

Identity Theft Prevention Program

I. PROGRAM PURPOSE AND DEFINITIONS

The purpose of this Identity Theft Prevention Program (“Program”) is to detect, prevent and mitigate identity theft in connection with a Covered Account.

A. Fulfilling requirements of the Red Flags Rule

The purpose of this Identity Theft Prevention Program (“Program”) is to detect, prevent and mitigate identity theft in connection with a Covered Account.

The Program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags as defined in the Rule and this Program for new and existing covered accounts 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. Update the Program periodically to reflect changes in risks to customers or to the safety and soundness of our Organization from identity theft.

B. Red Flags Rule definitions used in this Program

For the purposes of this Program, the following definitions apply:

1. Account. "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
2. Covered Account. A “Covered account” includes any account that involves or is designed to permit multiple payments and/or transactions. This Program covers every new and existing customer account that meets the following criteria:
 - a. Business, personal, and household accounts for which there is a reasonably foreseeable risk of identity theft to our customers or to the safety and/or soundness of our Organization from Identity Theft.
3. Creditor. "Creditor" includes a person or entity that arranges for the extension, renewal or continuation of credit, including our Organization.
4. Customer. A "customer" means a person or business entity that has a covered account with our Organization.

5. Identifying Information. "Identifying information" means 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, checking or savings account numbers, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number or unique electronic identification number.
6. Identity Theft. "Identity Theft" means fraud committed using the identifying information of another person.
7. Red Flag. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
8. Service Provider. "Service provider" means a person or business entity that provides a service directly to our Organization relating to or connection with a covered account.

II. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, our Organization shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. Our Organization identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Documents provided for identification that appears to be forged, altered or inauthentic;
2. Photograph or physical description on the identification that is not consistent with the person presenting the document;
3. Other information on the identification that is not consistent with existing customer information (such as a person's signature on a check appears forged); and
4. Application and/or contract for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a driver's license);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. Failing to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. Identifying information which is not consistent with the information that is on file for the customer.

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to our Organization that a customer is not receiving mail sent by our Organization;
6. Notice to our Organization that an account has unauthorized activity;
7. Change of billing address to address different from where service is received;
8. Establishment of residential account under business name;
9. Breach in our Organization's computer system security; and
10. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to our Organization from a customer, a victim of identity theft, a law enforcement authority or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

III. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, we will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, our Organization will take the following steps to monitor transactions with an account:

Detect Red Flags

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking and/or credit card information given for billing and payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event any identified Red Flag is detected, the involved personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate Identity Theft

1. Monitor a covered account for evidence of Identity Theft;
2. Contact the customer with the covered account;
3. Change any passwords or other security codes and devices that permit access to a covered account;
4. Not open a new covered account;
5. Close an existing covered account;
6. Reopen a covered account with a new number;

7. Not attempt to collect payment on a covered account;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement; or
10. Determine that no response is warranted under the particular circumstances.

Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to our Organization accounts, the Organization shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the Organization website, if applicable, but provide clear notice that the website is not secure;
2. Undertake complete and secure destruction of paper documents and computer files containing customer information;
3. Make office computers password protected and provide that computer screens lock after a set period of time;
4. Keep offices and work areas clear of papers containing customer identifying information;
5. Lock any file cabinets, desk drawers and any other storage space containing documents with customer identifying information;
6. Request only the last 4 digits of social security numbers (if any);
7. Maintain computer virus protection up to date; and
8. Require and keep only the kinds of customer information that are necessary for our Organization purposes.

V. PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to our customers and to the safety and soundness of our Organization from Identity Theft. The Program Administrator shall at least annually consider our Organization's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts that our Organization maintains and changes in our Organization's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update and implement.

VI. PROGRAM ADMINISTRATION

A. Oversight

The Program Administrator shall be responsible for developing, implementing and updating the Program. The Program Administrator shall be responsible for the Program administration, for appropriate training of our Organization 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.

B. Staff Training and Reports

Any of our staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, in the responsive steps to be taken when a Red Flag is detected and in the reports to be prepared on incidents of Identity Theft. The Program Administrator may request that staff provide opinions regarding the effectiveness of our Organization's Program and recommendations for improvement.

C. Service Provider Arrangements

If our Organization engages a service provider to perform an activity in connection with one or more covered accounts, the Organization shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require that service providers acknowledge receipt and review of our Program and agree to perform its activities with respect to our Organization covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program;

OR

2. Require that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to our Organization covered accounts in compliance with the terms and conditions of the service provider's identity theft prevention program and will take appropriate action to prevent and mitigate identity theft; and that the service providers agree to report promptly to the Organization in writing if the service provider in connection with our Organization's covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.