DEADLINE LOOMS FOR COMPLIANCE WITH IDENTITY THEFT “RED FLAG” GUIDELINES

Congress passed the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”) in response to widespread concerns about misuse of personal information of consumers, including identity theft. The Act expanded the coverage of financial regulation to many businesses that obtain and handle personal information of consumers. The federal regulators, including the Federal Trade Commission (“FTC”), issued final identity theft “red flag” rules and guidelines earlier this year. Many types of businesses or enterprises – including utilities, municipalities, telecom providers, internet service providers, security companies and even small retailers - may be surprised to find they are covered by these newly-implemented requirements of the FACT Act. Determining whether your business or enterprise is covered by the new Red Flag Guidelines requires a careful review of definitions in the FACT Act and the new regulation. Simply stated, the new rule’s coverage is based on what you do and not who you are.

The FTC and the federal banking agencies jointly issued final rules and guidelines implementing Sections 114 and 315 of the FACT Act. The final rules and guidelines require “financial institutions” and “creditors” to establish and implement a comprehensive written program that prevents, detects, and mitigates identity theft.

The final rules were effective on January 1, 2008, with full compliance mandated by November 1, 2008. The FTC has the duty of enforcing and administering this part of the FACT Act. Failure to comply with these rules could result in injunctions, damages and civil penalties imposed by the agency and form the basis of private rights of action.

The Red Flag Rules

Increased Scope of Businesses Covered

The final “red flag” rule requires each “financial institution” and “creditor” that has one or more “covered accounts” to develop and implement a written “Identity Theft Prevention Program” (“Program”). The Program must be designed to detect, prevent and mitigate identity theft in connection with the opening of new “covered accounts” or activity relating to existing “covered accounts.” Unlike most other provisions of the FACT Act, the “red flag” rule also applies to businesses that do not pull credit reports or offer a traditional financial product or service. Whether the new rule reaches parties other than “financial institutions” (generally, banks, savings institution and credit unions and their affiliates) turns on two definitions: “creditor” and “covered account.”
The final rule broadly defines “creditor” as “anyone who 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.” In turn, “credit” is defined as the right to defer payment of a debt whether in just one or multiple payments and regardless of whether any charge is imposed for the deferment.

A “covered account” is 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, cell phone account, utility account, open account at a retailer, checking account or savings account) or 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. Consistent with the definition of “creditor,” the new rule defines “account” as a continuing relationship established by a person with a “financial institution” or a “creditor” to obtain a product or service for consumer purposes, including a purchase of property or services involving a deferred payment.

Risk Assessment

Prior to establishing a Program, each “financial institution” or “creditor” should determine whether it offers or maintains “covered accounts” and how it opens and maintains “covered accounts.” This should be a risk-based assessment, aimed at initially establishing the scope and focal points of a Program, taking into account:

- The methods the business provides to open its accounts, e.g., online, in person, over the phone, by mail or through intermediaries;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.

These factors should be reviewed based on foreseeable threats of identity theft and points of vulnerability. The risk assessment should result in identifying possible “gaps” in existing controls and procedures or the need to establish new controls and procedures to minimize the risk of identity theft. The risk assessment should include an analysis of the possible impact of the threat and the likelihood of its occurrence.

The entire risk assessment process should be documented and assembled into a report for review by the board of directors or senior management.

Elements of the Program

The final rule requires “financial institutions” and “creditors” to establish reasonable policies and procedures to:
• identify patterns, practice or specific activity that would indicate the possible existence of identity theft (referred to as “Red Flags”);

• incorporate the identified Red Flags into the Program;

• detect Red Flags that have been incorporated into the Program, when they occur;

• provide for an appropriate response when Red Flags are detected to prevent and mitigate possible identity theft; and

• update and monitor the Program on regular intervals to ensure the relevancy of existing Program Red Flags and incorporate new Red Flags due to changes in risk to customers or risks to the safety and soundness of the “financial institution” or to the “creditor” from identity theft.

The Program must be designed to be specific to the nature and complexity of each “financial institution” or “creditor.” When designing its Program, a “financial institution” or “creditor” may incorporate, as appropriate, any of its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the “financial institution” or “creditor” from identity theft. In effect, this means that a Program may be integrated into existing privacy and information security policies.

Identification of Red Flags

The Program should identify and include Red Flags from the following categories, as applicable:

• alerts, notifications, or other warnings received from consumer reporting agencies or service providers;

• the presentation of suspicious documents;

• the presentation of suspicious personal identifying information;

• the unusual use of, or other suspicious activity related to, a covered account; and

• notices from customers, victims of identity theft, law enforcement authorities, or other person regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

In Appendix A to Supplement J of the final rules, there is an extensive listing of illustrative examples of possible Red Flags in each of these categories. Each “financial institution” or “creditor” should consider whether these Red Flags are relevant to its business and should be included in its Program. These Red Flag examples are listed at the end of this document.

Detection of Red Flags

The Program should include policies and procedures that address the detection of Red Flags in connection with the opening of covered accounts. Examples of reasonable policies and procedures would include: obtaining and identifying information from a person opening an account, verifying the identity of a
person opening account, authenticating customers, monitoring transactions and verifying the validity of change of address requests, in the case of covered accounts.

Preventing and Mitigating Identity Theft

The Program should include policies and procedures that provide for appropriate responses to the Red Flags that the “financial institution” or “creditor” has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a “financial institution” or “creditor” should consider aggravating factors that may heighten the risk of identity theft. These factors may include a data security incident that results in unauthorized access to a customer’s account records, or notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the “financial institution” or “creditor” or to a fraudulent website. Appropriate responses may include:

- monitoring a “covered account” for evidence of identity theft;
- contacting the customer;
- changing any passwords, security codes, or other security devices that permit access to a “covered account”;
- re-opening a “covered account” with a new account number;
- not opening a new “covered account”;
- closing an existing “covered account”;
- not attempting to collect on a “covered account” or not selling a “covered account” to a debt collector;
- notifying law enforcement; or
- determining that no response is warranted under the particular circumstances.

Updating the Program

“Financial institutions” and “creditors” should update the Program periodically, to reflect changes in risks to customers or to the safety and soundness of the “financial institution” or “creditor” from identity theft, based on factors such as:

- the experiences of the “financial institution” or “creditor” with identity theft;
- changes in methods of identity theft experienced by the industry;
- changes in methods to detect, prevent, and mitigate identity theft;
- changes in the types of accounts that the “financial institution” or “creditor” offers or maintains; and
• changes in the business arrangements of the “financial institution” or “creditor,” including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Administration of the Program

The final rule requires that oversight of the Program should be performed by the Board of Directors, an appropriate committee of the board, or a designated employee at the level of senior management. The responsibilities for such oversight should include assigning specific responsibility for the Program’s implementation, reviewing reports prepared by staff regarding compliance by the “financial institution” or “creditor” with the Program, and for approving material changes to the Program as necessary to address changing identity theft risks.

In addition, the staff of the “financial institution” or “creditor” responsible for the 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 the compliance with the Program. The report should address material matters related to the Program and evaluate issues such as the effectiveness of the policies and procedures of the “financial institution” or “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.

The new rule requires that whenever a “financial institution” or “creditor” engages a service provider to perform an activity in connection with one or more “covered accounts,” the “financial institution” or “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 “financial institution” or “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 to either report the Red Flags to the “financial institution” or “creditor,” or take appropriate steps to prevent or mitigate identity theft.

The final rule requires training of the relevant staff to “effectively implement” the Program. There would need to be adequate training for responsible staff to know the procedures outlined in the Program to detect Red Flags on “covered accounts” and respond as necessary.

Red Flags Supplement

As previously indicated, in Supplement A of Appendix J of the Guidelines, each “financial institution” or “creditor” is encouraged to consider incorporating into its Program, whether individually or in combination, Red Flags from the following illustrative examples in connection with “covered accounts”:

Alerts, Notifications, or Warnings from a Consumer Reporting Agency

A fraud or active duty alert is included with a consumer report;
A consumer reporting agency provides a notice of a credit freeze in response to a request for a consumer report;

A consumer reporting agency provides a notice of address discrepancy; and

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 recent and significant increase in the volume of inquiries, an unusual number of recently established credit relationships, a material change in the use of credit, especially with respect to recently established credit relationships, or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

Documents provided for identification appear to have been altered or forged;

A photograph or physical description on the identification that is not consistent with the appearance of the applicant or the customer presenting the identification;

Other information on the identification that is not consistent with information provided by the person opening a new covered account or customer presenting the identification;

Other information on the identification that is not consistent with readily accessible information that is on file with the financial institution or creditor (e.g., a signature card or a recent check); and

An application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

Personal identifying information provided that is inconsistent when compared against external information sources used by the financial institution or creditor (e.g., the address does not match any address in the consumer report, or the SSN has not been issued or is listed on the Social Security Administration’s Death Master File);

Personal identifying information provided by the customer that is not consistent with other personal identifying information provided by the customer (e.g., there is a lack of correlation between the SSN range and date of birth);

Personal identifying information provided that is associated with known fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor (e.g., the address on an application is the same as the address provided on a fraudulent
application, or the phone number on an application is the same as the number provided on a fraudulent application);

Personal identifying information provided that is of a type commonly associated with fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor (e.g., the address on an application is fictitious, a mail drop, or a prison, or the phone number is invalid, or is associated with a pager or answering service);

The SSN provided is the same as that submitted by other persons opening an account or other customers;

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;

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;

Personal identifying information provided that is not consistent with personal identifying information that is on file with the financial institution or creditor; and

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

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;

A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example: the majority of available credit is used for cash advances or merchandise that is easily convertible to cash, such as electronics equipment or jewelry, or the customer fails to make the first payment or makes an initial payment but no subsequent payments;

A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is nonpayment when there is no history of late or missed payments, a material increase in the use of available credit, a material change in purchasing or spending patterns, a material change in electronic fund transfer patterns in
connection with a deposit account, or a material change in telephone call patterns in connection with a cellular phone account;

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);

Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account;

The financial institution or creditor is notified that the customer is not receiving paper account statements;

The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer’s covered account; and

The financial institution or 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.

Womble Carlyle client alerts are intended to provide general information about significant legal developments and should not be construed as legal advice regarding any specific facts and circumstances, nor should they be construed as advertisements for legal services.

IRS CIRCULAR 230 NOTICE: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (or in any attachment) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed in this communication (or in any attachment).

---

1 See FTC, Press Release, Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy (Oct. 31, 2007), at http://www.ftc.gov/opa/2007/10/redflag.shtm. Section 114 of the FACT Act, 15 U.S.C. § 1681m(e), amended section 615 of the Fair Credit Reporting Act (FCRA) and directed the agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances. Section 315 of FACTA, 15 U.S.C. § 1681c(h), and added a new section 605(h)(2) to the FCRA requiring the agencies to issue joint rules that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy. This overview only covers the new regulation and guidelines promulgated by the Federal Trade Commission covering the detection, prevention and mitigation of identity theft. The new regulation is codified at 16 CFR § 681.2 and the Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation are Appendix A to 16 CFR Part 681.

2 See Federal Register, Vol 72, No. 217, Friday November 9, 2007 at 63718.

3 See Appendix J to Part 681 Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.

4 12 CPR Part 41.90 (e)(3)