

Identity Theft Prevention Program

Objective

Red flags are suspicious patterns or practices, or specific activities, that indicate the possibility of identity theft. To comply with the Federal Red Flags Rule, we have implemented a program to identify, detect and respond to the indicators of identity theft. This program includes reasonable policies and procedures, assigns specific oversight, trains staff, and audits compliance to accomplish the following:

1. Identify Red Flags
2. Detect and evaluate Red Flags
3. Respond to Red Flags;
4. Update this program periodically to reflect changes in risks to our customers and to the safety and soundness of our company from identity theft.

“Red Flags” are designed to detect, prevent, and mitigate identity theft in connection with the gathering of information used in the opening of a covered account or the maintenance of an existing covered account.

Applicability

All accounts who make multiple payments and/or provide this organization with personal information are considered “covered accounts”. All employees of this organization are considered “covered staff”.

Administration

Senior management will approve development, implementation and staff training of this program. The Operations Manager (Program Coordinator) will be responsible for the day-to-day administration.

The Program Coordinator will develop this program using policies and procedures believed to be effective at identifying Red Flags associated with a reasonably foreseeable risk of identity theft.

The Program Coordinator will train staff with regard to their duties involving use and maintenance of non-public customer information.

The Program Coordinator will reevaluate and update the program on an annual basis or as needed during the year.

The Program Coordinator will prepare a report that will address matters such as:
Significant incidents involving identity theft and the companies’ response.
Recommendations necessary for changes to keep the program effective.

IDENTIFYING RED FLAGS

Alerts, notifications or other warnings received from consumer reporting agencies. These may include:

A fraud or active duty alert included with a consumer report.

A consumer-reporting agency provides a notice of address discrepancy.

A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of this particular applicant or customer.

A recent and significant increase in the volume of inquiries.

An unusual number of recently established credit relationships.

Presentation of suspicious documents. These may include:

The photograph or physical description on the identification is not consistent with information provided by the person presenting the application.

If the application appears to have been altered or forged or the consumer's identification appears to be forged or is inconsistent with the information on the application it may be a red flag.

Personal identifying information provided by the customer is inconsistent when compared against external information sources used by the company, for example:

The address provided on the application does not match any address in the customer's consumer report.

The Social Security Number has never been issued, or is listed on the Social Administration's Death Master File.

There is a lack of correlation between the Social Security Number range and date of birth.

The first three digits of a Social Security Number indicates the state of origin, if suspicious, ask questions.

The address on an application is invalid, a mail drop or a prison.

The phone number is invalid, or is associated with a pager or answering service.

"Synthetic" ID theft is where the thief uses another person's Social Security number but uses a different name, address, and birth date to establish credit accounts with the three national credit bureaus. Unfortunately, credit bureaus establish files for multiple consumers under the same Social Security number so it sometimes goes undiscovered. Unlike "true name" ID thieves, synthetic ID thieves generally are people trying to live under a fake identity, such as illegal immigrants, criminals, or people on the run. Many synthetic ID thieves make payments for a period of time before going delinquent or just disappearing, with or without the vehicle. Be sure to examine any patterns, practices, or activities that may suggest the customers were synthetic ID thieves before they stop paying and disappear.

Notice from other sources:

Sometimes a red flag that an account has been opened or used fraudulently can come from a customer, a victim of identity theft, a law enforcement authority or someone else.

DETECTING AND EVALUATION

All credit applications will be complete and will always include the following minimal information:

- Name
- Date of birth
- Address of current and previous residence
- Social Security Number
- Valid Drivers License or ID card issued by DMV
- Address and contact number of current employer

Acceptable documentation for identity verification purposes include:

Check Drivers License with DMV records.

Verify that applicant and the Drivers License are in fact the same person.

Check SSN against the credit report to determine whether the SSN is associated with fraud or identity theft.

Proof of current address such as utility bill or lease.

Verify any telephone numbers offered by applicant.

Check with the credit report that the address is not associated with more than one SSN.

Current pay stub from employer

Check that there is no match on the Office of Foreign Assets Control (OFAC) database provided either by an on-line service or through the Credit Report Service.

Responding to Red Flags

In the event a Red Flag is detected, the covered staff member will attempt to obtain additional information from the customer and acceptable third party sources to authenticate customer's identity.

In the event the covered staff is unable to reconcile a Red Flag with reasonable certainty, they should consult the Program Coordinator.

If a customer's identity cannot be authenticated with reasonable certainty, there will be no account opened.

Management will determine whether or not to notify law enforcement.

Maintenance of Covered Accounts

Only authorized staff will have access to files containing personal identifying information on customers.

Train relevant staff before authorizing them to have access to files containing personal identifying information.

All reports containing customer personal identity information will be shredded when no longer needed in the course of normal servicing activity (see program coordinator for minimum time requirement).

All service providers performing services for this organization will have identity theft policies in place and take appropriate steps to prevent or mitigate identity theft.

All consumer accounts will be updated with credit bureaus periodically as frequently as may be allowed. Any changes to the consumers address will be updated as required by law.

Change internal passwords, security codes, or other ways to access covered accounts on a regular basis.

Staff training:

All personnel will be indoctrinated upon hire and will be shown a copy of this Red Flags Program. They will be required to read it and sign an acknowledgment that they understand what they have read and that failure to protect the confidentiality of the information related to this organization or its clients may result in disciplinary actions or termination. From time to time new security items may be introduced to members of our staff.

Service provider confidentiality:

All service providers will be required to have their own satisfactory privacy procedures and Red Flags program in compliance with government regulations and will sign an agreement to keep all non-public information provided by us about our clients confidential.

Employee Confidentiality and Privacy Agreement

As an employee with this organization I am required to follow privacy procedures and protocols of this organization. In order to respect the privacy of this organization and of the clients that it represents, I agree to the following provisions of this agreement:

I have completely reviewed and I understand this organization's privacy policy as presented to me.

I understand the confidentiality and privacy procedures and protocols of this organization and do agree to comply with them;

I agree to protect this organization's proprietary information and all the non-public information of clients of this organization while I am employed and when I am no longer employed by this organization.

I also understand that failure to follow this agreement may result in disciplinary action or termination as deemed appropriate by this organization.

Signature of Employee

Printed Name

Position

Date

Provider: _____

Service Provider Confidentiality and Privacy Agreement

As a service provider for this organization I/we agree to follow the privacy procedures and protocols of this organization. Where required by law, I/we do certify that I/we have established my/our own privacy procedures. I/we agree to the following provisions of this agreement as required by this organization:

I/we have completely reviewed and do understand this organization's privacy policy as presented.

I/we understand the confidentiality and privacy procedures and protocols of this organization and do agree to comply with them;

I/we agree to protect all the non-public client information provided to me/us as a service provider and and keep it confidential even after such services have been terminated.

I/we also understand that failure to follow this agreement may result in legal actions or termination of any and all service provider agreements as deemed appropriate by this organization.

Signed On Behalf of Service Provider

Printed Name of Signer

Position

Date