

GOVERNANCE COMPLIANCE ALERT “GCA”

FACT Act: Identity Theft Red Flags and Address Discrepancies Rules

Introduction

On November 9, 2007, the Federal Agencies issued final rules implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The rules require financial institutions and creditors to implement a written program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Credit and debit card issuers must also develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. Lastly, additional rules implemented under section 315, require users of consumer reports to develop reasonable policies and procedures regarding notices of address discrepancies received from consumer reporting agencies.

The regulation and guidelines went into effective on January 1, 2008 and mandatory compliance is required no later than November 1, 2008.

I. Identity Theft Prevention Program

The underlying foundation of the final rules is the requirement that 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 a formal Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The definition of “creditor” has a fairly broad meaning and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility and telecommunications companies. Lastly, the rules governing the Program are flexible and allow covered entities to tailor their Program in accordance with the size and complexity of their operations and permit the incorporation of existing policies and procedures that control reasonably foreseeable risks to customers into its Program, such as those already developed in connection with an institution’s fraud prevention program.

A. Elements of the program

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.

B. 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 by:

- 1) Obtaining approval of the initial written Program from either its board of directors, or an appropriate committee of the board of directors;
- 2) Involving the board of directors, or 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) Training staff, as necessary, to effectively implement the Program; and
- 4) Exercising appropriate and effective oversight of service provider arrangements.

C. Guidelines

Finally, covered entities must consider the guidelines provided in Appendix J of the final rules and incorporate the appropriate activities into the four elements of their Program. *Information about the Appendix J guidelines is discussed in this paper under section III.*

II. Special Rule for Card Issuers

A card issuer that receives notification of a change of address for a consumer debit or credit card account and within a short period of time afterwards (during the first 30 days after it receives such notification) receives a request for an additional or replacement card for the same account, may not honor the request and issue such card, unless it assess the validity of the change of address request in at least one of three ways:

- 1) Notify the cardholder of the request at the cardholder's former address and provide the cardholder a means of promptly reporting incorrect address changes;
- 2) Notify the cardholder of the request by another means of communication that the card issuer and the cardholder have previously agreed to use; or
- 3) Use other means of assessing the validity of the change of address, in accordance with the policies and procedures that the card issuer has established.

Any written or electronic notice that the card issuer provides must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

While "debit card" is not defined in the final rules, the section-by-section analysis cross-references the meaning defined in section 603(r) of the FCRA, which points to the meaning of "account" provided by Regulation E. The significance of the definition of "debit card" is that Regulation E was recently amended to include certain stored value cards under its definition of "account," specifically prepaid payroll cards. Therefore, financial institutions issuing prepaid/ stored value payroll cards must also comply with the special rules for card issuers, as well as the applicable duties regarding the detection, prevention and mitigation of identity theft.

III. Guidelines on Detection, Prevention and Mitigation (Appendix J)

In order to help financial institutions and creditors satisfy the requirements of the final rules, the Agencies developed guidelines designed to assist institutions with the formulation of policies and procedures that address the four elements of a Program, as well as the ongoing maintenance to ensure its effectiveness.

A. The Program

When it comes to designing the Program, institutions should begin the process by examining its existing policies, procedures and other arrangements that control potential risks to customers or to the safety and soundness of the business from identity theft. Existing policies and procedures that are found to control reasonably foreseeable identity theft risk may be incorporated into the Program, as appropriate.

B. Identifying Red Flags

The first step to identifying relevant Red Flags is to examine:

- 1) The types of covered accounts offered or maintained;
- 2) The methods provided to open covered accounts;
- 3) The methods provided to access accounts; and
- 4) Previous experience with identity theft.

Next, incorporate the relevant Red Flags from sources such as: (i) incidents of identity theft that have been experienced; (ii) methods of identity theft that have been identified which reflect changes in identity theft risk; and (iii) applicable supervisory guidance.

Lastly, The Program should include relevant Red Flags from the examples listed under the five categories of Red Flags provided by the Agencies, in Supplement A to Appendix J and also provided in this paper under section IV. *Illustrative Examples of Red Flags.*

C. Detecting Red Flags

Once the Red Flags have been identified, the Program's policies and procedures should address the detection of those Red Flags, in connection with opening an account, as well as for existing accounts, such as by:

- i. Obtaining identifying information about and verifying the identify of a person, for example, using the policies and procedures set forth in the Customer Identification Program (CIP); and
- ii. Authenticating customers, monitoring transactions and verifying the validity of change of address requests.

D. Preventing and mitigating identity theft

The Program's policies and procedures should address the applicable responses to the Red Flags that are detected and take into account the degree of risk posed by the incident. Appropriate responses may include the following:

- Monitoring the account for evidence of identity theft;

- Contacting the customer;
- Changing passwords, security codes or other security devices that permit access to the customer's account;
- Reopening an account with a different or new account number;
- Not opening a new account;
- Closing an existing 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.

E. Updating the program

The Program should be reviewed and periodically updated to reflect any changes in the risks to customers or to the institution. Factors to be considered include:

- a. The experiences with identity theft;
- b. Changes in the methods of identity theft;
- c. Changes in methods to detect, prevent and mitigate identity theft;
- d. Changes in the type of accounts that are offered or maintained; and
- e. Changes in the business arrangements of the institution including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

F. Methods for Administrating the Program

Once the Program has been formalized and implemented, ongoing maintenance is required in order to ensure continued effectiveness. The following components should be included in the administration of the Program:

Oversight: Oversight by the board of directors, an appropriate committee of the board or a designated senior level employee should include assigning specific responsibility for the program's implementation; reviewing reports prepared by staff regarding compliance; and approving changes to the program.

Reports: At least annually, the person responsible for the development, implementation and administration of the Program should report to the designated committee or senior management on the compliance with the Identity Theft Red Flags rules. The report should address material matters related to the Program and evaluate the effectiveness of the policies and procedures in addressing: the risk of identity theft in connection with the opening of covered accounts and existing accounts; service provider arrangements; and significant incidents involving identity theft and management's response. The report should also include any recommendations for material changes to the Program.

Training: Training should be conducted for relevant staff upon the implementation of the Program and as necessary where current anti-fraud prevention training does not cover or address relevant identity theft risks.

Service provider arrangements: Steps should be taken to ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft associated with covered accounts. For example, an institution 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 institution or take appropriate steps to prevent or mitigate identity theft.

IV. Illustrative Red Flag Examples

The final rule provides five categories of Red Flags and examples that should be considered and included in the Program as appropriate. The Agencies did not make any specific Red Flag mandatory and allows financial institutions and creditors to follow a risk-based approach regarding the identification of Red Flags.

Red Flag Categories				
Alerts, Notices, or Warnings from Credit Reporting Agency	Suspicious Documents	Suspicious Personal Identifying Information	Suspicious Account Activity	Identity Theft Notice
1. A fraud or active duty alert is included with a consumer report.	1. Documents provided for ID appear to have been altered or forged.	1. Personal identifying information provided is inconsistent when compared against external information sources.	1. Shortly following the notice of a change of address, a request for a new, additional or replacement card or new authorized user is made.	1. The creditor is notified by a consumer, a victim of identity theft, or a law enforcement authority that it has opened a fraudulent account for a person engaged in identity theft.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.	2. The photo or physical description on the ID is not consistent w/ the appearance of the applicant or customer presenting the ID.	2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.	2. A new credit account is used in a manner commonly associated with patterns of fraud.	
3. A consumer reporting agency provides a notice of address discrepancy.	3. Other information on the ID is not consistent w/ the info provided by the person presenting the identification.	3. Personal identifying information provided is associated with known fraudulent activity.	3. An account is used in a manner that is not consistent with established patterns of activity on the account.	

<p>4. A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:</p> <p>a. A recent and significant increase in the volume of inquiries; b. An unusual number of recently established credit accounts; c. A material change in the use of credit; or d. An account that was closed for cause or identified for abuse of account privileges.</p>	<p>4. Other information on the ID is not consistent w/ readily accessible information on file w/ the creditor, such as a signature card or recent check.</p>	<p>4. Personal identifying information provided is of a type commonly associated with fraudulent activity.</p>	<p>4. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected patterns of usage and other relevant factors.)</p>	
	<p>5. An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.</p>	<p>5. The SSN provided is the same as that submitted by other persons opening an account or other customers.</p>	<p>5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted.</p>	
		<p>6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other person opening accounts or other customers.</p>	<p>6. Notification is received that the customer is not receiving paper account statements.</p>	
		<p>7. The person opening the covered account or the customer fails to provide all required personal identifying information on an application.</p>	<p>7. Notification of unauthorized charges or transactions.</p>	
		<p>8. Personal identifying information provided is not consistent with personal identifying information that is on file.</p>		
		<p>9. For challenge questions, the customer cannot provided authenticating information beyond what generally would be available from a wallet or consumer report.</p>		

V. Address Discrepancies Reported by Consumer Reporting Agencies

Section 315 of the FACT Act provides that users of consumer reports must establish reasonable policies and procedures for handling notices of address discrepancies received from consumer reporting agencies. The policies and procedures should enable a user to:

- (i) form a reasonable belief that the user knows the identity of the person to whom the report pertain; and
- (ii) if the user establishes a continuing relationship with the consumer, to reconcile the discrepancy by furnishing such address to the notifying consumer reporting agency as part of the information regularly furnished by the user in the ordinary course of business.

In order to satisfy the requirements in (i), users may compare the information provided by the consumer reporting agency with information the user:

- A. Obtains and uses to verify the consumer's identity in accordance with any Customer Identification Program (CIP);
- B. Maintains in its own records, such as applications, change of address notification or other customer account records;
- C. Obtains from third-party sources; or
- D. Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.