Risk Management Examiners

Introduction to Red Flags Examination Procedures

Section 615(e) requires the federal banking agencies and the NCUA (the Agencies) as well as the FTC 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 implementing this section. (72 FR 63718)

Definitions (12 CFR 334.90(b). The following regulatory definitions pertain to the regulations regarding identity 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.

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.

---

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

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

Periodic identification of covered accounts (12 CFR 334.90(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

a. the methods it provides to open its accounts,
b. the methods it provides to access its accounts, and
c. its previous experiences with identity theft.

Establishment of an identity theft prevention program (Program) (12 CFR 334.90 (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:

a. identify red flags for the covered accounts the financial institution offers or maintains and incorporate those red flags into the Program;

b. detect red flags that have been incorporated into the Program;

c. respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

d. 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_334.90 (e)). A financial institution must provide for the continued administration of the Program by:

a. obtaining approval of the initial written Program by the board of directors or an appropriate committee of the board;

b. 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;

c. training staff, as necessary, to implement the Program effectively; and

d. exercising appropriate and effective oversight of service provider arrangements.

Guidelines (12 CFR 334.90(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.

Red Flags Examination Procedures (12 CFR 334.90)

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 334.90(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

[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 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 334.90(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.

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 334.90(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 334.90(d)(1))

    - 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 334.90(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 334.90(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 334.90(d)(2); Guidelines, 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 to detect, prevent, and mitigate identity theft.

    - 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 334.90(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 334.90(e)(1) and (2))

5. Verify that the financial institution trains appropriate staff to effectively implement and administer the Program. (12 CFR 334.90(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 334.90(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.

Compliance Examiners

Introduction to Address Discrepancy Examination Procedures

Section 605(h)(1) requires that, when providing a consumer report to a person that requests the report (a user), a nationwide consumer reporting agency (NCRA) must provide a notice of address discrepancy to the user if the address provided by the user in its request "substantially differs" from the address the NCRA has in the consumer's file. Section 605(h)(2) requires the federal banking agencies and the NCUA (the Agencies) and the FTC to prescribe regulations providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice of address discrepancy. On November 9, 2007, the agencies published final rules in the Federal Register implementing this section. (72 FR 63718)

Definitions

1. Nationwide consumer reporting agency. Section 603(p) defines an NCRA as one that compiles and maintains files on consumers on a nationwide basis and regularly engages in the practice of assembling or evaluating and maintaining the following two pieces of information about consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity:
    a. Public record information and
    b. Credit account information from persons who furnish that information regularly and in the ordinary course of business.

2. Notice of address discrepancy (12 CFR 334.82(b)). A "notice of address discrepancy" is a notice sent to a user by an NCRA (section 603(p)) that informs the user 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 NCRA's file for the consumer.

Requirement to form a reasonable belief (12 CFR 334.82(c)). A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that the consumer report relates to the consumer whose report was requested, when the user receives a notice of address discrepancy in connection with a new or existing account.

The rules provide the following examples of reasonable policies and procedures for forming a reasonable belief that a consumer report relates to the consumer whose report was requested:

1. Comparing information in the consumer report with information the user:
    a. has obtained and used to verify the consumer's identity as required by the Customer Identification Program rules (31 CFR 103.121);
    b. maintains in its records; or
    c. obtains from a third party; or
2. Verifying the information in the consumer report with the consumer.

Requirement to furnish a consumer's address to an NCRA (12 CFR 334.82(d)). A user must develop and implement reasonable policies and procedures for furnishing to the NCRA an address for the consumer that the user has reasonably confirmed is accurate when the user

a. can form a reasonable belief that the report relates to the consumer whose report was requested;

b. establishes a continuing relationship with the consumer (i.e., in connection with a new account); and

c. regularly furnishes information to the NCRA that provided the notice of address discrepancy.

A user's policies and procedures for furnishing a consumer's address to an NCRA must require the user to furnish the confirmed address as part of the information it regularly furnishes to the NCRA during the reporting period when it establishes a continuing relationship with the consumer.

The rules also provide the following examples of how a user may reasonably confirm an address is accurate:

1. Verifying the address with the consumer whose report was requested;
2. Reviewing its own records;
3. Verifying the address through third-party sources; or
4. Using other reasonable means.

Address Discrepancy Examination Procedures (12 CFR 334.82)

1. Determine whether a user of consumer reports has policies and procedures to recognize notices of address discrepancy that it receives from a nationwide consumer reporting agency (NCRA) [5] in connection with consumer reports.

2. Determine whether a user that receives notices of address discrepancy has policies and procedures to form a reasonable belief that the consumer report relates to the consumer whose report was requested. (12 CFR 334.82(c))

   See examples of reasonable policies and procedures "to form a reasonable belief" in 12 CFR 334.82(c)(2).

3. Determine whether a user that receives notices of address discrepancy has policies and procedures to furnish to the NCRA an address for the consumer that the user has reasonably confirmed is accurate, if the user:

   a. can form a reasonable belief that the report relates to the consumer,
   b. establishes a continuing relationship with the consumer, and
   c. regularly furnishes information to the NCRA. (12 CFR 334.82(d)(1))

   See examples of reasonable confirmation methods in 12 CFR 334.82(d)(2).

4. Determine whether the user's policies and procedures require it to furnish the confirmed address as part of the information it regularly furnishes to an NCRA during the reporting period when it establishes a relationship with the consumer. (12 CFR 334.82(d)(3)

5. If procedural weaknesses or other risks requiring further information are noted, obtain a sample of consumer reports requested by the user from an NCRA that included notices of address discrepancy and determine:

   a. how the user established a reasonable belief that the consumer reports related to the consumers whose reports were requested, and

   b. if a consumer relationship was established:
      i. whether the institution furnished a consumer's address that it reasonably confirmed to the NCRA from which it received the notice of address discrepancy; and
      ii. whether it furnished the address in the reporting period during which it established the relationship.

[5] A NCRA compiles and maintains files on consumers on a nationwide basis. As of the effective date of the rule (January 1, 2008) there were three such consumer reporting agencies: Experian, Equifax, and TransUnion. Section 603(p) of FCRA (15 USC 1681a).

Conclusion: On the basis of examination procedures completed, form a conclusion about the ability of user's policies and procedures to meet regulatory requirements for the proper handling of address discrepancies reported by an NCRA.

Introduction to Change of Address Examination Procedures

Section 615(e)(1)(C) requires the Agencies and the FTC to prescribe regulations for debit and credit card issuers regarding the assessment of the validity of address changes for existing accounts. The regulations require card issuers to have procedures to assess the validity of an address change if the card issuer receives a notice of change of address for an existing account, and within a short period of time (during at least the first 30 days) receives a request for an additional or replacement card for the same account. On November 9, 2007, the Agencies published final rules in the Federal Register implementing this section. (72 FR 63718)

Definitions (12 CFR 334.91(b)). The following definitions pertain to the rules governing the duties of card issuers regarding changes of address:

1. A "cardholder" is 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.

Address validation requirements (12 CFR 334.91(c)). A card issuer must establish and implement 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. In such situations, the card issuer must not issue an additional or replacement card until it assesses the validity of the change of address in accordance with its policies and procedures.

The policies and procedures must provide that the card issuer will:

1. a. Notify the cardholder of the request for an additional or replacement card
   (i) at the cardholder's former address; or

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

1. b. Provide to the cardholder a reasonable means of promptly reporting incorrect address changes; or

2. Assess the validity of the change of address according to the procedures the card issuer has established as a part of its Identity Theft Prevention Program (12 CFR 334.90).

Alternative timing of address validation (12 CFR 334.91(d). A card issuer may satisfy the requirements of these rules prior to receiving any request for an additional or replacement card by validating an address when it receives an address change notification.

Form of notice (12 CFR 334.91(e)). Any written or electronic notice that a card issuer provides to satisfy these rules must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Change of Address Examination Procedures (12 CFR 334.91)

1. Verify that the card issuer has 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. (12 CFR 334.91(c))

2. Determine whether the policies and procedures prevent the card issuer from issuing additional or replacement cards until it:

    - notifies the cardholder at the cardholder's former address or by any other means previously agreed to and provides the cardholder a reasonable means to promptly report an incorrect address (12 CFR 334.91(c)(1)(i)-(ii)); or

    - uses other reasonable means of evaluating the validity of the address change. (12 CFR 334.91(c)(2)).

    In the alternative, a card issuer may validate a change of address request when it is received, using the above methods, prior to receiving any request for an additional or replacement card. (12 CFR 334.91(d))

3. Determine whether any written or electronic notice sent to cardholders for purposes of validating a change of address request is clear and conspicuous and is provided separately from any regular correspondence with the cardholder. (12 CFR 334.91(e))

4. If procedural weaknesses or other risks requiring further information are noted, obtain a sample of notifications from cardholders of changes of address and requests for additional or replacement cards to determine whether the card issuer complied with the regulatory requirement to evaluate the validity of the notice of address change before issuing additional or replacement cards.

Conclusion: On the basis of examination procedures completed, form a conclusion about whether a card issuer's policies and procedures effectively meet regulatory requirements for evaluating the validity of change of address requests received in connection with credit or debit card accounts.