



COMPLYING WITH THE FTC “RED FLAGS” RULE

NLBMDA SAMPLE TEMPLATE TEXT AND WORK SHEETS FOR THE DESIGN AND IMPLEMENTATION OF A “RED FLAG IDENTITY THEFT PREVENTION PROGRAM”

SUMMARY

The Federal Trade Commission (FTC) has issued regulations (“Red Flags Rule”) requiring entities that meet the definition of “creditor” to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by November 1, 2008, and must provide for the identification, detection, and response to patterns, practices, or specific activities — known as “red flags” — that could indicate identity theft.

A business is a “creditor” if it:

- (1) regularly extends “credit,” including deferring payment by customers for the provision of goods and services; and
- (2) maintains a “covered account.”

The rule requires those creditors to develop a written program that identifies and detects the relevant warning signs — or “red flags” — of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the creditor, include appropriate staff training, and provide for oversight of any service providers.

The FTC defines a “creditor” as any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

Accepting credit cards as a form of payment does not in and of itself make an entity a creditor.

A “covered account” is an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

A covered account is also an account used for personal, family, or household purposes, and that involves multiple payments or transactions.

Additionally, a covered account includes credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

NLBMDA has developed "template text" for its members to develop a Red Flag Identity Prevention Program if covered under the Red Flag Rule. The provisions outlined below are intended to be as comprehensive as possible, and includes all requirements and examples that apply to creditors as provided by the Federal Trade Commission as of the last update of this document.

NLBMDA has also developed work sheets, including a sample compliance record and a sample Log to record the detection and response to Red Flags to suggest how member staff assigned to the Program may track Red Flags and document appropriate responses.

Note: This document and the following sample program and work sheets do not constitute legal advice. Individual circumstances may vary so members should seek the services of competent legal counsel for guidance.

SAMPLE “RED FLAG” IDENTITY THEFT PREVENTION PROGRAM (“PROGRAM”)

The following approved Program has been designed, and an appropriate employee at the level of senior management has been designated to its oversight, development, implementation and continued administration, to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

1. Program Purpose & Establishment

- 1.1. The Program is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.
- 1.2. The Program is appropriate to the size and complexity of the Company and the nature and scope of the Company's activities.
- 1.3. The design of the Program includes the incorporation, as appropriate, of existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the Company from identity theft.
- 1.4. The Program is updated (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the Company from identity theft, based on factors such as:
 - 1.4.1. The experiences of the Company with identity theft;
 - 1.4.2. Changes in methods of identity theft;
 - 1.4.3. Changes in methods to detect, prevent, and mitigate identity theft;
 - 1.4.4. Changes in the types of accounts that the Company offers or maintains; and
 - 1.4.5. Changes in the business arrangements of the Company, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

2. Administration of the Program

- 2.1. The Program is designed and administered in compliance with 16 CFR Part 681.2.
- 2.2. The initial Program has been approved by [the board of directors, or if no board of directors exists, an appropriate employee at the level of senior management].

- 2.3. An appropriate employee at the level of senior management has been designated to its oversight, development, implementation and continued administration of the Program.
- 2.4. The Program includes appropriate staff training.
- 2.5. The Program includes oversight of service provider arrangements, including steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
- 2.6. The Program includes the periodic determination of the offering or maintenance of a covered account.
- 2.7. The Program includes a risk assessment to determine whether a covered account has been offered or is maintained (as the term is defined in the Applicable Definitions section below), taking into consideration:
 - 2.7.1. The methods used to open a covered account;
 - 2.7.2. The methods provided to access a covered account; and
 - 2.7.3. Any previous experiences with identity theft.

3. Reports

- 3.1. Staff responsible for development, implementation, and administration of the Program reports to [the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management], at least annually, on compliance by the Company with 16 CFR 681.2.
- 3.2. The report addresses material matters related to the Program and evaluates issues such as:
 - 3.2.1. The effectiveness of the 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;
 - 3.2.2. Service provider arrangements;
 - 3.2.3. Significant incidents involving identity theft and management's response; and
 - 3.2.4. Recommendations for material changes to the Program.

4. Policies and Procedures

- 4.1. The Program's policies and procedures provide for appropriate responses to the Red Flags that have been detected that are commensurate with the degree of risk posed.
- 4.2. In determining an appropriate response, aggravating factors are considered that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the Company, or third party, or notice that a customer has provided information related to a covered account held by the Company to someone fraudulently claiming to represent the Company or to a fraudulent website.
- 4.3. Appropriate responses may include the following:
 - 4.3.1. Monitoring a covered account for evidence of identity theft;
 - 4.3.2. Contacting the customer;
 - 4.3.3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
 - 4.3.4. Reopening a covered account with a new account number;
 - 4.3.5. Not opening a new covered account;
 - 4.3.6. Closing an existing covered account;
 - 4.3.7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
 - 4.3.8. Notifying law enforcement; or
 - 4.3.9. Determining that no response is warranted under the particular circumstances.

5. Applicable Definitions

- 5.1. **Account** means a continuing relationship established by a person with the Company to obtain a product or service for personal, family, household or business purposes. Account includes:
 - 5.1.1. An extension of credit, such as the purchase of property or services involving a deferred payment; and
 - 5.1.2. A deposit account.
- 5.2. The term **board of directors** includes:
 - 5.2.1. In the case of a Company that does not have a board of directors, a designated employee at the level of senior management.

- 5.3. **Covered account** means:
- 5.3.1. An account that the Company offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
 - 5.3.2. Any other account that the Company offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Company from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- 5.4. **Credit** has the same meaning as in 15 U.S.C. 1681a(r)(5).
- 5.5. **Creditor** has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. In the context of this Program, the term "Company" is used to denote an entity that has been determined or may be covered by the Red Flag Rule, 16 CFR 681.2.
- 5.6. **Customer** means a person that has a covered account with the Company.
- 5.7. **Identity theft** has the same meaning as in 16 CFR 603.2(a).
- 5.8. **Red Flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- 5.9. **Service provider** means a person that provides a service directly to the Company.

6. Program Elements

- 6.1. The Program includes reasonable policies and procedures to:
- 6.1.1. Identify relevant Red Flags for the covered accounts that are offered or maintained, and incorporate those Red Flags into the Program;
 - 6.1.2. Detect Red Flags that have been incorporated into the Program;
 - 6.1.3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
 - 6.1.4. Ensure the 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.

7. Incorporation of Red Flags

The Program includes one or more of the following Red Flags:

7.1. Alerts, Notifications or Warning from a Consumer Reporting Agency

- 7.1.1. A fraud or active duty alert is included with a consumer report.
- 7.1.2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- 7.1.3. A consumer reporting agency provides a notice of address discrepancy, as defined in 16 CFR 681.1(b).
- 7.1.4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - 7.1.4.1. A recent and significant increase in the volume of inquiries;
 - 7.1.4.2. An unusual number of recently established credit relationships;
 - 7.1.4.3. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - 7.1.4.4. An account that was closed for cause or identified for abuse of account privileges by the Company.

7.2. Suspicious Documents

- 7.2.1. Documents provided for identification appear to have been altered or forged.
- 7.2.2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- 7.2.3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- 7.2.4. Other information on the identification is not consistent with readily accessible information that is on file with the Company, such as a signature card or a recent check.
- 7.2.5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

7.3. Suspicious Personal Identifying Information

- 7.3.1. Personal identifying information provided is inconsistent when compared against external information sources used by the Company. For example:
 - 7.3.1.1. The address does not match any address in the consumer report; or
 - 7.3.1.2. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- 7.3.2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- 7.3.3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Company. For example:
 - 7.3.3.1. The address on an application is the same as the address provided on a fraudulent application; or
 - 7.3.3.2. The phone number on an application is the same as the number provided on a fraudulent application.
- 7.3.4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Company. For example:
 - 7.3.4.1. The address on an application is fictitious, a mail drop, or a prison; or
 - 7.3.4.2. The phone number is invalid, or is associated with a pager or answering service.
- 7.3.5. The SSN provided is the same as that submitted by other persons opening an account or other customers.
- 7.3.6. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- 7.3.7. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- 7.3.8. Personal identifying information provided is not consistent with personal identifying information that is on file with the Company.

- 7.3.9. The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

7.4. Unusual Use of, or Suspicious Activity Related to, the Covered Account

- 7.4.1. Shortly following the notice of a change of address for a covered account, the Company receives a request for the addition of authorized users on the account.
- 7.4.2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - 7.4.2.1. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash; or
 - 7.4.2.2. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
- 7.4.3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - 7.4.3.1. Nonpayment when there is no history of late or missed payments;
 - 7.4.3.2. A material increase in the use of available credit;
 - 7.4.3.3. A material change in purchasing or spending patterns; or
 - 7.4.3.4. A material change in electronic fund transfer patterns in connection with a deposit account;
- 7.4.4. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- 7.4.5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- 7.4.6. The Company is notified that the customer is not receiving paper account statements.
- 7.4.7. The Company is notified of unauthorized charges or transactions in connection with a customer's covered account.

7.5. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Company.

- 7.5.1. The Company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

SAMPLE RED FLAG IDENTITY THEFT PREVENTION PROGRAM (“PROGRAM”)

COMPLIANCE RECORDS

FISCAL YEAR	
PROGRAM MANAGER	
TRAINED STAFF	
SERVICE PROVIDERS	

STAFF TRAINING

APPLICABLE PROGRAM ELEMENT(S):

2.4. The Program includes appropriate staff training.

**LOG
STAFF TRAINING**

DATE	NAME OF STAFF	DESCRIPTION OF TRAINING

PERIODIC RISK ASSESSMENT

APPLICABLE PROGRAM ELEMENT(S):

2.7. The Program includes a risk assessment to determine whether a covered account has been offered or is maintained, taking into consideration:

- 2.7.1. The methods used to open a covered account;
- 2.7.2. The methods provided to access a covered account; and
- 2.7.3. Any previous experiences with identity theft.

**LOG
RISK ASSESSMENT**

DATE	ASSESSMENT OF RISK	ACTION TAKEN

PERIODIC DETERMINATION OF COVERED ACCOUNTS

APPLICABLE PROGRAM ELEMENT(S):

2.6. The Program includes the periodic determination of the offering or maintenance of a covered account.

**LOG
COVERED ACCOUNTS**

DATE	DESCRIPTION OF REVIEW	ACTION TAKEN

LOG: REPORTS, RECOMMENDATIONS AND CHANGES

APPLICABLE PROGRAM ELEMENT(S):

3.1. Staff responsible for development, implementation, and administration of the Program reports to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the Company with 16 CFR 681.2.

3.2. The report addresses material matters related to the Program and evaluates issues such as:

3.2.1. The effectiveness of the 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;

3.2.2. Service provider arrangements;

3.2.3. Significant incidents involving identity theft and management's response; and

3.2.4. Recommendations for material changes to the Program.

**LOG
REPORTS, RECOMMENDATIONS AND CHANGES**

DATE	REPORT OR CHANGE	ACTION TAKEN

LOG: SERVICE PROVIDER OVERSIGHT

APPLICABLE PROGRAM ELEMENT(S):

2.5. The Program includes oversight of service provider arrangements, including steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

**LOG
SERVICE PROVIDER OVERSIGHT**

DATE	NAME OF SERVICE PROVIDER	OVERSIGHT

SAMPLE RED FLAG IDENTITY THEFT PREVENTION PROGRAM (“PROGRAM”)

LOG: DETECTION AND RESONSE TO RED FLAGS LOG

FISCAL YEAR: _____

PROGRAM MANAGER: _____

**LOG
DETECTION AND RESPONSE TO RED FLAGS**

DATE	ACCOUNT	RED FLAG (CODE OR EXPLANATION)	RESPONSE (CODE OR EXPLANATION)

RED FLAGS: CODES AND EXAMPLES

7. The Program includes one or more of the following Red Flags:

CODE	EXAMPLES OF RED FLAGS
7.1	Alerts, Notifications or Warnings from a Consumer Reporting Agency
7.1.1	A fraud or active duty alert is included with a consumer report.
7.1.2	A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
7.1.3	A consumer reporting agency provides a notice of address discrepancy.
7.1.4	A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer
7.2	Suspicious Documents
7.2.1	Documents provided for identification appear to have been altered or forged.
7.2.2	The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7.2.3	Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
7.2.4	Other information on the identification is not consistent with readily accessible information that is on file with the Company, such as a signature card or a recent check.
7.2.5	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
7.3	Suspicious Personal Identifying Information
7.3.1	Personal identifying information provided is inconsistent when compared against external information sources used by the Company.
7.3.2	Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
7.3.3	Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Company.
7.3.4	Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Company.
7.3.5	The SSN provided is the same as that submitted by other persons opening an account or other customers.

7.3.6	The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
7.3.7	The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
7.3.8	Personal identifying information provided is not consistent with personal identifying information that is on file with the Company.
7.3.9	The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
7.4	Unusual Use of, or Suspicious Activity Related to, the Covered Account
7.4.1	Shortly following the notice of a change of address for a covered account, the Company receives a request for the addition of authorized users on the account.
7.4.2	A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns.
7.4.3	A covered account is used in a manner that is not consistent with established patterns of activity on the account.
7.4.4	A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
7.4.5	Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
7.4.6	The Company is notified that the customer is not receiving paper account statements.
7.4.7	The Company is notified of unauthorized charges or transactions in connection with a customer's covered account.
7.5	Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Company.
7.5.1	The Company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

APPROPRIATE RESPONSES TO IDENTIFIED RED FLAGS

APPLICABLE PROGRAM ELEMENT(S):

4.1. The Program's policies and procedures provide for appropriate responses to the Red Flags that have been detected that are commensurate with the degree of risk posed.

4.2. In determining an appropriate response, aggravating factors are considered that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the Company, or third party, or notice that a customer has provided information related to a covered account held by the Company to someone fraudulently claiming to represent the Company or to a fraudulent website.

CODE	APPROPRIATE RESPONSES TO IDENTIFIED RED FLAGS
4.3.1	Monitoring a covered account for evidence of identity theft
4.3.2	Contacting the customer
4.3.3	Changing any passwords, security codes, or other security devices that permit access to a covered account
4.3.4	Reopening a covered account with a new account number
4.3.5	Not opening a new covered account
4.3.6	Closing an existing covered account
4.3.7	Not attempting to collect on a covered account or not selling a covered account to a debt collector
4.3.8	Notifying law enforcement
4.3.9	Determining that no response is warranted under the particular circumstances