**“Insert Company Here”  
  
  
  
  
Identity Theft and Red Flags Policy**

Effective Date: XXXXXX, XX, XXXX

**TABLE OF CONTENTS**

1. OVERVIEW 3

1.1 Policy Overview 3

1.2 Purpose 3

1.3 Scope 3

1.4 Related Documents 4

2. DEFINITIONS 4

3. REQUIREMENTS 5

3.1 Program requirements 5

3.2 Training 6

3.3 Monitoring and testing 7

3.4 Issue Management 7

3.5 Documentation and Record Retention 7

4. ROLES AND RESPONSIBILITIES 7

5. EXCEPTIONS 8

6. POLICY ADMINISTRATION 9

6.1 Effective Date 9

6.2 Document Management 9

6.3 Approval Management 9

# OVERVIEW

## 

## Policy Overview

[Insert Company Here] (“[Insert Company Here]” or the “Company”) is committed to preventing fraudulent use of personally identifiable information on its lending platform. This document (“Policy”) governs the oversight of the Identity Theft Red Flags used by [Insert Company Here] in connection with the lending program with [Insert Financial Institution Here] (“Bank”). This Policy also outlines the practices [Insert Company Here] uses to detect, prevent and mitigate instances of identity theft.

In November 2007, Federal Banking Agencies issued a set of regulations, known as the “Identity Theft Red Flags and Address Discrepancies Rule,” requiring that banks develop and implement written identity theft prevention and detection programs to protect consumers from identity theft. This rule implements sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), which amends the Fair Credit Reporting Act (“FCRA”).

[Insert Company Here] complies with all applicable laws, regulations and guidance pertaining to Identity Theft/Red Flags for regulated financial institutions.

## Purpose

The purpose of the Policy is to ensure that the risks related to Identity Theft Red Flags are understood and managed in a systematic fashion that is compliant with Bank policy, applicable laws, regulations and guidance, and serves the best interests of [Insert Company Here], the Bank, and consumers. This Policy is intended to assist [Insert Company Here] in:

* Minimizing the threat of identity theft through disclosure or compromise of customer information held by the Company;
* Responding to known or suspected identity theft involving the Company or its customers;
* Aiding Company customers who may have been victims of identity theft;
* Establishing processes or procedures for training Company personnel; and
* Establishing processes or procedures for educating Company customers.

Except where specifically addressed herein, this Policy follows the Roles and Responsibilities, Training, Monitoring and Testing, Issue Management, and Document and Record Retention sections in the Compliance Management System Policy (“CMS”).

## Scope

This Policy governs all aspects of [Insert Company Here]’s Red Flags/Identity Theft Program (“Program”), and is applicable to all personnel at [Insert Company Here], including both employees and consultants. It is also applicable to all third parties with whom [Insert Company Here] has entered into business arrangements for ongoing operational activities. Third parties include, but are not limited to, dental office partnerships, bank partnerships, and service providers.

## Related Documents

### Related Policies and Procedures

* Compliance Management System Policy
* BSA/AML and OFAC Policy
* Data Handling and Retention Policy
* Identity Theft and Red Flags Procedure

### Applicable Law and Regulations

* Fair Credit Reporting Act (FCRA)
* Fair and Accurate Credit Transactions Act of 2003 (FACTA)

# DEFINITIONS

For the purposes of this policy, the following terms are defined –

A ***Credit Reporting Agency (“CRA”)*** is a company that collects credit information on individual consumers from various sources and provides that individual’s borrowing and bill-paying history to financial institutions, creditors, and others.

A ***Covered Account*** is any consumer account [Insert Company Here] offers on behalf of its banking partners primarily for personal, family or household purposes, that involves multiple payments or transactions, for which there is a reasonably foreseeable risk of identity theft. All [Insert Company Here] consumer accounts are covered accounts.

***Identifying Information*** encompasses any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.

***Identity Theft*** is fraud committed using the identifying information of another person.

A ***Red Flag*** is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

# REQUIREMENTS

The processes listed below constitute the required Program elements as executed day-to-day. Standards, requirements and execution steps are further defined in supporting procedures.

## Program requirements

**3.1.1 Periodic Review**. [Insert Company Here]’s Red Flag Policy will be reviewed by the Bank and submitted to the Bank for review and approval. In addition, the Bank will conduct period reviews of [Insert Company Here]’s practices in this area, and through ongoing testing and periodic site visits, will ensure the Policy and programs are properly followed.

**3.1.2 Policy Updates**. [Insert Company Here] will update this Identity Theft Red Flags Policy (including the Red Flags determined to be relevant) periodically, to reflect change in risks to customers or to the safety and soundness of [Insert Company Here] or the Bank from Identity Theft. [Insert Company Here] will use risk assessments and other policies, and work with the Bank to make changes that may be necessary to the Identity Theft prevention and detection programs that [Insert Company Here] has developed and implemented. [Insert Company Here] will manage and administer an Identity Theft/Red Flags Program that is specifically tailored to the needs and experience of the program administered by [Insert Company Here]. [Insert Company Here] will assign a qualified individual with responsibility and accountability for overseeing the program. Changes to [Insert Company Here]’s policy or program may be required based on factors, including, but not limited to:

* Previous experience with Identity Theft;
* Changes in methods to detect, prevent, and mitigate Identity Theft;
* Changes in types of accounts offered or maintained; and
* Changes in business arrangements between [Insert Company Here] and its partners

**3.1.3 Identity Theft Detection, Prevention and Mitigation**. [Insert Company Here] will adhere to the guidelines presented in Appendix J to the Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation. The Program shall include the following elements:

* Identification of relevant Red Flags;
* Detection of Red Flags that are part of the Program;
* Responding appropriately to any detected Red Flags to prevent and mitigate Identity Theft; and
* Ensuring the Program is updated periodically to reflect changes in risks

**3.1.4 Third Party Servicers**. [Insert Company Here]’s Program must also address the oversight of any third-party servicers that perform services in connection with Covered Accounts.

**3.1.5 Annual Reporting**. [Insert Company Here] will provide a report to the Bank on the effectiveness of its Identity Theft/Red Flags Policy no less than annually. The report provided to the Bank by [Insert Company Here] should address material matters related to the Program and evaluate issues such as:

* The effectiveness of the policies and procedure sin addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
* Service provider arrangements;
* Significant instances involving Identity Theft and management response; and
* Recommendations for material changes to the Program

**3.1.6 Program Categories**. The Rule requires all financial institutions and creditors to design and implement a risk-based program that is appropriate for the size, complexity, and nature of operations. Guidelines issues by the FDIC and other federal law enforcement agencies were used by [Insert Company Here] in designing its Program. A supplement to the Guidelines identifies 26 possible Red Flags. These Red Flags are not a checklist, but rather examples that may be used be used as a starting point in identifying concerns. [Insert Company Here]’s Program should ensure that they have appropriately addressed each of the five categories of Red Flags as necessary. These five categories are as follows:

* Alerts, notifications, or warnings from a CRA or other service provider;
* Suspicious Documents
* Suspicious personally identifying information, such as a suspicious address change
* Usual use of – or suspicious activity relating to – a Covered Account; and
* Notices from customers, victims of Identity Theft, law enforcement authorities, or other businesses about possible Identity Theft in connection with Covered Accounts.

In addition to addressing these five categories, [Insert Company Here]’s Program includes a requirement for annual review and approval of the Red Flags Program, designation of a Program Administrator, and mandatory annual training.

**3.1.7 Address Discrepancies**. On behalf of the Bank, [Insert Company Here] must also develop and implement reasonable processes and procedure designed to handle notices of address discrepancy received from CRAs. Whenever [Insert Company Here] receives a notice of address discrepancy in connection with a new or existing account, it must take action to resolve the discrepancy and form a reasonable belief that the consumer report related to the consumer whose report was requested. See Fair Credit Reporting Act Policy and associated procedures for additional information related to handling address discrepancies.

## Training

In accordance with the Compliance Management System Policy, all employees and, as appropriate, contractors and temporary staff receive training on the Red Flag Policy/Program at least annually. Additional training should occur commensurate with roles and responsibilities for personnel more actively involved in the execution and development of related-policies and procedures. Evidence of training is retained and made available upon request.

## Monitoring and testing

[Insert Company Here] maintains appropriate monitoring and testing to reasonably detect and prevent control design or effectiveness failures. Additionally, [Insert Company Here] will provide necessary reporting or data to the Bank in support of its monitoring and testing requirements. The Bank and [Insert Company Here] will work closely to ensure effective coordination and communication of such activities

## Issue Management

Issues or changes related to risk, process or control failures pertaining to Identity are tracked and managed by [Insert Company Here]. Issues logged have an owner, issue date, issue description, priority level, risk level, and an action plan for remediation, including a target date for closure. A summary of issues is reported to Risk Management Committee and the Bank on a monthly basis. Issues requiring action or management attention are managed through the issue escalation process.

## Documentation and Record Retention

All activities supporting adherence to this Policy are documented and retained for review by the Bank and external auditors, including federal and state regulators in compliance with *the Data Handling and Retention Policy*. This includes policies and procedure, risk assessments, monitoring reports, training materials, and issues that are currently opened or closed.

# 

# ROLES AND RESPONSIBILITIES

| **Responsible Party** | **Roles** |
| --- | --- |
| Risk Management Committee – Chief Executive Officer, Chief Risk Officer, Chief Compliance Officer, Chief Information Technology Officer | * Review this Policy, and either approve proposed changes or return to the Policy Owner for revision and resubmission * Provide oversight of the Company’s compliance with requirements outlined in this Policy, including monitoring and testing results, and recommendations for corrective action. |
| Policy Owner: Chief Compliance Officer | * Review and maintain this Policy and submit for approval to the Risk Management Committee; * Document, approve (if applicable), and report Policy exceptions to the Risk Management Committee; * Assist senior management in developing procedures and controls to implement the Policy (for example, changes in operating procedures, standards, guidelines, and technologies); * Provide reports to the Risk Management Committee regarding material noncompliance with respect to identity theft and red flags, as appropriate; * Engage Legal Counsel, as appropriate, to ensure Policy risks are appropriately evaluated; * Monitor implementation of and compliance with this Policy; and * Advise and support senior management, business units and service providers with respect to identity theft and red flags as appropriate |
| Business Lines and Service Providers | * Comply with the requirements of this Policy * Develop, implement and maintain procedures, processes, and controls to detect, prevent, and mitigate identity theft; * Resolve and escalate identity theft and red flags as appropriate; * Perform related responsibilities defined under the BSA/AML and OFAC Policy; * Escalate any questions or issues regarding this Policy or its implementation to the CCO; * Immediately notify the CCO if they become aware of a failure to comply with this Policy; * Immediately submit any conflicts between this Policy and [Insert Company Here]’s other legal obligations to the CCO; and * Ensure that employees receive adequate training on this Policy/Program for their roles and responsibilities. |
| Legal Counsel | * Provide direction to the CCO and business lines on interpreting [Insert Company Here]’s obligations under this Policy. |

# EXCEPTIONS

From time to time, [Insert Company Here] may reasonably determine that a Policy exception is warranted. All exceptions must be approved in writing by the Policy Owner and reported to both the Compliance Committee and the Risk Management Committee. The Risk Management Committee must be appraised of potential risks associated with the exception as well as any proposed actions for mitigating risks.

Notwithstanding the foregoing, under no circumstances does this Policy permit an exception that would result in a violation of law.

# POLICY ADMINISTRATION

## 

## Effective Date

## 

## Document Management

This section is intended to track minor updates. Minor updates to the Policy/Program may be approved by the chair of the responsible management committee.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modified Date** | **Modified By** | **Approved By** | **Revision** | **Version** |
|  | Chief Compliance Officer | Risk Management Committee |  | 1.1 |

## 

## Approval Management

(This section is intended to track formal approval dates/authority)

|  |  |  |
| --- | --- | --- |
| **Approved Date** | **Approved By** | **Version** |
|  | Risk Management Committee | 1.0 |