [COMPANY NAME]'s business arrangements, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

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

DRAFTING NOTE

UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The Red Flags Rule requires that the written identity theft prevention program be updated periodically. This master policy provides that the policy will be updated no less than once per year and includes a list of activities or processes that should be considered when reviewing and updating the program.

APPROVAL AND ADMINISTRATION OF THE IDENTITY THEFT PREVENTION PROGRAM

The initial written Identity Theft Prevention Program must be approved by [COMPANY NAME]'s Board of Directors or an appropriate committee of the Board of Directors. 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 the 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, personnel shall be trained, as necessary, to effectively implement the Identity Theft Prevention Program.

DRAFTING NOTE

APPROVAL AND ADMINISTRATION OF THE IDENTITY THEFT PREVENTION PROGRAM

The Red Flags Rule includes certain requirements regarding approval and administration of the written identity theft prevention program. In particular, the Red Flags Rule requires that:

- The initial written program be approved by the covered entity's board of directors or an appropriate board committee. For those companies without boards, a member of senior management must approve the program, in which case, the first sentence of this paragraph must be modified to reflect that.
- A specific staff member be assigned to oversee implementation of the policy and procedures.
- The covered entity monitor its services providers.
- Relevant staff receive training on policy and procedures.

(16 C.F.R. §681, Appendix A.)

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 compliance by [COMPANY NAME] with the Identity Theft Prevention Program requirements. The Annual Report must address:

- The effectiveness of [COMPANY NAME]'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 (i.e., a written review of what [COMPANY NAME] 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 material changes to the Identity Theft Prevention Program.

DRAFTING NOTE

ANNUAL COMPLIANCE REPORT

This paragraph reflects the Red Flags Rule guideline that responsible staff report annually on matters related to the program to the board of directors or an appropriate committee of the board of directors. If a covered entity does not have a board of directors, the report should be made to a member of senior management. The categories of items that the Red Flags Rule suggests the report cover are listed in this paragraph. *(16 C.F.R. §681, Appendix A.)*

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
- [16 C.F.R. Part 681, Appendix A]
- [LIST ALL POLICY/PROCEDURE DOCUMENTS THAT RELATE TO THE MASTER POLICY, INCLUDING POLICIES THAT ADDRESS HOW TO RESOLVE IDENTIFIED RED FLAGS]

AUTHORS

Dana B. Rosenfeld, Alysa Zeltzer Hutnik and Christopher M. Loeffler are attorneys in Kelley Drye & Warren LLP's Washington, D.C. office. Dana is Chair of the Privacy and Information Security practice group. They counsel clients on all facets of privacy, data security and consumer protection issues at the federal and state level.

Dana B. Rosenfeld
Partner
KELLEY DRYE & WARREN LLP

Alysa Zeltzer Hutnik
Associate
KELLEY DRYE & WARREN LLP

Christopher M. Loeffler
Associate
KELLEY DRYE & WARREN LLP

Article photo by Jonathan Gayman/Flickr/Getty Images.