NEW FTC “RED FLAG” REQUIREMENTS AS APPLICABLE TO “CREDITORS” AND “COVERED ACCOUNTS”

Last Updated: August 14, 2008

SUMMARY

The new “Red Flag” rule, finalized in November 2007, goes into effect on November 1, 2008. The rule was promulgated after public comment as required under the FACT Act, signed into law on December 4, 2003.¹ The FACT Act added several new provisions to the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. 1681 et seq. Section 114 of the FACT Act, 15 U.S.C. 1681m(e), amends section 615 of the FCRA, and directs the various banking regulators and the Federal Trade Commission (FTC) to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft.

The FTC regulations will apply to non-financial institutions that may engage in the extension of credit within the meaning of the new rules, and therefore this analysis is limited to those provisions and aspects of the new rule within the jurisdiction of the FTC.

On July 18, 2006, the banking regulators and the FTC published a joint notice of proposed rulemaking (NPRM) in the Federal Register (71 FR 40786) proposing rules and guidelines to implement section 114 and proposing rules to implement section 315 of the FACT Act. The public comment period closed on September 18, 2006. The agencies collectively received a total of 129 comments in response to the NPRM.

The new rule requires creditors to implement “a program to detect, prevent, and mitigate instances of identity theft”. The program, if required, must be in place by November 1, 2008, and “must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft”.²


² The rule states: “Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (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.”
FTC staff has emphasized the intended flexibility of the new rule as the rule applies to business accounts and the determination of the risk of identity theft relating to such accounts.

**ANALYSIS**

The operative definitions in the new rule center on the words “creditor” and “covered account”. Only a “creditor” that “maintains one or more covered accounts” is subject to the new rule.

Therefore, to determine if an entity is covered by the new Red Flag rule, a two-step process is recommended: first, to determine if the entity is a “creditor” within the meaning of the rule, and second, to determine if the entity as a “creditor” maintains a “covered account” within the meaning of the rule.³ -

1. **ARE YOU A “CREDITOR”?**

The final rule adopts the statutory definitions of “creditor” and “credit” found at 15 U.S.C. 1681a(r)(5).⁴

The term “creditor” is therefore defined by statute to mean -

> The term “creditor” means 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.

The term “credit” is likewise defined by statute to mean -

> The term “credit” means 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.⁵

The FTC restates this in its discussion of the final rule (emphasis added)⁶ -

---

³ This analysis should in no way be considered a legal opinion by NLBMDA.


⁵ See 15 U.S.C. 1691a for the definition of “credit”.

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

If an entity does fall within the meaning of “creditor” as defined by the new rule, the next inquiry will be to determine if that entity maintains a “covered account”.

2. **DO I MAINTAIN A “COVERED ACCOUNT”?**

The final rule provides the following definition for “covered account” (emphasis added) –

(3) *Covered account* means:

(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.

The FTC restates this definition in its discussion of the final rule (emphasis added)⁷ –

_A covered account_ is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. **Covered accounts** include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

---

If as a “creditor” as defined by the new rule, an entity maintains a “covered account” as defined by the new rule, that entity will be subject to the requirements of the new rule: to develop a written program that identifies and detects the relevant warning signs - or “red flags” - of identity theft.

For guidance of these requirements, read more below.

PRESS RELEASE OF RED FLAG RULE FROM THE FTC

The following text is posted on the FTC web page (underlining added for emphasis):

New ‘Red Flag’ Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft

Identity thieves use people's personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. Financial institutions and creditors soon will be required to implement a program to detect, prevent, and mitigate instances of identity theft.

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by November 1, 2008, and must provide for the identification, detection, and response to patterns, practices, or specific activities - known as “red flags” - that could indicate identity theft.

Who must comply with the Red Flags Rules?

The Red Flags Rules apply to “financial institutions” and “creditors” with “covered accounts.”

Under the Rules, a financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC’s jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A transaction account is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

---

8 This text may be found at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.
A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A **covered account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. **Covered accounts** include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

**Complying with the Red Flags Rules**

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs – or “red flags” – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

**How flexible are the Red Flags Rules?**

The Red Flags Rules provide all financial institutions and creditors the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. Guidelines issued by the FTC, the federal banking agencies, and the NCUA ([www.ftc.gov/opa/2007/10/redflag.shtm](http://www.ftc.gov/opa/2007/10/redflag.shtm)) should be helpful in assisting covered entities in designing their programs. A supplement to the Guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point.

They fall into five categories:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of – or suspicious activity relating to – a covered account; and
notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

More detailed compliance guidance on the Red Flags Rules will be forthcoming. For questions about compliance with the Rules, you may contact RedFlags@ftc.gov.

NEW RULE LANGUAGE

The new rule as applicable to “creditors” within the jurisdiction of the FTC will read as follows –

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Scope. This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) Definitions. For purposes of this section, and Appendix A, the following definitions apply:

(1) Account means 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. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term board of directors includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) Covered account means:

(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.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) **Periodic Identification of Covered Accounts.** Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(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.

(d) **Establishment of an Identity Theft Prevention Program.** (1) **Program requirement.** Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention 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. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) **Elements of the Program.** The Program must include reasonable policies and procedures to:
(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) Administration of the Program. Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) Guidelines. Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate.