

PIERCE
ATWOOD

— LLP —

ATTORNEYS AT LAW

“Red Flag” Regulations

**Maine Association of Community Banks
BANK EXPO 2008**

April 15, 2008

**PIERCE
ATWOOD**

— LLP —

ATTORNEYS AT LAW

Introduction

- A. The purpose of this presentation is to summarize the new “Red Flag” regulations.
- B. We will also provide a brief summary of the Fair and Accurate Credit Transactions Act (FACT Act) provisions that are the basis for the regulations.
- C. Finally, we will provide some pointers regarding compliance with the final rule.

Prologue

- A. Passage of the FACT Act in December of 2003 was preceded by a number of events highlighting identity theft as a pervasive and growing problem:
 - 1. Series of Congressional hearings regarding Fair Credit Reporting Act (FCRA) reauthorization. Last hearing dealt with role of FCRA in fighting identity theft.
 - 2. In September of 2003 the Federal Trade Commission (FTC) released the results of a detailed study regarding the impact and scope of ID Theft.
 - 3. Countless mainstream press articles on ID theft.
- B. Sections 114 and 315 of the FACT Act are the basis for the Red Flag regulations.

FACT Act Provisions

A. Section 114

1. Inserts subsection (e) in FCRA § 615.
2. Requires agencies to:
 - a. Establish and maintain guidelines regarding ID theft and to update them regularly. In developing such guidelines the agencies were instructed to identify “patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.”
 - b. Prescribe regulations requiring the establishment of “reasonable policies and procedures” to implement the guidelines “to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers.”

FACT Act Provisions

- c. Prescribe regulations requiring card issuers to delay fulfilling requests for additional or replacement cards received within a “short period of time” (min. 30 days) of an address change request unless the issuer:
 - i. Notifies the cardholder of the request at the old address and provides a means for “promptly reporting” incorrect address changes;
 - ii. Notifies the cardholder of the request by other means of communication previously agreed to; or
 - iii. Uses other means to assess the validity of the address change request.
- d. Develop (a) through (c) so that they are “not inconsistent” with CIP policies and procedures.

FACT Act Provisions

B. Section 315

1. Inserts a new subsection (h) in FCRA § 605.
2. Requires consumer reporting agencies to notify parties requesting consumer reports of substantial address discrepancies.
3. Directs agencies to develop regulations providing guidance on “reasonable policies and procedures” for financial institutions and creditors to follow upon receipt of a notice of address discrepancy, including:
 - a. Formation of a reasonable belief that user knows identity of consumer; and
 - b. Reconciliation of address with consumer reporting agency that provided the notice if a continuing relationship is established.

Rulemaking History

- A. Proposed version of Red Flag regulations published in July of 2006.
- B. Final rule was released by the regulatory agencies on October 31, 2007, and became effective January 1st.
- C. Mandatory compliance date: November 1, 2008.

Address Discrepancies

A. Definitions

1. Notice of Address Discrepancy: means a notice sent to a user by a consumer reporting agency that informs the user of a “substantial difference” (which is up to the agency) between the address for the consumer that the user provided to request the consumer report and the address(es) in the file at the consumer reporting agency for the consumer.
2. User: a user of a consumer report.

Address Discrepancies

- B. User Must Form Reasonable Belief: User must develop and implement reasonable policies and procedures that enable it to form a “reasonable belief” that the consumer report relates to the consumer about whom it requested the report when the user receives a notice of address discrepancy.
1. This obligation applies whenever a notice of address discrepancy is received – not just at account opening.
 2. Reasonable policies and procedures could include:
 - a. Verifying the information in the consumer report provided by the consumer reporting agency with the consumer; or

Address Discrepancies

- b. Comparing the information in the consumer report provided by the consumer reporting agency with information that the user:
 - i. Obtains and uses to verify the consumer's identity in accordance with its CIP;
 - ii. Maintains in its own records (such as applications, change of address notifications, other account records or retained CIP documentation); or
 - iii. Obtains from third party sources.

- c. If the user cannot establish a reasonable belief that the consumer report relates to the consumer about whom it requested the report, then:
 - i. The user should not use the report; and
 - ii. It should follow its procedures under its CIP and/or Identity Theft Prevention Program (discussed momentarily) for appropriate treatment of the subject account.

Address Discrepancies

C. Furnishing Confirmed Addresses: User must develop and implement reasonable policies and procedures for furnishing an address that it has reasonably confirmed is accurate to the consumer reporting agency that provided the notice of address discrepancy.

1. This reporting obligation arises when three (3) conditions are present:
 - a. User forms a reasonable belief that the consumer report relates to the consumer about whom the report was requested;

Address Discrepancies

- b. User establishes a continuing relationship with the consumer; and
 - c. User regularly and in the ordinary course of business furnishes information to the consumer reporting agency that provided the notice of address discrepancy.
2. User may reasonably confirm an address is accurate by:
- a. Verifying the address with the consumer;
 - b. Reviewing its own records;
 - c. Verifying the address through third-party sources; or
 - d. Using “other reasonable means”.

Address Discrepancies

3. The user must furnish the address it has reasonably confirmed as accurate to the consumer reporting agency that provided the notice of address discrepancy. It must do so as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

Identity Theft Prevention

A. Definitions

1. Board of Directors: the common definition of this term is expanded under the rule to include (a) the managing official in charge of a branch or agency of a foreign bank and (b) a designated senior management employee for creditors that do not have boards.

2. Covered Account: means any account that a financial institution or creditor offers or maintains:
 - a. That is primarily for personal, family, or household purposes that involves, or is designed to permit, multiple payments or transactions (such as a credit card, mortgage, auto loan, checking account, or savings account); and

Identity Theft Prevention

- b. That presents a reasonably foreseeable risk to customers (including business account customers) or to the safety and soundness of the financial institution or creditor from identity theft.
3. Customer: means a person that has a covered account with a financial institution or creditor. Preamble notes that this term has a broader meaning than in the Information Security Standards, and includes businesses.
4. Identity Theft: is defined by cross-reference to the definition found in FTC regulations at 16 CFR § 603.2(a) and means “a fraud committed or attempted using the identifying information of another person without authority.” Identifying information is any name or number that may be used (alone or in conjunction with other information) to identify a specific person. It includes any:

Identity Theft Prevention

- a. Name;
 - b. Date of Birth;
 - c. Identifying Numbers (SSN, EIN, TIN, official state or government issued driver's license or identification number, alien registration number, passport number);
 - d. Biometric data;
 - e. Unique electronic identification number, address, or routing code; or
 - f. Telecommunication identifying information or access device.
5. Red Flag: means a “pattern, practice, or specific activity that indicates the possible existence of identity theft.”

Identity Theft Prevention

B. Periodically Identify Covered Accounts: Each financial institution or creditor must periodically determine if it offers or maintains covered accounts. This determination process must include a risk assessment to determine if it maintains any accounts other than consumer accounts that might present a reasonably foreseeable risk of identity theft, taking the following points into consideration:

1. Methods it provides to open accounts;
2. Methods it provides to access its accounts; and
3. Its prior experiences with identity theft.

Identity Theft Prevention

- C. Identity Theft Prevention Program: Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program. This program may include existing policies and procedures, as appropriate. The Program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

Identity Theft Prevention

- D. Program Elements: Program development should be done in consultation with the Guidelines provided in Appendix J. Program should be risk-based and must include reasonable policies and procedures to cover the following four (4) elements:
1. Identification of Red Flags: The Program should identify relevant Red Flags for the covered accounts, and incorporate them into the Program.
 - a. The following factors should be considered by financial institutions and creditors in identifying relevant Red Flags:
 - i. Types of covered accounts offered or maintained;
 - ii. Methods provided to open covered accounts;
 - iii. Methods provided to access covered accounts; and
 - iv. Previous experiences with identity theft.

Identity Theft Prevention

- b. Financial institutions and creditors should incorporate relevant Red Flags from:
 - i. Their experiences with identity theft;
 - ii. Identity theft methods that reflect changes in identity theft risks; and
 - iii. Applicable supervisory guidance.

- c. Program should include relevant Red Flags from the following categories, as appropriate (examples are in Supplement A to Appendix J of final rule):
 - i. Alerts, notifications, or other warnings received from consumer reporting agencies and other vendors;
 - ii. Presentation of suspicious documents;
 - iii. Presentation of suspicious personal identifying information (e.g.: suspicious address change);
 - iv. Unusual use of, or other suspicious activity related to, a covered account; and
 - v. Notice from customers, victims of identity theft, law enforcement authorities, or other persons.

Identity Theft Prevention

2. Detection of Red Flags: The Program must contain policies and procedures to detect the Red Flags that it has determined are relevant and incorporated into its Program. These policies and procedures should address the detection of Red Flags for both the opening of covered accounts and existing covered accounts. This can be done by:
 - a. Obtaining identifying information about, and verifying the identity of, a person opening a covered account (for example, by using CIP policies and procedures regarding identification and verification).
 - b. Authenticating customers, monitoring transactions, and verifying the validity of address change requests for existing covered accounts.

Identity Theft Prevention

3. Responding to Red Flags: The Program must include reasonable policies and procedures to respond appropriately to the Red Flags detected to prevent and mitigate identity theft. The response should be commensurate with the degree of risk. This risk calculus should include consideration of potential aggravating factors that could heighten the risk of identity theft (such as a data security incident, or notice from the customer that s/he responded to a phishing scheme).
 - a. To respond appropriately, the financial institution or creditor must have a reasonable basis for concluding whether or not the presence of a Red Flag evidences a risk of identity theft.
 - b. A number of responses may be appropriate, including simply monitoring a covered account for evidence of identity theft, to closing (or not opening a new) covered account. However, when responding be mindful of other compliance obligations (such as ECOA compliance).

Identity Theft Prevention

4. Updating the Program: Financial institutions and creditors should update the Program (including the list of relevant Red Flags) periodically to reflect changes to the risk environment. No specific “update schedule” is required. Rather, updates should be based on factors including:
 - a. Experiences with identity theft;
 - b. Changes in identity theft methods;
 - c. Changes in the methods to detect, prevent, and mitigate identity theft;
 - d. Changes in the types of accounts the financial institution or creditor offers or maintains; and
 - e. Changes in the business arrangements of the financial institution or creditor (mergers, acquisitions, changes in vendors, etc.).

Identity Theft Prevention

E. Program Administration: The Program should be administered as follows:

1. The initial written Program must be approved by the Board of Directors or an appropriate board committee.
2. Either the Board of Directors, a board committee, or a designated senior management employee must be responsible for the oversight, development, implementation, and administration of the Program.
 - a. Note: Staff of the financial institution or creditor responsible for the development, implementation, and administration of the Program should provide annual reports to the Board of Directors, a committee of the board, or the responsible senior executive regarding matters material to the Program (such as its effectiveness, service provider arrangements, significant identity theft incidents, and suggestions material changes to the Program).

Identity Theft Prevention

3. Staff should be trained, as necessary, to implement the Program.
4. Financial institutions and creditors must exercise appropriate and effective oversight of service provider arrangements. It must be ensured that the activities of the service provider are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate identity theft.

Special Card Issuer Duties

A. Definitions

1. Cardholder: means a consumer that has been issued a credit card (including card access HELOCs) or debit card. Holders of gift cards and other prepaid products are not included in this definition.
2. Clear and Conspicuous: means “reasonably understandable and designed to call attention to the nature and significance” of the information in question.

Special Card Issuer Duties

- B. Address Validation: Card issuers must establish and implement reasonable policies and procedures to assess the validity of address changes that are followed shortly thereafter (at least the first 30 days after the address change) by a request for additional or replacement cards for the same account. The new or new or replacement cards may not be issued until:
1. The card issuer clearly and conspicuously notifies the cardholder at his/her former address (or by other means of communication previously agreed to) and provides the cardholder with a reasonable means of promptly reporting incorrect address changes; or

Special Card Issuer Duties

2. The card issuer otherwise assesses the validity of the address in accordance with the policies and procedures established as part of its Identity Theft Prevention Program.
- C. Alternative Timing: Card issuers may satisfy the address validation requirements discussed above when it receives notice of an address change, but before it receives a request for additional or replacement cards.

Compliance Pointers

- A. Program Development is Centerpiece: Although there are three (3) distinct regulatory requirements, the core requirement should be development of your Identity Theft Prevention Program.

- B. Appoint a Project Manager: Development of the Program will be an interdisciplinary affair that will require centralized management and ownership.

Compliance Pointers

C. Gather Your Facts: When developing your Program consider:

1. Talking to your security personnel regarding what early warning signs they would consider indicative of identity theft.
2. Talking to your consumer reporting agency contacts. Are there flags or services that you could purchase (or may already be purchasing) to help in this regard?
3. Reviewing the Guidelines found in Appendix J of the final rule, including the list of potential Red Flags found in Supplement A.
4. Reviewing your CIP policies and procedures. Do they need to be updated/revised in light of how they may be used in your Program?
5. Reviewing address change request procedures. Can these be tied in to card reorder requests?

Compliance Pointers

- D. Agent Banks: Banks that are agent banks for credit card issuers should discuss what role it will play in the duties that fall on the card issuer.

- E. Service Providers: Review your service provider relationships.

LEGAL STUFF:

Because of its generality, the information provided in this program may not be applicable to all situations and should not be acted upon without specific advice from your compliance officer or legal counsel.

If you have any questions concerning this program, please contact Ryan Stinneford at:

- (207) 791-1154
- rstinneford@pierceatwood.com