
The Red Flag Rules

Overview

To help combat identity theft, Congress enacted sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003 (FACTA). These final rules and guidelines became effective January 1, 2008 with mandatory compliance by November 1, 2008 (The FTC has extended enforcement of the deadline to May 1, 2009). (<http://www.ftc.gov/opa/2007/10/redflag.shtm>)

- Section 114 of the Act contains the Red Flag Rules that require businesses, including utilities, to develop and implement a written Identity Theft Prevention Program for combating identity theft in connection with certain accounts.

The program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable a utility to:

1. Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the plan;
2. Detect red flags that have been incorporated;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks.

It has been determined that while utility accounts are subject to this rule that many other municipal revenues such as property taxes, business licenses and police tickets are not subject to the rule. Because of this determination, training efforts by the Municipal Association will focus on utility accounts. However, the information learned in these training sessions will be applicable towards other municipal accounts.

- Section 315 requires that users of credit reports verify and report address discrepancies noted between what the credit reporting agency has on file and the information being collected by the utility. In addition, the final rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency.

Section 315 - Address Discrepancies

Duties of users of consumer reports regarding address discrepancies from 681.1

Users of credit reports have a responsibility to verify address information.

Credit reporting agencies must now provide a “notice of address discrepancy” when the address on file is substantially different from the address provided by the person requesting the report (or user).

Because of this, policies and procedures must be in place to:

1. Obtain a reasonable belief that a consumer report relates to the consumer about whom it has been requested when a notice of address discrepancy is received.

Examples of reasonable policies and procedures:

(A) *Comparing the information in the consumer report provided by the consumer reporting agency with information the user:*

- *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(l) (31 CFR 103.121);*
- *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; or*

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

2. Provide an address to the consumer reporting agency once it has been confirmed as accurate. Do this within a reasonable timeframe.

Examples of methods to reasonably confirm an address is accurate:

- (A) *Verify the address with the consumer about whom it has requested the report;*
- (B) *Review its own records to verify the address of the consumer;*
- (C) *Verify the address through third-party sources; or*
- (D) *Use other reasonable means.*

Section 114 - Red Flag Rules

Section 114 Guidelines on Identity Theft Detection, Prevention, and Mitigation

This rule requires each creditor that offers or maintains one or more covered accounts to develop and provide for the continued administration of a written Program 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 creditors in the formulation and maintenance of a Program that satisfies the requirements.

I. The Program

In designing its Program, a 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 creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors*. A 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;
- (2) The methods it provides to open its covered accounts;
- (3) The methods it provides to access its covered accounts; and
- (4) 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 creditor has experienced;
- (2) Methods 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.

- (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 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(l)* (*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 creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a 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 creditor to someone fraudulently claiming to represent the 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; or
- (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 creditor from identity theft, based on factors such as:

- (a) The experiences of the 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 creditor offers or maintains; and
- (e) Changes in the business arrangements of the 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 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 the 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 creditor with § 681.2 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the 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 creditor engages a service provider to perform an activity in connection with one or more covered accounts the 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 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 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 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.

Section 114 Appendix A - Illustrative Examples of Red Flags

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines, each 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 consumer 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 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 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 and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the 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 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 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 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 account number 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 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 creditor is notified that the customer is not receiving paper account statements.
25. The 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 Creditor

26. The 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.

Definitions and other excerpts from the Federal Register “*Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*”

Overview of Section 114:

Creditors that offer or maintain "covered accounts" must develop and implement a written Program. A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) **any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.** Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."

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. In addition, the Program must be tailored to the entity's size, complexity and nature of its operations. [*63720]

The final regulations list the four basic elements that must be included in the Program of a creditor. The Program must contain "reasonable policies and procedures" to:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The regulations also enumerate certain steps that creditors must take to administer the Program. These steps include obtaining approval of the initial written Program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the Program, training staff, and overseeing service provider arrangements.

In order to provide creditors with more flexibility in developing a Program, the Agencies have moved certain detail formerly contained in the proposed regulations to the guidelines located in Appendix J. This detailed guidance should assist in the formulation and maintenance of a Program that satisfies the requirements of the regulations to detect, prevent, and mitigate identity theft. Each creditor that is required to implement a Program must consider the guidelines and include in its Program those guidelines that are appropriate.

The guidelines provide policies and procedures for use by institutions and creditors, where appropriate, to satisfy the requirements of the final rules, including the four elements listed above. While a creditor may determine that particular guidelines are not appropriate to incorporate into its Program, the Program must nonetheless contain reasonable policies and procedures to meet the specific requirements of the final rules. The illustrative examples of Red Flags formerly in Appendix J are now listed in a supplement to the guidelines.

Note: financial institution was removed from the above language to increase readability.

Definition of Account .90(b)(1)

Account covers any relationship to obtain a product or service that an account holder or customer may have with a financial institution or creditor. Through examples, the definition makes clear that the purchase of property or services involving a deferred payment is considered to be an account.

The Agencies also recognize that a person may establish a relationship with a creditor, such as an automobile dealer or a telecommunications provider, primarily to obtain a product or service that is not financial in nature. To make clear that an "account" includes relationships with creditors that are not financial institutions, the definition is no longer tied to the provision of "financial" products and services. Accordingly, the Agencies have deleted the reference to the Bank Holding Company Act.

Definition of Covered Account .90(b)(3)

The Agencies recognize that consumer accounts are presently the most common target of identity theft and acknowledge that Congress expected the final regulation to address risks of identity theft to consumers. n13 For this reason, the final rules require each Program to cover accounts established primarily for personal, family or household purposes, that involve or are designed to permit multiple payments or transactions, *i.e.*, consumer accounts. As discussed above in connection with the definition of "account," the final rules also require the Programs of to cover any other type of account that the institution or creditor offers or maintains for which there is a reasonably foreseeable risk from identity theft.

Accordingly, the definition of "covered account" is divided into two parts. The first part refers to "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." The definition provides examples to illustrate that these types of consumer accounts include, "a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account." n14

n14 These examples reflect the fact that the rules are applicable to a variety of financial institutions and creditors. They are not intended to confer any additional powers on covered entities. Nonetheless, some of the Agencies have chosen to limit the examples in their rule texts to those products covered entities subject to their jurisdiction are legally permitted to offer.

The second part of the definition refers to "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." This part of the definition reflects the Agencies' belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft, and, therefore, should be considered for coverage by the Program of a financial institution or creditor.

Definition of Creditor .90(5)

Sections .90(b)(4) and (b)(5) Credit and Creditor. The proposed rules defined these terms by cross-reference to the relevant sections of the FCRA. There were no comments on the definition of "creditor" and § .90(b)(4) of the final rules adopts the definition as proposed.

Some commenters asked the Agencies to clarify that the term "creditor" does not cover third-party debt collectors who regularly arrange for the extension, renewal, or continuation of credit.

Section 114 applies to financial institutions and creditors. Under the FCRA, the term "creditor" has the same meaning as in section 702 of the Equal Credit Opportunity Act (ECOA), *15 U.S.C. 1691a*. n15 ECOA defines "creditor" to include a person who arranges for the extension, renewal, or continuation of credit, which in some cases could include third-party debt collectors. *15 U.S.C. 1691a(e)*. Therefore, the Agencies are not excluding third-party debt collectors from the scope of the final rules, and § .90(b)(5) of the final rules adopts the definition of "creditor" as proposed.

Definition of Customer .90(b)(6)

The proposed definition of "customer" applied to any "person," defined by the FCRA as any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity. n16 The proposal explained that the Agencies chose this broad definition because, in addition to individuals, various types of entities (*e.g.*, small businesses) can be victims of identity theft. Under the proposed definition, however, a financial institution or creditor would have had the discretion to determine which type of customer accounts would be covered under its Program, since the proposed regulations were risk-based. n17

Section .90(b)(6) of the final rule defines "customer" to mean a person that has a "covered account" with a financial institution or creditor. Under the definition of "covered account," an individual who has a consumer account will always be a "customer." A "customer" may also be a person that has another type of account for which a financial institution or creditor determines there is a reasonably foreseeable risk to its customers or to its own safety and soundness from identity theft.

The definition of "customer" in the final rules continues to cover only customers that already have accounts. The Agencies note, however, that the substantive provisions of the final rules, described later, require the Program of a financial institution or creditor to detect, prevent, and mitigate identity theft in connection with the opening of a covered account as well as any existing covered account. The final rules address persons whose identities are

used by an imposter to open an account in these substantive provisions, rather than through the definition of "customer."

Definition of Identity Theft .90(b)(8)

Section __.90(b)(8) of the final rules adopts the definition of "identity theft" as proposed. The Agencies believe that it is important to ensure that all provisions of the FACT Act that address identity theft are interpreted in a consistent manner. Therefore, the final rule continues to define identity theft with reference to the FTC's regulation, which as currently drafted provides that the term "**identity theft**" means "**a fraud committed or attempted using the identifying information of another person without authority.**" n19 The FTC defines the term "**identifying information**" to mean "**any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any--**

n19 See 16 CFR 603.2(a).

(1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Thus, under the FTC's regulation, the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of "identity theft" because such a fraud involves "using the identifying information of another person without authority." n20

Definition of Service Provider .90(b)(10)

Section __.90(b)(10) *Service Provider*. The proposed regulations defined "service provider" as a person that provides a service directly to the financial institution or creditor. This definition was based upon the definition of "service provider" in the Information Security Standards. n23

The Information Security Standards define "service provider" to mean any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through the provision of services directly to the financial institution.

The Agencies have interpreted section 114 broadly to require each financial institution and creditor to detect, prevent, and mitigate identity theft not only in connection with any existing covered account, but also in connection with the opening of an account.

A financial institution or creditor is ultimately responsible for complying with the final rules and guidelines even if it outsources an activity to a third-party service provider. Thus, a financial institution or creditor that uses a service provider to open accounts will need to provide for the detection, prevention, and mitigation of identity theft in connection with this activity, even when the service provider has access to the information of a person who is not yet, and may not become, a "customer."

Section __.90(c) **Periodic Identification of Covered Accounts**

To simplify compliance with the final rules, the Agencies added a new provision in § __.90(c) that requires each financial institution and creditor to periodically determine whether it offers or maintains any covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it [*63724] offers or maintains covered accounts described in § __.90(b)(3)(ii) (accounts other than consumer accounts), taking into consideration:

- . The methods it provides to open its accounts;
- . The methods it provides to access its accounts; and
- . Its previous experiences with identity theft.

Thus, a financial institution or creditor should consider whether, for example, a reasonably foreseeable risk of identity theft may exist in connection with business accounts it offers or maintains that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the internet or telephone. In

addition, those institutions and creditors that offer or maintain business accounts that have been the target of identity theft should factor those experiences with identity theft into their determination.

This provision is modeled on various process-oriented and risk-based regulations issued by the Agencies, such as the Information Security Standards. Compliance with this type of regulation is based upon a regulated entity's own preliminary risk assessment. The risk assessment required here directs a financial institution or creditor to determine, as a threshold matter, whether it will need to have a Program. n24 If a financial institution or creditor determines that it does need a Program, then this risk assessment will enable the financial institution or creditor to identify those accounts the Program must address. This provision also requires a financial institution or creditor that initially determines that it does not need to have a Program to reassess periodically whether it must develop and implement a Program in light of changes in the accounts that it offers or maintains and the various other factors set forth in the provision.

n24 The Agencies anticipate that some financial institutions and creditors, such as various creditors regulated by the FTC that solely engage in business-to-business transactions, will be able to determine that they do not need to develop and implement a Program.

Section .90(d) of the final rules requires each financial institution or creditor that offers or maintains one or more covered accounts to develop and implement a written 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. To signal that the final rules are flexible, and allow smaller financial institutions and creditors to tailor their Programs to their operations, the final rules state that the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

The guidelines are appended to the final rules to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the regulation. Section I of the guidelines, titled "The Program," makes clear that a covered entity may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program. This will avoid duplication and allow covered entities to benefit from existing policies and procedures.

Overview of Section 315 of the FACT Act:

Section 605(h)(2) requires the Agencies to issue joint regulations that provide guidance regarding reasonable policies and procedures a user of a consumer report should employ when the user receives a notice of address discrepancy. These regulations must describe reasonable policies and procedures for a user of a consumer report to employ to enable it to form a reasonable belief that the user knows the identity of the person for whom it has obtained a consumer report, and (ii) reconcile the address of the consumer with the CRA, if the user establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the CRA.

Proposed § .82(a) noted that the scope of section 315 differs from the scope of section 114 and explained that **section 315 applies to "users of consumer reports" and "persons requesting consumer reports" (hereinafter referred to as "users"), as opposed to financial institutions and creditors. Therefore, section 315 does not apply to a financial institution or creditor that does not use consumer reports.** The Agencies did not receive any comments on this section and have adopted it as proposed in the final rules.

The purpose of section 315 is to enhance the accuracy of consumer information, specifically to ensure that the user has obtained the correct consumer report for the consumer about whom it has requested such a report. To implement this concept more clearly, § .82(c) of **the final rules provides that 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.** n47