



---

## Do the Red Flag Rules apply to MASCO and/or Municipalities?

Prepared by: Stephanie O’Cain, CFO-MASCO

**Summary:** According to a report of the President’s Identity Theft Task Force, identity theft (a fraud attempted or committed using identifying information of another person without authority), results in billions of dollars in losses each year to individuals and businesses.

The final rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor 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 Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks from identity theft.

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. Effective Date: The joint final rules and guidelines are effective January 1, 2008. The mandatory compliance date for this rule is November 1, 2008. (<http://www.ftc.gov/opa/2007/10/redflag.shtm>)

**Conclusion:** It appears that all businesses, including MASCO and municipalities, will need to walk through the analysis of whether they obtain personal identification information in accordance with the red flag rules. In addition, policies and procedures should be implemented to support the rules as well as future evaluations. It is clear that utilities and the Collection programs fall under these rules, but other situations are more interpretative. An account is defined as one with a deferred payment, but a creditor is not fully defined. These are two key terms throughout the document and on the surface appear to define who this applies. Upon further review, however, the document implies that other types of accounts are eligible as well. Regardless, these are good business practices that all entities should adhere.

Municipalities and MASCO should use the FTC website guidelines along with the Red Flag Rules to implement programs that meet these guidelines. The Program should be modified to include requirements of SC S453 “Financial Identity Fraud and Identity Theft Protection Act” adopted on April 2, 2008 and effective for December 31, 2008.

<p><b>Overview of Section 114:</b></p> <p>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) <b>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.</b> Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."</p> <p>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]</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;</li> <li>• Detect Red Flags that have been incorporated into the Program;</li> <li>• Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and</li> <li>• 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.</li> </ul> <p>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.</p> <p>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.</p> <p>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.</p> <p><i>Note: financial institution was removed from the above language to increase readability.</i></p>	<p>The definition of creditor determines whether or not an entity must comply, but the reference to "accounts for which there is a reasonable foreseeable risk to the customers or the safety and soundness of the creditor from identity theft" is found throughout the documents which seem to include both creditors and non-creditors.</p>
<p><b>Definition of Account .90(b)(1)</b></p> <p>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.</p>	<p>"Primarily to obtain a product or service that is not financial in nature" is included in the definition of account which implies that this is not limited to</p>

<p><b>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</b>, 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.</p>	<p>only utilities.</p>
<p><b>Definition of Covered Account .90(b)(3)</b></p> <p>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>i.e.</i>, 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.</p> <p>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</p> <p>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.</p> <p>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.</p>	<p>This section focuses on personal versus business and other accounts. The final rules basically encompass them all.</p>
<p><b>Definition of Creditor .90(5)</b></p> <p><i>Sections .90(b)(4) and (b)(5) Credit and Creditor.</i> The proposed rules defined these terms by cross-reference to the relevant sections of the FCRA. There were no comments on the definition of "credit" and § .90(b)(4) of the final rules adopts the definition as proposed.</p> <p>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.</p> <p>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.</p>	<p>Creditor is a key term in this document. The FCRA definition needs to be determined. On the surface, it appears that MASC &amp; municipalities would be subject to this if they had accounts of any type.</p> <p>In addition, other areas of the document suggest that these rules apply regardless of the creditor definition.</p>

<p><b>Definition of Customer .90(b)(6)</b></p> <p>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</p> <p>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.</p> <p>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."</p>	
<p><b>Definition of Identity Theft .90(b)(8)</b></p> <p>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 <b>"identity theft" means "a fraud committed or attempted using the identifying information of another person without authority."</b> n19 The FTC defines the term <b>"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--</b></p> <p>n19 See 16 CFR 603.2(a).</p> <p>(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;</p> <p>(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;</p> <p>(3) Unique electronic identification number, address, or routing code; or</p> <p>(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).</p> <p>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</p>	<p>Interestingly, bank account numbers are not included on this list. It is, however, something that should be considered.</p>

<p><b>Definition of Service Provider .90(b)(10)</b></p> <p><i>Section __.90(b)(10) Service Provider.</i> 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</p> <p><b>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.</b></p> <p>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.</p> <p><b>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.</b> 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."</p>	<p>Third party vendors such as the collection programs provided by MASC and RMS' claims processors are included in this definition.</p> <p>What kinds of third party relationships do our members have?</p>
<p><i>Section __.90(c) <b>Periodic Identification of Covered Accounts</b></i></p> <p>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:</p> <ul style="list-style-type: none"> <li>• . The methods it provides to open its accounts;</li> <li>• . The methods it provides to access its accounts; and</li> <li>• . Its previous experiences with identity theft.</li> </ul> <p>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.</p> <p>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.</p> <p>n24 The Agencies anticipate that some financial institutions and creditors, such as</p>	<p>It appears that all entities will need to walk through an analysis process to identify these items.</p>

<p>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.</p>	
<p><b>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.</b> 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.</p> <p>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.</p>	
<p><b>Overview of Section 315 of the FACT Act:</b></p> <p>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.</p> <p>Proposed § 82(a) noted that the scope of section 315 differs from the scope of section 114 and explained that section <b>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.</b> The Agencies did not receive any comments on this section and have adopted it as proposed in the final rules.</p> <p>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 <b>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.</b> n47</p>	<p>Only applies to groups using credit reports.</p> <p>MASC uses credit reports for new hires, therefore it will need to develop a policy and follow these guidelines.</p>
<p>Resources: Excerpts from above are from the Federal Register <i>“Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule”</i></p>	