

An Overview of the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 Final Rules

By: Andrea J. Shaw, Esq., Compliance Officer, Gorham Savings Bank

Introduction

The purpose of this article is to provide an overview of the requirements of the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 Final Rules (the “Final Rules”). The Final Rules are already effective; however, the mandatory compliance date is November 1, 2008. The Final Rules are accompanied by Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation (the “Guidelines”), which further illustrate the Program (as defined below) requirements. The Final Rules mandate that financial institutions and creditors consider the Guidelines and include in their Programs those that are appropriate.¹

This article is organized in a functional manner, rather than in sequential order of the Final Rules. Citations refer to the Federal Deposit Insurance Corporation (“FDIC”) version of the Final Rules whenever possible. The Final Rules apply to “financial institutions and creditors” but for ease of reading this article uses the term “financial institutions” when referring to both financial institutions and creditors.

Legislative Background

Congress passed the Fair and Accurate Credit Transaction Act (“FACTA”) in 2003. FACTA amended the preexisting Fair Credit Reporting Act (“FCRA”). FACTA included a provision mandating that the Federal Financial Institutions Examination Council and the Federal Trade Commission (together, the “Agencies”) develop regulations regarding the implementation of sections 114 and 315 of FCRA. Sections 114 and 315 focus on identity theft and address discrepancies.

The Program; Identifying, Detecting and Responding to Red Flags

Definitions

The following key definitions are found in section 90(b) of the Final Rules:

“Covered Account” means (i) 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, 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 offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation or litigation risks.² The new definition of “covered account” is divided into two parts. The first part refers to consumer accounts that involve multiple payments or transactions. The second part of the definition refers to any other account that the financial institution offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation, or litigation risks. This reflects the “Agencies views that small business accounts or sole proprietorship accounts, may be vulnerable to identify theft, and therefore, should be considered for coverage by the Program.”³ As such, both consumer and business accounts are subject to the Final Rule.

“Customer” is similarly defined as it includes businesses. The Final Rules define “customer” as a person that has a Covered Account with the financial institution.⁴ Thus, an individual with a consumer account will always be a customer. However, a “customer” may also be a person that has another type of account for which the financial institution determines there is a reasonably foreseeable risk to its customers

¹ 72 Fed. Reg. 63761 (9 November 2007), 12 CFR 334.90(f).

² 72 Fed Reg 63761 (9 November 2007).

³ 72 Fed Reg 63721(9 November 2007).

⁴ 72 Fed Reg 63761 (9 November 2007).

or its own safety and soundness from identity theft.⁵ Note, also, that “person” as defined by the FCRA includes business entities of all types.

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of identity theft.⁶

The Program

The Final Rules require the financial institution to implement a written identity theft prevention program (the “Program”).⁷ The Program must be designed to detect, prevent, and mitigate identity theft in connection with a Covered Account (at account opening and with respect to existing Covered Accounts). The size of the Program should be appropriate for the size and complexity of the financial institution.⁸ The Final Rules mandate that the Program have policies and procedures that:

- Identify Red Flags relevant to detecting possible risk of identity theft;
- Verify the identity of persons opening accounts;
- Detect Red Flags that are relevant in connection with opening an account or with existing accounts;
- Assess whether Red Flags detected are evidence of identity theft;
- Mitigate the risk of identity theft that is appropriate for the level of risk;
- Respond appropriately to any detected Red Flags;
- Ensure that the Program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution from identity theft;⁹
- Train staff; and
- Oversee service provider arrangements.

Identifying Red Flags

The Final Rules state that one element of the Program must consist of identifying Red Flags, without any elaboration.¹⁰ The Guidelines in *Appendix J* of the Final Rules set forth the framework the financial institution should follow to meet this element of the Program.

The Guidelines state that financial institution should consider the following risk factors in identifying relevant Red Flags, as appropriate for the financial institution:

- The types of Covered Accounts the financial institution offers or maintains;
- The methods the financial institution provides to open its Covered Accounts;
- The methods the financial institution provides to access its Covered Accounts; and
- The financial institution’s previous experiences with identity theft.¹¹

Next, the Guidelines set forth possible sources of Red Flags in addition to those listed in *Appendix J*. These additional sources may include, without limitation:

- Incidents of identity theft that the financial institution has experienced;
- Methods of identity theft that the financial institution has identified that reflect changes in identity theft risks; and
- Applicable supervisory guidance¹².

Finally, the Guidelines set forth the following categories of Red Flags that the financial institution’s Program should include, as appropriate for the institution:

⁵ 72 Fed Reg 63722 (9 November 2007).

⁶ 72 Fed Reg 63761 (9 November 2007).

⁷ 12 CFR 334.90 implements FCRA section 615(e)(1)(A).

⁸ *Id.*

⁹ *Id.*

¹⁰ 72 Fed Reg 63761 (9 November 2007), 12 CFR 33490(d)(1).

¹¹ 72 Fed Reg 63761 (9 November 2007).

¹² *Id.*

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a Covered Account; and
- 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.¹³

Detecting Red Flags

The Final Rules mandate that the Program implemented by each financial institution contain policies and procedures for detecting Red Flags. The Guidelines found in *Appendix J* provide further explanation of how each financial institution is required to comply with this provision. The Program should address the detection of Red Flags in connection with the opening of Covered Accounts and with respect to existing Covered Accounts by:

- Obtaining identifying information about, and verifying the identity of a person opening a Covered Account by, for example, using the policies and procedures regarding the identification and verification set forth in the financial institution’s Customer Identification Program (“CIP”); and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing Covered Accounts.

Responding to Red Flags

Once identified, the Final Rules state that the Program must address how the financial institution will respond appropriately to any detected Red Flags and mitigate identity theft.¹⁴ The corresponding Guidelines section is titled “Preventing and Mitigating Identity Theft”. The Guidelines indicate the financial institution should “appropriately respond” to detected Red Flags. In order for a response to be “appropriate” the financial institution 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, or notice that a customer has provided information related to a Covered Account held by the financial institution to someone fraudulently claiming to represent the financial institution or to a fraudulent website.¹⁵ Appropriate responses may include:

- Monitoring a Covered Account for evidence of identity theft;
- Contacting the customer, changing any passwords, security codes, or other security devices that permit access to a Covered Account;
- Reopening a Covered Account with a new account number;
- Not opening a new Covered Account;
- Closing an existing Covered Account;
- Not attempting to collect on a Covered Account;
- Not selling a Covered Account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.¹⁶

Updating the Program

The Final Rules require financial institutions ensure that the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution from

¹³ 72 Fed Reg 63762 (9 November 2007).

¹⁴ 72 Fed Reg 63761 (9 November 2007), 12 CFR 334.90(d)(iii).

¹⁵ 72 Fed Reg 63862 (9 November 2007).

¹⁶ 72 Fed. Reg 63762 (9 November 2007).

identity theft.¹⁷ The Guidelines set forth a list of factors to assist the financial institution in determining when the program needs updating. The Guidelines provide that the following relevant factors should be considered:

- The experiences of the financial institution with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts the financial institution offers or maintains; and
- Changes in the business arrangement of the financial institution (such as a merger).

Program Administration

The final element of the Program discussed in the Final Rules is program administration. The board of directors or appropriate committee of the board must approve the initial written Program. The Program must require that the board of directors or a board committee approve annual reports on compliance.¹⁸ On an ongoing basis, the Final Rules require the involvement of the board of directors, a board committee or a designated senior management level employee in the oversight, development, implementation and administration of the Program. However, in order to not impair the ability of the financial institution to update its Program in a timely manner, the Final Rules allow, at the discretion of the financial institution, for the board of directors, a board committee, or senior management to update the Program once it has received initial board approval.¹⁹

The Guidelines require that the board of directors (or designated committee or member of senior management) receive a report on compliance at least annually by the financial institution in accordance with section 12 CFR 344.90.²⁰ 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 in addressing the risk of identity theft in connection with the opening of Covered Accounts or with respect to existing Covered Accounts; and
- Recommendations for material changes to the Program.²¹

The financial institution's employees are required to receive appropriate training with respect to the Program.²² There is no corresponding section in the Guidelines that addresses training of employees. Finally, the financial institution must exercise appropriate and effective oversight of service provider arrangements.²³ The purpose of this final requirement is to make it clear that a financial institution may not evade its obligations to comply with any provisions of the Final Rules by outsourcing one or more activities.²⁴

Card Issuer Requirements

Additional or Replacement Cards

The Final Rules require credit or debit card issuers to resolve address discrepancies whenever they receive a request for an additional or replacement card.²⁵ The definition of a "Card Issuer" is set forth in the FCRA. The act by a financial institution of issuing its own debit and credit cards is sufficient to meet the definition.

The following definitions apply only to this section of the Final Rules:

¹⁷ 72 Fed. Reg. 63761 (9 November 2007), 12 CFR 334.90(d)(iv).

¹⁸ 72 Fed. Reg. 63861 (9 November 2007), 12 CFR 334.90(f)(1).

¹⁹ 72 Fed. Reg. 63730 (9 November 2007).

²⁰ 72 Fed. Reg. 63762 (9 November 2007).

²¹ 72 Fed. Reg. 63763 (9 November 2007).

²² 72 Fed. Reg. 63731 (9 November 2007).

²³ 72 Fed. Reg. 63761 (9 November 2007).

²⁴ 72 Fed. Reg. 63732 (9 November 2007).

²⁵ 12 CFR 334.91 implements FCRA section 615(e)(1)(C).

“Cardholder” means a consumer who has been issued a credit or debit card.²⁶ The preamble to the proposed rules provided that a Card Issuer could assess the validity of a “consumer” request for an additional or replacement card for an existing account by notifying the cardholder.²⁷ Note, however, that the term “consumer” is defined by the FCRA simply as an “individual.” Therefore, the Final Rules apply to any individual requesting an additional or replacement card, including a card for business purposes.²⁸ The Final Rules only apply to those types of cards that are covered by Regulation E. Therefore, gift cards and other prepaid card products are not covered by the Final Rules *unless and until* these types of cards are covered by an amendment to Regulation E. The Final Rules do apply to a recipient of a home equity loan, if the holder is able to access the proceeds of the loan with a credit or debit card.²⁹

“Clear and conspicuous” means reasonably understandable and designed to call attention to the nature and significance of the information presented.³⁰

Address Validation

12 CFR 334.91(c) sets forth requirements regarding address validation. Under the Final Rules, for a Card Issuer that receives an address change notification within thirty (30) days of a request for an additional or replacement card, the Card Issuer should not issue the additional or replacement card until it has notified the Cardholder or has otherwise assessed the validity of the change of address.³¹ The Final Rules provide two options to comply with this provision. The first option is to notify the Cardholder at the Cardholder’s former address or by any other means of communication that the Card Issuer and the Cardholder have previously agreed to use. The notice must provide the Cardholder with a reasonable means of promptly reporting an incorrect address change. The second option is for the Card Issuer to “otherwise assess the validity of the change of address in accordance with the policies and procedures the card issuer has established to comply with this rule.”³² Any notice provided under this provision must be “clear and conspicuous,” therefore, it must be provided separately from the Card Issuer’s regular correspondence with the Cardholder.³³

Address Discrepancies

Notice from Credit Reporting Agency

The Final Rules set forth certain steps that a financial institution is required to take upon receipt of a notice from a credit reporting agency of an address discrepancy. This section of the Final Rules applies to the users of consumer reports.³⁴

The following definition applies only to this section of the Final Rules:

“Notice of address discrepancy” means as a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1) 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 agency’s file for the consumer.³⁵

The FCRA and Final Rules leave the determination of what constitutes a “substantial difference” to the consumer reporting agency. When the financial institution receives a notice of an address discrepancy from a consumer reporting agency it must develop a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. Written policies and procedures must be in

²⁶ 72 Fed Reg 63761 (9 November 2007), 12 CFR 334.91(b)(1).

²⁷ 72 Fed Reg 63733 (9 November 2007).

²⁸ *Id.*

²⁹ 72 Fed Reg 63734 (9 November 2007).

³⁰ 72 Fed Reg 63761 (9 November 2007), 12 CFR 334.91(b)(2).

³¹ 72 Fed Reg 63734 (9 November 2007).

³² 72 Fed Reg 63762 (9 November 2007), 12 CFR 334.91(c) (1) and (2).

³³ 72 Fed Reg 63735 (9 November 2007).

³⁴ 12 CFR 334.82 implements FCRA section 605(h).

³⁵ 72 Fed Reg 63760 (9 November 2007), 12 CFR 334.82(b).

place to facilitate this determination.³⁶ Comments received in response to the proposed rule requested that this requirement be limited to situations in which the financial institution has established a continuing relationship with the consumer. However, the Final Rules reject this proposition, and the requirement applies to any notification from a consumer reporting agency regarding a substantial address discrepancy.³⁷ The Final Rules specifically state that if the financial institution employs the policies and procedures regarding identification and verification set forth in the CIP rules it would satisfy the requirement to have policies and procedures to verify the identify of the customer.³⁸ However, the CIP would need to be applied whenever the financial institution receives a notice of an address discrepancy. The commentary accompanying the Final Rules indicates that if the financial institution received a notice of address discrepancy in connection with a previously established account, the Agencies would not expect the financial institution to rely on the CIP rules a second time.³⁹

The Final Rules provide two examples of reasonable policies and procedures:

First, the financial institution may compare the information in the consumer report provided by the consumer reporting agency with information that the financial institution:

- Obtains and uses to verify the consumer's identity in accordance with the requirements of the CIP rules; or
- Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
- Obtains from third party sources.

Second, the financial institution may verify the information in the consumer report provided by the consumer reporting agency directly with the consumer.⁴⁰

If the financial institution cannot establish a reasonable belief that the consumer report relates to the consumer about whom it requested the report, the Agencies expect that the financial institution will not use that report.⁴¹

Furnishing a Consumer's Address to a Consumer Reporting Agency

The Final Rules require, in certain circumstances, that financial institutions furnish consumer addresses to consumer reporting agencies. The Agencies believe that the FCRA, implemented by these provisions in the Final Rules, is intended to enhance the accuracy of information relating to consumers. The requirement to furnish consumer addresses only applies when the financial institution receives a notice of address discrepancy when dealing with a newly established account.⁴² The Final Rules require the financial institution to have reasonable policies and procedures for furnishing an address for the consumer.

As a precondition to providing an updated consumer address, the financial institution must reasonably confirm that the address is accurate. The Final Rules provide the following examples of methods that the financial institution may use satisfy this requirement:

- Verifying the address with the consumer about whom it has requested the report;
- Reviewing its own records to verify the address of the consumer;
- Verifying the address through third-party sources; or
- Using other reasonable means.

Provided that the financial institution has reasonably confirmed that the address is accurate, it must provide the address to the consumer reporting agency from which it received the notice of address discrepancy when the following circumstances are met:

³⁶ 72 Fed Reg 63760 (9 November 2007), 12 CFR 334.82(c).

³⁷ 72 Fed Reg 63736 (9 November 2007).

³⁸ 72 Fed Reg 63736 (9 November 2007), 12 CFR 334.81(c)(2)(A).

³⁹ 72 Fed Reg 63737 (9 November 2007).

⁴⁰ 72 Fed Reg 63760 (9 November 2007), 12 CFR 334.82(c).

⁴¹ 72 Fed Reg 63737 (9 November 2007).

⁴² 72 Fed Reg 63738 (9 November 2007).

- The financial institution can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
- The financial institution establishes a continuing relationship with the consumer; and
- The financial institution 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.⁴³

The financial institution must respond to the consumer reporting agency in the same time period in which the financial institution regularly furnishes updates to the reporting agency and in which the financial institution establishes a continuing relationship with the consumer.⁴⁴ In other words, the financial institution will furnish the consumer's updated address during the next regular report that the financial institution provides to the reporting agency in question, after the financial institution has established the required relationship with the consumer.

Conclusion

With the adoption of the Final Rules and the mandatory compliance date approaching, financial institutions need to be actively developing their Program and the related policies and procedures required to comply with the provisions of the Final Rules. A working group, drawing on expertise throughout the organization, should be convened to identify and assess potential difficulties. For example, financial institutions may find that their core system may not interface with the system used to order debit and credit cards, leading to time intensive programming and/or the development of manual processes, which, if unanticipated, may delay compliance.

⁴³ 72 Fed Reg 63760 (9 November 2007), 12 CFR 334.82(d).

⁴⁴ 72 Fed Reg 63761 (9 November 2007), 12 CFR 334.82(d)(3).