

# Name

## Identity Theft Prevention Program (ITPP)

### A. OBJECTIVE

This Identity Theft Prevention Program (ITPP) is designed specifically to comply with the Red Flags Rule (16 C.F.R. § 681.2). It is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The policies and procedures herein are designed to (1) identify Red Flags, (2) detect and evaluate Red Flags, (3) respond to Red Flags, and (4) update the ITPP periodically to reflect changes in risks to customers and to the safety and soundness of the dealership from identity theft. A Red Flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

### B. APPLICABILITY

This ITPP applies to Covered Accounts. Covered Accounts refers to all financial transactions consisting of a loan, installment sale or lease transaction for a consumer purposes (i.e., a personal, family or household purpose) that is originated, or documented, by this dealership. This ITPP applies to all such transactions, whether or not they are held and serviced by this dealership, or whether they are sold/assigned to another individual, entity, or a financing source.

This ITPP also applies to transactions for business or commercial purposes to the extent it is determined by this dealership that transactions for such purposes pose a reasonably foreseeable risk of identity theft.

### C. ITPP ADMINISTRATION

#### Development and Implementation

[The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] is responsible for overseeing the development, implementation and administration of this ITPP. [The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] must approve this ITPP and any updates to this ITPP, and such approval(s) shall be in writing and shall be maintained with this ITPP.

[The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] may appoint a Program Coordinator to manage the day-to-day responsibility for developing, implementing and administering this ITPP. In the absence of such appointment, [The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] shall perform the duties of the Program Coordinator, provided however, that [The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] may appoint various persons in the dealership to be responsible for specific tasks necessary to develop, implement, and

administer this ITPP. A person or persons appointed with such responsibilities, for purposes of this ITPP, shall be considered a Program Coordinator.

1. The Program Coordinator shall develop this ITPP using policies and procedures reasonably believed to be effective at identifying Red Flags associated with a reasonably foreseeable risk of identity theft.
2. This ITPP shall include existing Red Flags that the Program Coordinator has determined are an effective means of detecting identity theft.
3. To the extent the dealership has implemented, or in the future implements, a Customer Identification Program (CIP) as provided under the USA PATRIOT Act, this ITPP may be combined with such CIP. Any such combination will comply with both the USA PATRIOT Act and the FTC's Red Flags Rule.

### **Training**

The Program Coordinator(s) shall ensure that all Staff who are involved in the collection, use, and maintenance of non-public customer information, or who have access to such information, receive appropriate training with regard to their duties and obligations under this ITPP.

1. The Program Coordinator will prepare or approve a training program designed to educate Staff about their duties and obligations under this ITPP.
2. The first training will be provided to all Staff prior to November 1, 2008. Training for Staff hired on or after November 1, 2008 shall occur as part of a new-hire orientation process.
3. Staff will receive refresher training each time this ITPP is updated. In the event this ITPP is not updated during any particular 12-month period, all Covered Staff will receive refresher training prior to the expiration of such 12-month period.

### **Maintenance and Updating**

1. The Program Coordinator(s) will review this ITPP after any identity theft incident in the dealership that was not prevented, and at least once every 12 months.
2. The Program Coordinator(s) will update this ITPP after such review, if necessary, to reflect changes in risks to customers and to the safety of the dealership from identity theft. In recommending changes to this ITPP, the Program Coordinator(s) shall consider factors such as:
  - a. Instances of identity theft involving the dealership;
  - b. New technology or changes in methods of identify theft;

- c. New technology or changes in methods to detect, prevent, and mitigate identity theft;
  - d. Changes in the types of Covered Accounts the dealership offers or maintains;
  - e. Changes in business structure and business arrangement, including, but not limited to, relationships with vendors and third party contractors who deal with Covered Accounts or may have access to Covered Account information.
3. The Program Coordinator(s) shall maintain written reporting to document the dealership's compliance with this ITPP, the effectiveness of this ITPP, and recommend any changes to this ITPP that are, in the opinion of the Program Coordinator(s), reasonably necessary (1) after any incident of non-prevented identity theft, or (2) in no incidents of non-prevented identity theft, at least every twelve (12) months.

Following any incident of non-prevented identity theft, or at least every twelve (12) months, the Program Administrator(s) shall submit a written report to [The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] for review and action, if necessary. The report shall specifically address any incident of non-prevented identity theft, or if none, address material matters related to the ITPP, and provide an evaluation of:

- a. The effectiveness of the ITPP in addressing the risk of identity theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
- b. Arrangements or contracts with third parties who may provide services with regard to Covered Accounts, including the identity and obligations of each;
- c. Incidents involving identity theft and the dealership's response; and
- d. Recommendations for material changes to the ITPP.

[The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management] shall review, analyze, and evaluate the written report(s) from the Program Coordinator(s) and may approve recommendations for material changes, if any, to this ITPP.

The Program Coordinator(s) shall implement any changes to the ITPP as directed by [The Board of Directors] [Committee of The Board of Directors] [The General Manager] [Specified Individual in Senior Management].

Updates and changes to this ITPP and the approvals of the same shall be documented and maintained for a period of five (5) years.

4. ***Risk Assessment***

The Program Coordinator(s) will identify the Covered Accounts subject to this ITPP and conduct an assessment of the dealership's risks relative to an identity theft incident relating to such Covered Accounts (Covered Accounts are defined on page 1 of this ITPP)

The risk assessment shall consist of a review of the dealership's current policies and procedures aimed at detecting and preventing identity theft, and the Red Flags related to such policies and procedures.

The Program Coordinator(s) shall evaluate the effectiveness of the current policies and procedures with respect to detecting, preventing and mitigation identity theft relating to Covered Accounts and prepare a written report documenting such policies and procedures and his/her conclusions regarding their effectiveness.

**D. IDENTIFYING RED FLAGS**

1. A list of Red Flags made part of this ITPP is located in Appendix A. The Program Coordinator(s) shall update such Red Flags list from time to time, as is determined reasonably necessary by the Program Coordinator(s), to comply with the terms and scope of this ITPP.
2. To identify relevant Red Flags associated with the origination or maintenance of the dealership's Covered Accounts, the Program Coordinator(s) shall:
  - a. Identify and evaluate the methods employed by the dealership to open Covered Accounts (i.e. in person, telephone, internet, etc.);
  - b. Identify and evaluate the methods by which the dealership allows access to Covered Accounts, whether such access is by customers, employees, third parties, or others.
3. The Program Coordinator shall identify Red Flags to be part of this ITPP from the following sources:
  - a. Existing policies and procedures

i. \_\_\_\_\_

ii. \_\_\_\_\_

iii. \_\_\_\_\_

iv. \_\_\_\_\_

v. \_\_\_\_\_

vi. \_\_\_\_\_

vii. \_\_\_\_\_

b. Incidences of identity

i. \_\_\_\_\_

ii. \_\_\_\_\_

iii. \_\_\_\_\_

iv. \_\_\_\_\_

v. \_\_\_\_\_

vi. \_\_\_\_\_

vii. \_\_\_\_\_

c. Methods of identity theft reflecting changes in identity theft risks

i. \_\_\_\_\_

ii. \_\_\_\_\_

iii. \_\_\_\_\_

iv. \_\_\_\_\_

v. \_\_\_\_\_

vi. \_\_\_\_\_

vii. \_\_\_\_\_

d. Guidance from supervisory/government agencies

i. \_\_\_\_\_

ii. \_\_\_\_\_

iii. \_\_\_\_\_

iv. \_\_\_\_\_

v. \_\_\_\_\_

vi. \_\_\_\_\_

vii. \_\_\_\_\_

4. The Program Coordinator shall identify Red Flags to be part of this ITPP from the following categories:
- a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
    - i. fraud or active duty alerts included with a consumer report.
    - ii. A consumer reporting agency notice of credit freeze in response to a request for a consumer report.
    - iii. A consumer reporting agency notice of address discrepancy.
    - iv. A consumer report showing a pattern of activity that is inconsistent with the history and usual pattern of activity of an application or customer, such as:
      - recent and significant increase in the volume of inquiries;
      - unusual number of recently established credit relationships;
      - A material change in the use of credit, i.e. significant recent use of existing credit accounts that only been recently established, or accounts that have otherwise been relatively inactive or only moderately active; or
      - An account was closed for cause or for abuse of account privileges by a financial institution or creditor.
  - b. Suspicious or altered documents.
    - i. Documents provided for identification that appear to have been altered or forged (i.e. fraudulent driver licenses or passports, or foreign or any other identification documents that may be unfamiliar);
    - ii. Photograph, physical description, or other information on the form of identification that is not consistent with the appearance of the applicant or customer presenting the identification;
    - iii. Information on the identification is inconsistent with information provided by the person presenting the identification;

iv. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

v. \_\_\_\_\_

vi. \_\_\_\_\_

c. Presentation of suspicious personal identifying information.

- i. Personal identifying information provided by the customer is inconsistent when compared against external information sources used by the dealership for credit, fraud detection, or other purposes. (i.e. the address provided by the customer in the application does not match any address in the customer's consumer report, or the Social Security Number has not been issued or is listed on the Social Security Administration's Death Master File).
- ii. The customer presents conflicting personal identifying information (i.e. no correlation between the SSN range and date of birth, or no correlation between the SSN geo-code and the customer's address at the time the SSN was issued)
- iii. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the dealership.
- iv. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the dealership (i.e. address on an application is fictitious, a mail drop, or a prison, or the phone number is invalid, or is associated with a pager or answering service)
- v. The SSN provided is a duplication of another social security number submitted by other persons opening a Covered Account or other customers.
- vi. The address or telephone number provided is the same as or similar to the address or telephone number submitted by other persons submitting credit applications.
- vii. The customer fails to provide all required personal identifying information on an application, especially if such information is not provided in response to notification that the application is incomplete.
- viii. Personal identifying information provided is not consistent with personal identifying information that the dealership has on file.

ix. \_\_\_\_\_

x. \_\_\_\_\_

- d. Suspicious activity related to the Covered Account. These Red Flags generally arise in the context of *existing* Covered Accounts, i.e., not Red Flags in the context of originating a Covered Account (i.e. first payment default, or nonpayment with no history of late or missed payments).
- e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts maintained by the dealership.

## **E. DETECTING/EVALUATING RED FLAGS**

### **1. Processing Credit Process**

**(Needs filled in)**

### **2. Credit Applications**

All credit applications will be taken or scribed at the dealership, in writing or electronically. Customers may not take applications out of the dealership for completion.

All credit applications will contain the following minimum information:

**(Needs Filled IN)**

### **3. Verifying Identification**

The Program Coordinator(s) shall develop an ITPP Origination Checklist to be used by Staff responsible for verifying customer identities each time a Covered Account is opened. The ITPP Origination Checklist shall be completed with each credit application, and maintained with the credit application in the deal jacket or dead credit file, whichever may be applicable. The Program Coordinator(s) shall update such ITPP Origination Checklist from time to time as may be necessary to comply with the terms of this ITPP.

- a. Authentication: acceptable documentation for identity verification purposes includes:
  - i. Individuals: an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard (i.e. driver's license, passport, etc.)

- ii. Business Entities: documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, partnership agreement, or trust instrument. Identification for the individual acting on behalf of the business entity should also be obtained.
- b. Absentee Customers: for customers who are not present in the dealership, additional steps shall be taken to authenticate their identities.
- i. Contact the customer by telephone on each number provided prior to opening the Covered Account
  - ii. Independently verify the customer's identity by comparing information provided by the customer with information obtained from a consumer reporting agency, such as:
    - 1. Name of the financial institution holding his or her mortgage, if any, and the total amount of such mortgage;
    - 2. The financial institution servicing the customer's current vehicle financing, and the remaining balance on the account;
    - 3. Prior addresses where the customer lived;
    - 4. Name(s) of employer(s).
  - iii. Check references with other financial institutions.
- c. Customer-Provided Information
- i. Social Security Number
    - 1. Check the SSN against the SSA Death Master File. If the SSN appears on file;
    - 2. Validate that the first three numbers of the SSN match the state of the customer's residence at the time of issue;
    - 3. Use third party service providers to determine whether the SSN is associated with fraud or identity theft.
- If any discrepancies are revealed, contact Program Coordinator for action.

## ii. Address

1. Consumer Report Notice of Address Discrepancy – inquire of the customer the reason for the discrepancy and request additional documentation to verify the address (i.e. utility bill). If the customer is unable to provide verifiable information, contact the Program Coordinator for action. If the dealership services Covered Accounts and reports to the consumer reporting agencies, follow applicable dealership procedures for verifying address discrepancies.
2. Customer Provided Address not on consumer report – inquire of the customer the reason for the discrepancy and request additional documentation to verify the address (i.e. utility bill). If the consumer is unable to provide verifiable information, contact the Program Coordinator for action.
3. Use third party service providers to determine whether the address provided by the customer is associated with fraud or identity theft.

## iii. Consumer Report Alert, Activity, and Credit Freeze

1. Active Duty Alerts – if a consumer report contains an active duty alert, obtain a military ID from the customer as well as orders indicating where he or she is stationed. If the customer is unable to provide either, or you are unable to determine the validity of such documents, contact the Program Coordinator for action.
2. Fraud Alerts – A consumer report may contain an initial or extended fraud alert.
  - a. An initial fraud alert stays on the consumer report for 90 days and indicates that the customer believes he or she may have been a victim of identity theft. Require additional photo identification and documentation (i.e. utility bills, etc.) when verifying the customer's identify. If the consumer report provides a specific method to identify the customer, employ that method in addition to obtaining additional documentation. Additional efforts to verify the customer's identity should be documented on the ITPP checklist.
  - b. An extended fraud alert stays on the consumer report for 7 years and indicates that the customer has notified the authorities that he or she has been a victim of identity theft. The consumer report will indicate a specific method to

identity the customer, and you must use this method. Additional verification methods used in the case of an initial fraud alert should also be employed. Additional efforts to verify the customer's identity should be documented on the ITPP checklist.

3. Credit Activity – trade lines in a consumer report shall be reviewed for suspicious activity. If activity is present, inquire of the customer the reason for such activity. If the customer cannot explain the activity or acts suspicious upon inquiry, contact the Program Coordinator for action. Suspicious activity may include, but is not limited to, the following:
  - a. recent and significant increases in the volume of inquiries;
  - b. unusual number of recent credit relationships created;
  - c. A change in the use of credit, especially with respect to recently established credit relationships (i.e. significant recent use of existing credit accounts that have otherwise been relatively inactive or only moderately active);
  - d. An account closed for cause or identified for abuse of account privileges by a financial institution or creditor.

#### 4. Credit Freeze

If a consumer reporting agency indicates that a consumer report file is subject to a security freeze, advise the customer that he or she will have to contact the consumer reporting agency to temporarily thaw the file.

#### iv. Law Enforcement or Customer Notice

The dealership shall maintain a file of notices from law enforcement, customers, victims of identity theft, and others who have advised the dealership of identity theft activity relating to certain names, addresses, phone numbers, Social Security Numbers, etc. All credit applications should be checked against this information before submission of the application to a financing source.

#### d. Existing Accounts

To the extent the dealership holds and services Covered Accounts, in cases of first payment default or payment default where there is no history of late or missed payments, the dealership shall attempt to contact the customer at the

address(es) and telephone number(s) provided to determine the cause for the default. If the customer cannot be contacted and it is believed that a fraud or identity theft has occurred, law enforcement should be contacted or such other action undertaken as may be necessary and proper under the circumstances to protect the dealership and its customers.

4. Access to Non-Public Information

(Needs filled in.)

5. Storage of Non-Public Information

(Needs filled in)

6. Destruction Policy of Documents Containing Non-Public Information

(Needs filled in.)

**F. RESPONSE TO RED FLAGS**

1. General Response

(Needs filled in.)

2. Opening Covered Accounts

*(needs filled in.)*

3. Maintaining a Covered Account

(Needs filled in)

**G. UPDATING THE ITPP**

1. The Program Coordinator(s) shall review and evaluate the effectiveness of the ITPP (1) after any incident of non-prevented identity theft, or (2) in no incidents of non-prevented identity theft, at least every twelve (12) months

2. In the significant incidence of identity theft, the Program Coordinator(s) will conduct and document an investigation into the facts and circumstances surrounding the incident, and recommend changes to the ITPP, if necessary. The scope of any such investigation shall determine:

a. Whether Red Flags already identified in the ITPP were present in the identity theft incident.

- b. Whether current ITPP procedures for detecting such Red Flags were used in the particular transaction.
  - c. Whether current ITPP procedures are sufficient to detect the particular Red Flags.
  - b. Whether changes to the ITPP are necessary to identify new Red Flags or detect new or existing Red Flags.
  - c. Whether additional training of dealership personnel is needed.
- 3. After any incident of non-prevented identity theft, the Program Coordinator(s) shall prepare a report for [The Board of Directors] [A Committee of the Board of Directors] [The General Manager] [Specified Individual] specifically addressing any incident of non-prevented identity theft and providing an evaluation of:
  - a. The effectiveness of the ITPP in addressing the risk of identity theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
  - b. Arrangements or contracts with third parties who may provide services with regard to Covered Accounts, including the identity and obligations of each;
  - c. Incidents involving identity theft and the dealership's response; and
  - d. Recommendations for material changes to the ITPP.
- 7. New Methods of Identity Theft/Theft Detection Methods

As the Program Coordinator(s) becomes aware of changes in methods of identity theft, he or she will review the ITPP and recommend changes, if any, that are appropriate.

As the Program Coordinator becomes aware of changes in technology or methods to detect and prevent identity theft, he or she will review the ITPP and recommend changes, if necessary, that are appropriate.
- 8. New Covered Accounts

The Program Coordinator(s) will monitor the financial products and services offered by the dealership to determine whether any products and services are Covered Accounts subject to this ITPP. Upon determining that a new financial product or service is a Covered Account subject to this ITPP, the Program Coordinator will update this ITPP as necessary.
- 9. Change in Business Arrangements

The Program Coordinator(s) will monitor the business arrangements of the dealership, including any changes in organization structure or contracts with third parties with Covered Account access or access to information contained in Covered Accounts. The Program Coordinator(s) will update this ITPP as necessary to take into account such changes in the dealership.

Appendix A  
ITPP Origination Checklist

Appendix B  
ITPP Red Flag Rules

Appendix C  
Identity Theft Incident Report

Appendix D  
Third-Party Compliance Agreement

## APPENDIX B: The Red Flag Rules

### Federal Trade Commission

16 CFR Part 681

#### Authority and Issuance

For the reasons discussed in the joint preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

#### **PART 681 – IDENTITIIY THEFT RULES**

Sec.

681.1 Duties of users of consumer reports regarding address discrepancies.

681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

681.3 Duties of card issuers regarding changes of address.

Appendix A to Part 681 Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

15 U.S.C. 1681c(h)

#### **§ 681.1 Duties of users regarding address discrepancies**

(a) *Scope.* This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681 s(a)(1) (users).

(b) *Definition.* For purposes of this section, a notice of address discrepancy means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user<sup>4</sup> of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(1) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirements to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

## **§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.**

(a) *Scope.* This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) *Definitions.* For purposes of this section, and Appendix A, the following definitions apply:

(1) Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch of agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered Account* means:

(i) An account that a financial institution or creditor 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

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(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.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial Institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) Program requirement. Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program.

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) 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 financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate.

### **§ 681.3 Duties of card issuers regarding changes of address.**

(a) *Scope.* This section applies to a person described in § 681.2(a) that issues a debit or credit card (card issuer).

(b) *Definition.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request;

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 681.2 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

## **APPENDIX A TO PART 681 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION**

Sections 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program and to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

### **I. *The Program.***

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

## II. *Identifying Relevant Red Flags*

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate: (1) the types of covered accounts it offers or maintains;

- (1) The methods it provides to open its covered accounts;
- (2) The methods it provides to access its covered accounts; and
- (3) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that the financial institution or creditor has experienced;
- (2) Incidents of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

- (3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

- (2) The presentation of suspicious documents;

- (3) The presentation of suspicious personal identifying information, such as a suspicious address change

- (4) The unusual use of, or other suspicious activity related to, a covered account; and

- (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 financial institution or creditor.

## III. *Detecting Red Flags*

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(1) (31 CFR 103.121); and

- (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

## IV. *Preventing and Mitigating Identity Theft*

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors 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 financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor or to a fraudulent website.

Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;

- (b) Contacting the customer;

- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

- (d) Reopening a covered account with a new account number;

- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement;
- (i) Determining that no response is warranted under the particular circumstances.

#### **V. *Updating the Program***

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

- (a) The experiences of the financial institution or creditor with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

#### **VI. *Methods for Administering the Program***

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

- (1) Assigning specific responsibility for the Program's implementation;
- (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and
- (3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of a financial institution or creditor responsible for development, implementation, and administration of its Program should report 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 financial institution or creditor with § 681.2 of this part.

(2) *Content of reports.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in 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 incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take 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. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

#### **VII. *Other Applicable Legal Requirements***

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

### **Supplement A to Appendix A**

In addition to incorporating Red Flags from the sources recommended in section II.b of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

#### ***Alerts, Notifications or Warnings from a Consumer Reporting Agency***

1. A fraud or active duty alert is included with a customer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
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:
  - a. A recent and significant increase in the volume of inquiries.
  - b. An unusual number of recently established credit relationships.
  - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
  - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

#### ***Suspicious Documents***

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

***Suspicious Personal Identifying information***

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - a. The address does not match any address in the consumer report; or
  - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. 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 the date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - a. The address on an application is the same as the address provided on a fraudulent application; or
  - b. The phone number on an application is the same as the number provided on a fraudulent application.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - a. The address on an application is fictitious, a mail drop, or a prison; or
  - b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. 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.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or the creditor.

18. For financial institutions and creditors that use challenge questions, 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.

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

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
- b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- a. Nonpayment when there is no history of late or missed payments;
- b. A material increase in the use of available credit;
- c. A material change in purchasing or spending patterns;
- d. A material change in electronic fund transfer patterns in connection with a deposit account; or
- e. A material change in telephone call patterns in connection with a cellular phone account.

22. 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).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

***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 Financial Institution or Creditor.***

26. The financial institution or creditor 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.