

“Red Flag” Rules and Aging Services:
What You Need to Know

Late in 2007, six federal agencies, including the Federal Trade Commission (“FTC”), jointly issued final rules and accompanying guidelines to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”). These so-called “Red Flag Rules” (the “Rules” or “Red Flag Rules”) require financial institutions and creditors to establish and implement a written identity theft prevention program to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. The Rules also require users of consumer reports, such as credit reports, to develop and implement reasonable policies and procedures for situations in which a consumer reporting agency sends the user a notice of address deficiency with respect to a consumer. Although the Rules became effective on January 1, 2008, they will not be enforced by the FTC until May 1, 2009.

A. Applicability; Definitions; Application.

1. Applicability

The Rules, as promulgated by the FTC in 16 C.F.R. Part 681, have applicability to aging services providers that defer payment for services rendered. Such providers are considered to be “Creditors” under the Rules. Specifically, the FTC’s version of the Rules applies to “Creditors” that offer or maintain one or more “Covered Accounts.” Section 2 below defines the terms that are relevant to the applicability analysis.

2. Definitions.

“Account” is defined in Section 681.2(b)(1) as “a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes,” and includes (i) *an extension of credit involving a deferred payment*, and (ii) a deposit account.

“Covered Account” is defined in Section 681.2(b)(3) as (i) 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, 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 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.

“Credit” is defined in Section 681.2(b)(4) of the Rules as having the same meaning as in 15 U.S.C. § 1681a(r)(5). Section 1681a(r)(5), in turn, refers to 15

U.S.C. 1691a(d), which defines the term as “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.”

“Creditor” is defined in Section 681.2(b)(5) of the Rules as having the same meaning as in 15 U.S.C. § 1681a(r)(5). Section 1681a(r)(5), in turn, refers to 15 U.S.C. 1691a(e), which defines the term to include “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.”

3. Applicability Analysis in the Context of Aging Services

Attached to this document is a decision tree that can be used by aging services providers to determine whether their organization is covered by the Red Flag Rules. To the extent that the organization creates an account for a senior and bills him or her for services after such services have been rendered, the provider organization qualifies as a creditor under the Rules. According to the FTC, if the provider accepts insurance, it will be deemed to be a creditor if the senior covered by the insurance is ultimately responsible for any charges incurred.

To the extent that the account is offered for the senior’s personal (the most likely purpose), family or household purposes and is designed to permit multiple payments or transactions, the provider organization is considered to maintain a “covered account” and thus is subject to the requirements of the Red Flag Rules. In the unlikely event that the provider’s accounts are not “covered accounts” under the above analysis, they may still qualify as “covered accounts” if there is a reasonably foreseeable risk to (a) the seniors served by the provider, or (b) the safety and soundness of the provider organization, from identity theft, including financial, operational, compliance, reputation or litigation risks. To determine whether this is the case, the provider will need to undertake a comprehensive risk assessment analysis. Section 681.2(c) of the Rules requires provider organizations to undertake this risk assessment periodically to determine whether they offer or maintains covered accounts, taking into consideration (i) the methods they provide to open accounts, (ii) the methods they provide to access accounts, and (iii) previous experiences with identity theft.

Finally, although the aging services provider’s focus will be on the accounts of the seniors they serve, providers should also consider employee accounts as possible sources of identity theft. This would include 401(k) or 403(b) accounts of employees.

B. Risk Assessment.

Section 681.2(c) governs the steps that must be taken to satisfy the requirement that a creditor periodically determine whether it offers or maintains covered accounts. Specifically, the creditor must conduct a risk assessment that looks at (1) the methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) its previous experiences with identity theft. Reviewing and analyzing each of these areas, as well as looking at the types of covered accounts it maintains, will provide valuable insight into vulnerabilities for identity theft and will indicate the direction that the creditor must follow in addressing the vulnerabilities. While not all of these risk factors will present a problem for aging services providers, they should nevertheless be considered and documented as part of the risk analysis. In order to incorporate multiple perspectives and perform a comprehensive risk assessment, it is best to take a team approach to the task, including members from many departments within the organization.

C. Identity Theft Protection program.

Once a creditor's vulnerabilities are identified through a risk assessment, Section 681.2(d) of the Red Flag Rules calls for the establishment of a written identity theft program. The program must be designed to detect, prevent and mitigate the incidence of identity theft with respect to the covered account(s) offered or maintained by the creditor. In an effort to make the Rules as flexible and scalable as possible, the FTC states specifically that the program should be appropriate to the size and complexity of the creditor as well as to the nature and scope of its activities. As a result, the type of identity theft program required by the Rules for aging services providers will differ from provider to provider based on a number of factors.

1. Required Elements.

Despite the flexibility and scalability of the Rules, Section 681.2(d)(2), nevertheless, prescribes four basic elements that must be a part of each program: The creditor must (i) identify relevant red flags for the covered account(s) and incorporate those red flags into its program; (ii) detect the identified red flags; (3) respond appropriately to any red flags that are detected to prevent and mitigate identity theft, and (iv) ensure that the program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft. Additionally, Section 681.2(f) mandates that creditors also consider guidelines specified in Appendix A to the Rules and include in their program those guidelines that are appropriate.

a. Appendix A Guidelines.

i. Existing Policies and Procedures.

Creditors may use existing policies and procedures that control reasonably foreseeable risks to customers or to the safety and soundness of the creditor from identity theft. In the case of aging services providers covered by the HIPAA security rule, policies and procedures put in place to comply with that rule can be used as a starting point to develop policies and procedures for the Red Flag Rules.

ii. Sources of Red Flags. There are three (3) primary resources from which creditors can obtain information about red flags:

- I) Past incidents of identity theft experienced by the creditor
- II) Methods of identity theft that the creditor has identified that reflect changes in identity theft risk
- III) Applicable supervisory guidance – This would include published guidance from outside sources, including the FTC.

iii. Categories of Red Flags. The program should include red flags from **each** of the following categories.

- I) Alerts, notifications or other warnings received from consumer reporting agencies/service providers. This category includes anything suspicious revealed by credit checks or other sources of credit-related information. Some examples of this category of red flags include:
 - A fraud or active duty alert is included with a consumer report
 - A notice of credit freeze issued in response to a request for a credit report
 - A notice of address discrepancy is received
 - A credit report indicates a pattern of activity that is inconsistent with the history and usual pattern of

activity established by the subject of the report. This can include a recent, significant increase in the volume of inquiries, an unusual number of recently established credit relationships, a material change in the use of credit that is not otherwise explained, or a notice that an account was closed for cause or identified for abuse of account privileges.

Accordingly, it becomes incumbent upon the aging services provider to undertake a thorough review of a senior's credit report in order to identify possible red flags. No longer is it acceptable merely to look at the bottom line of a credit report and file it away.

II) The presentation of suspicious documents

- Identification documents, such as medical records, appear to have been altered or forged or are otherwise inconsistent with other records or a physical examination of the senior.
- The photograph or physical description on the identification is not consistent with the appearance of the senior or his/her family member, as the case may be.
- Other information on the identification is not consistent with readily accessible information on file with the creditor, such as a signature or recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

Again, more than a cursory review of all documentation with respect to a senior is required. Policies and procedures for staff should reflect the degree of thoroughness required to identify red flags.

III) The presentation of suspicious personal identifying information. This would include the following:

- An address that doesn't match any address in a credit report or other document.

- The Social Security Number (“SSN”) has not been issued or is listed on the Social Security Administration’s “Death Master File.”
 - Personal identifying information provided by the senior is not consistent with other personal identifying information provided by the senior. The example given by the FTC is where there is no correlation between a person’s SSN range and the person’s date of birth.
 - Personal identifying information given by a senior is associated with known fraudulent activity. This would be the case where the provider’s own information or information from a third party alerts the provider to the use of fraudulent information.
 - Personal identifying information given by a senior is of a type commonly associated with fraudulent activity. This would be case where the address given is fictitious, a mail drop, a prison or a hotel, or where a phone number is invalid or is associated with a pager or answering service.
 - The SSN provided by the senior is the same as another senior.
 - The senior or the senior’s family member or other representative fails to provide all required personal identifying information in response to notification that the information is incomplete. This would be the case where a senior or family member provides an insurance policy number but cannot produce a written policy or insurance card.
- IV) The unusual use of, or other suspicious activity related to, a covered account.
- V) Notice from seniors or their families, victims of identity theft, law enforcement authorities, or others regarding possible identity theft in connection with accounts held by the provider. This is the most significant source of information about red flags. Specific examples in the health care field include the following:
- A senior questions or complains about receiving a bill or health insurance Explanation of Benefits for (i)

another person, (ii) products or services never received by the senior, (iii) a healthcare provider that the senior never saw.

- A senior receives a collection notice from a bill collector.
- Coverage by an insurer of a legitimate hospital stay by the senior is denied because the senior's insurance benefits have been depleted or a lifetime cap has been reached when the senior's medical history or records do not indicate anything to that effect.
- A senior questions or complains about information added to the senior's credit report by a healthcare provider or insurer.
- A notice or inquiry from an insurance fraud investigator, federal healthcare agency or law enforcement agency.

iv. Detecting Red Flags

- I) Obtaining identifying information about, and verifying the identity of a person opening a covered account
- II) Authenticating the identity or seniors, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

v. Preventing and Mitigating Identity Theft – This part of the program involves policies and procedures aimed at appropriately responding to red flags in a manner that is commensurate with the degree of risk posed. The degree of risk is increased by certain aggravating factors, such as a data security incident that results in unauthorized access to a senior's account records held by the provider, or notice that a senior has provided information about his or her account to someone fraudulently claiming to represent the provider or to a website representing that it is maintained by the provider. In such circumstances, appropriate responses by the provider include the following:

- Monitoring the senior's account for evidence of identity theft.
- Contacting the senior.

- Changing any passwords, security codes, or other security devices that permit access to the account.
- Reopening the senior's account with a new number.
- Not opening a new account.
- Closing the existing account.
- Not attempting to collect on the account or not selling the account to a debt collector.
- Notifying law enforcement.
- Determining that no response is necessary under the particular circumstances.

In each case, the response, and the reason(s) therefor, should be documented.

vi. Updating the Program – The program should be updated periodically to reflect changes in risk, both to seniors and the provider. Factors to be evaluated include the following:

- The experiences of the provider with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent and mitigate theft.
- Changes in the types of accounts that the provider maintains with respect to seniors.
- Changes in the business arrangements of the provider, such as vendor contracts, other service providers, etc.

vii. Methods for Administering the program

- Oversight – Responsibility for oversight of the program should be vested with the Board of Directors (or an appropriate committee of the board), or a senior-level employee. In most cases, this would be the executive director of the provider organization. Duties of the overseer include assigning specific responsibility for implementation of the program, reviewing reports from staff with respect to compliance with the requirements of the program, and approving material changes

to the program as necessary to address changing identity theft risks. In the long-term care context, responsibility for implementation and administration of the program should be given to the compliance officer or the staff member responsible for compliance with the HIPAA privacy and security rules. In most cases, the requirements of the Red Flag Rules can be dovetailed with the aforementioned compliance programs.

- Reports – Staff of the provider responsible for development, implementation and administration of the program should report to the person or entity having oversight over the program at least annually regarding compliance with the requirements of the Red Flag Rule. Specifically, the report should evaluate (i) the effectiveness of the policies and procedures designed to address the risk of identity theft, (ii) service provider arrangements, (iii) incidents of identity theft and the organization’s response to them, and (iv) recommendations for material changes to the program.
- Training – Relevant staff should be trained, as necessary, to effectively implement the program. Training should be documented.
- Oversight of service provider arrangements – This provision deals with any business arrangements a provider may have with other service providers in connection with seniors’ accounts. For instance, a provider might contract out its accounting or other financial functions to a third party. If this is the case, the provider should ensure that the activities of the third party are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, much as is the case with Business Associates under the HIPAA privacy rule.

D. Address Discrepancy Requirements. To the extent that an aging services provider uses credit reports during the course of the application or admissions process, the provider will be required to comply with the address discrepancy provisions of the Rules at 16 C.F.R. §681.1, which became effective and enforceable on November 1, 2008. The provisions apply in situations where there is a substantial difference between the address given to the provider by the senior and the address maintained by the credit reporting agency. The address discrepancy requirements require the provider to develop and implement policies and procedures designed to enable it to form a reasonable belief that the credit report relates to the person about whom it was requested. Specifically, in the event of a discrepancy, a provider will be required to compare information about the senior in its files to that of the credit reporting agency, and to provide the agency with the address that the provider has reasonably confirmed is accurate.

- E. Penalties for Noncompliance. Civil monetary penalties may be assessed by the FTC against providers who violate the Red Flag Rules. In addition, any enforcement action by the FTC may trigger scrutiny of the provider by HHS for any related violations of the HIPAA security rule.

- F. Additional Resources: <http://ftc.gov/bcp/edu/pubs/articles/art11.shtm> (The “Red Flag” Rule: What Health Care Providers Need to Know about Complying with the New Requirements for Fighting Identity Theft).

