

10/13/2008

FEDERAL TRADE COMMISSION

16 CFR Part 681

RIN 3084-AA94

**Identity Theft Red Flags and Address Discrepancies under the
Fair and Accurate Credit Transactions Act (FACTA) of 2003**

Executive Summary for the

University of Cincinnati

Kevin L. McLaughlin

FACTA Red Flag Legislation

What it Means to the University of Cincinnati

- The University of Cincinnati (UC) must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft in regards to covered accounts.
 - An “account” includes relationships with creditors that are not financial institutions; the definition is no longer tied to the provision of “financial” products and services.
 - The obligations of the final rule apply not only to existing accounts, where a relationship already has been established, but also to account openings, when a relationship has not yet been established.
 - The definition of “covered account” is divided into two parts.
 - “An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, which 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.”
 - “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.”
 - “Customer” is defined as a person that has an account with a financial institution or creditor.
- UC is required to implement a written Program to detect, prevent and mitigate identity theft in regards to covered accounts.
- UC must consider including reasonable guidelines that would apply when a transaction occurs in connection with a consumer’s credit or deposit account that has been inactive for two years
- UC is required to incorporate into its Program relevant indicators of a possible risk of identity theft (Red Flags) (see appendix A).
- UC is required to address accounts where identity theft is most likely to occur in regards to its covered accounts.
- UC is required to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account

- UC’s FACTA Red Flag Compliance Program (RFCP) must contain “reasonable policies and procedures” to:
 - Identify relevant Red Flags for covered accounts & incorporate those Red Flags into the overall methodology deployed
 - Detect Red Flags.
 - Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
- Ensure the FACTA RFCP is updated periodically, to reflect changes in risks.
- FACTA RED FLAG LEGISLATION believes that a business customer can be a target of identity theft, the final rules contain a risk-based process designed to ensure that these types of business customers will be covered by the RFCP.
- FACTA RED FLAG LEGISLATION defines the term “identity theft” to mean “a fraud committed or attempted using the identifying information of another person without authority.” FACTA RED FLAG LEGISLATION defines the term “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—
 - 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;
 - Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
 - Unique electronic identification number, address, or routing code; or Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).
- Under the FACTA Red Flag Legislation the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of “identity theft.”
- Red Flag is defined as “a pattern, practice, or specific activity that indicates the possible existence of identity theft.”
- UC is ultimately responsible for compliance even if it outsources an activity to a third-party service provider.
- UC must not only address the identification of the risk of identity theft, but also the prevention and mitigation of identity theft.
- FACTA RED FLAG LEGISLATION believes that the benefit of being able to assess a covered entity’s compliance with the final rules by evaluating the adequacy and implementation of its written Program outweighs the burdens imposed by the requirement to have a written program.

*FACTA Appendix J Abridged***I. The Program**

In designing its Program, UC may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to covered entities.

II. Identifying Relevant Red Flags

(a) Risk Factors. UC should consider the following factors in identifying relevant Red Flags for covered accounts:

- (1) The types of covered accounts it offers or maintains;
- (2) The methods it provides to open its covered accounts;
- (3) The methods it provides to access its covered accounts; and
- (4) Its previous experiences with identity theft.

(b) Sources of Red Flags. UC should incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that the financial institution or creditor has experienced;
- (2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks
- (3) Applicable supervisory guidance.

(c) Categories of Red Flags. UC's RFCP should include relevant Red Flags from the following categories. Examples of Red Flags from each of these categories are appended as Supplement A of Appendix J.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents;
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

UC's RFCP policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, by:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121) and;
- (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

UC's RFCP policies and procedures should provide for appropriate responses to the Red Flags detected that are commensurate with the degree of risk posed. In determining an appropriate response, UC should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by UC, or a UC trusted third party, or notice that a customer has provided information related to a covered account held by UC to someone fraudulently claiming to represent UC or to a fraudulent website. Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement
- (i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

UC should update the RFCP (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers based on factors such as:

- (a) The experiences of UC with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that UC offers or maintains; and
- (e) Changes in the business arrangements of UC, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) Oversight of Program. Oversight by the UC board of trustees, an appropriate committee of the board, or a designated employee at the level of senior management should include:

- (1) Assigning specific responsibility for the UC RFCP implementation;
- (2) Reviewing reports prepared by staff regarding UC compliance
- (3) Approving material changes to the UC RFCP as necessary to address changing identity theft risks.

(b) Reports. (1) UC staff responsible for development, implementation, and administration of its Program should report to the board of trustees, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance status.

(2) The report should address material matters related to the UC RFCP and evaluate issues such as: the effectiveness of the policies and procedures of UC 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 UC RFCP.

(c) Oversight of service provider arrangements. Whenever UC engages a service provider to perform an activity in connection with one or more covered accounts we must 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, UC could require the service provider by contract to have policies and procedures to detect prevent, and mitigate the risk of identity theft or UC 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 UC or take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

UC should be mindful of other related legal requirements that may be applicable, such as:

- (a) Items that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;
- (b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;
- (c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

The following items can be considered for incorporation into identifying red flags

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
4. 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. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
5. An application 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 is inconsistent when compared against external information sources used by UC. For example:

- a. The address does not match any address in the consumer report.
- b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- c. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- d. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by UC. For example:
 - i. The address on an application is the same as the address provided on a fraudulent application.
 - ii. The phone number on an application is the same as the number provided on a fraudulent application.
- e. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by UC. For example:
 - i. The address on an application is fictitious, a mail drop, or a prison.
 - ii. The phone number is invalid, or is associated with a pager or answering service.
 - iii. The SSN provided is the same as that submitted by other persons opening an account or other customers.
 - iv. 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.
 - v. 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.
- f. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. 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.
2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - i. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); o
 - ii. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - i. Nonpayment when there is no history of late or missed payments.
 - ii. A material increase in the use of available credit.
 - iii. A material change in purchasing or spending patterns.
 - iv. A material change in electronic fund transfer patterns
 - v. A material change in telephone call patterns in connection with a cellular phone account.
4. A covered account that has been inactive for a reasonably lengthy period of time is used.
5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
6. The financial institution or creditor is notified that the customer is not receiving paper account statements.
7. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.