**Attachment 2**

# Interagency Examination Procedures

## Section 615(e) Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft (12 CFR 222.90)

### Background

Section 615(e) of the Fair Credit Reporting Act requires the federal banking agencies and the National Credit Union Administration (collectively, the Agencies) as well as the Federal Trade Commission to prescribe regulations and guidelines for financial institutions and creditors[1] regarding identity theft. On November 9, 2007, the Agencies published final rules and guidelines in the Federal Register (72 FR 63718) implementing this section.

Definitions (12 CFR 222.90(b)). The following regulatory definitions pertain to the regulations regarding identify theft red flags:

1. An "account" is a continuing relationship established by a person with a financial institution to obtain a product or service for personal, family, household, or business purposes. An account includes:
    a. An extension of credit, such as the purchase of property or services involving a deferred payment; and
    b. A deposit account.
2. The "board of directors" includes, for a branch or agency of a foreign bank, the managing official in charge of the branch or agency and, for any other creditor that does not have a board of directors, a designated employee at the level of senior management.
3. A "covered account" is:
    a. An account that a financial institution offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and
    b. Any other account offered or maintained by the financial institution for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.
4. A "customer" is a person that has a "covered account" with a financial institution.

[1] For purposes of these examination procedures, "financial institutions and creditors" are referred to jointly as "financial institutions."

5. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. "Identifying information" means any name or number that may be used alone or in conjunction with any other information to identify a specific person (16 CFR 603.2).

6. A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

7. A "service provider" is a person that provides a service directly to a financial institution.

Periodic identification of covered accounts (12 CFR 222.90(c)). Each financial institution must periodically determine whether it offers or maintains covered accounts. As part of this determination, the financial institution must conduct a risk assessment to determine whether it offers or maintains covered accounts 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.

Establishment of an identity theft prevention program (Program) (12 CFR 222.90(d)). A financial institution must develop and implement a written Program 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 tailored to the financial institution's size and complexity and the nature and scope of its operations and must contain "reasonable policies and procedures" to:

1. Identify red flags for the covered accounts the financial institution offers or maintains and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. 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 from identity theft.

Administration of the Program (12 CFR 222.90(e)). A financial institution must provide for the continued administration of the Program by:

1. Obtaining approval of the initial written Program by the board of directors or an appropriate committee of the board;
2. Involving the board of directors, a committee of the board, or an employee at the level of senior management, in the oversight, development, implementation, and administration of the Program;
3. Training staff, as necessary, to implement the Program effectively; and
4. Exercising appropriate and effective oversight of service provider arrangements.

Guidelines (12 CFR 222.90(f)). Each financial institution that is required to implement a program also must consider the guidelines in Appendix J of the regulation and include in its Program those guidelines that are appropriate. The guidelines are intended to assist financial institutions in the formulation and maintenance of a Program that satisfies the regulatory requirements. A financial institution may determine that a particular guideline is not appropriate to incorporate into its Program; however, the financial institution must have policies and procedures that meet the specific requirements of the rules.

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

Illustrative examples of red flags are located in Supplement A to Appendix J of the regulation. A financial institution is not required to use the examples, nor will it need to justify its failure to include in its Program a specific red flag from the list of examples. However, the financial institution must be able to account for the overall effectiveness of its Program that is appropriate to its size and complexity and the nature and scope of its activities.

## Examination Procedures

1. Verify that the financial institution periodically[2] identifies covered accounts it offers or maintains.[3] Verify that the financial institution:

   - Included accounts for personal, family, and household purposes that permit multiple payments or transactions; and
   - Conducted a risk assessment to identify any other accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the institution's previous experiences with identity theft (12 CFR 222.90(c)).

2. Review examination findings in other areas (e.g. Bank Secrecy Act, Customer Identification Program and Customer Information Security Program) to determine whether there are deficiencies that adversely affect the financial institution's ability to comply with the Identity Theft Red Flags Rules (red flag rules).

3. Review any reports, such as audit reports and annual reports prepared by staff for the board of directors[4] (or an appropriate committee thereof or a designated senior management employee) on compliance with the red flag rules, including reports that address:

   - The effectiveness of the financial institution's Identity Theft Prevention Program (Program);
   - Significant incidents of identity theft and management's response;
   - Oversight of service providers that perform activities related to covered accounts; and
   - Recommendations for material changes to the Program.

   Determine whether management adequately addressed any deficiencies (12 CFR 222.90(f); Guidelines, Section VI).

4. Verify that the financial institution has developed and implemented a comprehensive written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account. The Program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities (12 CFR 222.90(d)(1)).

---

[2] The risk assessment and identification of covered accounts is not required to be done on an annual basis. This should be done periodically, as needed.

[3] A "covered account" includes: (i) an account primarily for personal, family, or household purposes, such as a credit card account, mortgage loan, auto loan, checking account, or savings account that permits multiple payments or transactions; and (ii) any other account that the institution offers or maintains for which there is a reasonable foreseeable risk to customers or the safety and soundness of the institution from identity theft (12 CFR 222.90(b)(3)).

[4] The term board of directors includes: (i) in the case of a branch or 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.

- Verify that the financial institution considered the Guidelines in Appendix J to the regulation (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation) in the formulation of its Program and included those that are appropriate (12 CFR 222.90(f)).
- Determine whether the Program has reasonable policies, procedures, and controls to effectively identify and detect relevant red flags and to respond appropriately to prevent and mitigate identity theft (12 CFR 222.90(d)(2)(i)-(iii)). Financial institutions may, but are not required to, use the illustrative examples of red flags in Supplement A to the Guidelines to identify relevant red flags (12 CFR 222.90(d)(2); Appendix J, Sections II, III and IV).
- Determine whether the financial institution uses technology to detect red flags. If it does, discuss with management the methods by which the financial institution confirms the technology is working effectively.
- Determine whether the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in the risks to customers and the safety and soundness of the financial institution from identity theft (12 CFR 222.90(d)(2)(iv)).
- Verify that (i) the board of directors (or appropriate committee thereof) initially approved the Program; and (ii) the board (or an appropriate committee thereof, or a designated senior management employee) is involved in the oversight, development, implementation, and administration of the Program (12 CFR 222.90(e)(1) and (2)).

5. Verify that the financial institution trains appropriate staff to effectively implement and administer the Program (12 CFR 222.90(e)(3)).

6. Determine whether the financial institution exercises appropriate and effective oversight of service providers that perform activities related to covered accounts (12 CFR 222.90(e)(4)).

***Conclusion:*** On the basis of examination procedures completed, form a conclusion about whether the financial institution has developed and implemented an effective, comprehensive written Program designed to detect, prevent, and mitigate identity theft.