BLACK | MANN & GRAHAM L.L.P.

4900 Woodway Drive, Suite 650

Houston, TX 77056

Phone: 713-871-0005

Fax: 713-871-1358

Thomas E. Black, Jr., P. C.*
Calvin C. Mann, Jr., P. C.
Gregory S. Graham, P. C.
David F. Dulock
Diane M. Gleason
Benjamin R. Idziak **
Shawn P. Black **
Margaret A. Noles
Robert J. Brewer
Regina Uhl

** Also Licensed in Iowa, New York, Washington and West Virginia*
*** Also Licensed in New York*

July 31, 2009

To: Clients and Friends

From: David F. Dulock

Subject: New Federal Rules - (1) Identity Theft Prevention Program; (2) Consumer Report Address Discrepancy Policies and Procedures. (***FTC Delays Enforcement of the Identity Theft Prevention Program until November 1, 2009***)

On October 17, 2008, we issued a memorandum explaining the above referenced federal rules. Subsequently, on October 22, 2008 and May 1, 2009, we updated the October 17, 2008 memorandum to advise you that the FTC had delayed enforcement of the Identify Theft Prevention Program ("Red Flags Rule"). The updated October 17, 2008 memorandum is posted on our website www.bmandg.com.

This memorandum is to advise you that the FTC has further delayed the enforcement of the Red Flags Rule for those entities subject to FTC oversight until November 1, 2009. For further information regarding this enforcement delay by the FTC and current information regarding the Red Flag Rule, please see the attached July 29, 2009 Press Release from the FTC.

FTC Announces Expanded Business Education Campaign on "Red Flags" Rule

To assist small businesses and other entities, the Federal Trade Commission staff will redouble its efforts to educate them about compliance with the "Red Flags" Rule and ease compliance by providing additional resources and guidance to clarify whether businesses are covered by the Rule and what they must do to comply. To give creditors and financial institutions more time to review this guidance and develop and implement written Identity Theft Prevention Programs, the FTC will further delay enforcement of the Rule until November 1, 2009.

The Red Flags Rule is an anti-fraud regulation, requiring "creditors" and "financial institutions" with covered accounts to implement programs to identify, detect, and respond to the warning signs, or "red flags," that could indicate identity theft. The financial regulatory agencies, including the FTC, developed the Rule, which was mandated by the Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA's definition of "creditor" includes any entity that regularly extends or renews credit – or arranges for others to do so – and includes all entities that regularly permit deferred payments for goods or services. Accepting credit cards as a form of payment does not, by itself, make an entity a creditor. "Financial institutions" include entities that offer accounts that enable consumers to write checks or make payments to third parties through other means, such as other negotiable instruments or telephone transfers.

The FTC's Red Flags Web site, www.ftc.gov/redflagsrule, offers resources to help entities determine if they are covered and, if they are, how to comply with the Rule. It includes an online compliance template that enables companies to design their own Identity Theft Prevention Program through an easy-to-do form, as well as articles directed to specific businesses and industries, guidance manuals, and Frequently Asked Questions to help companies navigate the Rule.

Although many covered entities have already developed and implemented appropriate, risk-based programs, some – particularly small businesses and entities with a low risk of identity theft – remain uncertain about their obligations. The additional compliance guidance that the Commission will make available shortly is designed to help them. Among other things, Commission staff will create a special link for small and low-risk entities on the Red Flags Rule Web site with materials that provide guidance and direction regarding the Rule. The Commission has already posted FAQs that address how the FTC intends to enforce the Rule and other topics – www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm. The enforcement FAQ states that Commission staff would be unlikely to recommend bringing a law enforcement action if entities know their customers or clients individually, or if they perform services in or around their customers' homes, or if they operate in sectors where identity theft is rare and they have not themselves been the target of identity theft.

The three-month extension, coupled with this new guidance, should enable businesses to gain a better understanding of the Rule and any obligations that they may have under it. These steps are consistent with the House Appropriations Committee's recent request that the Commission defer enforcement in conjunction with additional efforts to minimize the burdens of the Rule on health care providers and small businesses with a low risk of identity theft problems. Today's announcement that the Commission will delay enforcement of the Rule until November 1, 2009, does not affect other federal agencies' enforcement of the original November 1, 2008, compliance deadline for institutions subject to their oversight.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 1,500 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's Web site provides free information on a variety of consumer topics.

BLACK | MANN & GRAHAM L.L.P.

4900 Woodway Drive, Suite 650

Houston, TX 77056

Phone: 713-871-0005

Fax: 713-871-1358

Thomas E. Black, Jr., P. C.*
Calvin C. Mann, Jr., P. C.
Gregory S. Graham, P. C.
David F. Dulock
Diane M. Gleason
Benjamin R. Idziak **
Shawn P. Black **
Thomas L. Kapioltas
Margaret A. Noles
Robert J. Brewer

** Also Licensed in Iowa, New York, Washington and West Virginia*
*** Also Licensed in New York*

October 17, 2008 (**Rev.** October 22, 2008)

To: Clients and Friends

From: David F. Dulock

Subject: New Federal Rules - (1) Identity Theft Prevention Program; (2) Consumer Report Address Discrepancy Policies and Procedures.

INTRODUCTION

The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA) and Federal Trade Commission (FTC), herein Agency or Agencies, have jointly issued final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and final rules implementing section 315 of FACTA. **The mandatory compliance date for the final rules is November 1, 2008, except for the FTC Identity Theft Rules - *See attached FTC Enforcement Policy*.**

The final rules implementing section 114 of FACTA require each creditor and financial institution to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of covered accounts and existing covered accounts, which Program must be appropriate to the size and complexity of the creditor or financial institution and the nature and scope of its activities. To assist creditors and financial institutions in the formulation and maintenance of a Program that satisfies the requirements of the final rules, the Agencies also jointly issued guidelines that are attached as an appendix to the final rules. Additionally, and while not discussed in this memorandum, the Agencies also issued final rules implementing section 114 of FACTA to require credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances. Lastly, the Agencies jointly issued final rules under section 315 of FACTA that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

Each Agency's version of the final rules implementing sections 114 and 315 of FACTA are substantially identical (except for the sections identifying the persons to whom the rules apply). The final rules and interagency guidelines issued by the Agencies are located in the Code of Federal Regulations, as follows:

1. OCC Rules: 12 CFR Part 41, Chapter I, Subpart I, §41.82, Subpart J, §§41.90 and 41.91, Appendix J Guidelines. Applies to a national bank, Federal branch or agency of a foreign bank, and their operating subsidiaries.

2. FRB Rules: 12 CFR Part 222, Chapter II, Subpart I, §222.82, Subpart J, §§222.90 and 222.91, Appendix J Guidelines. Applies to a member bank of the Federal Reserve System (other than a national bank) and its operating subsidiaries, a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), and a commercial lending company owned or controlled by a foreign bank.

3. FDIC Rules: 12 CFR Part 334, Chapter III, Subpart I, §334.82, Subpart J, §§334.90 and 334.91, Appendix J Guidelines, and Part 364, Chapter III, §364.101(b). Applies to an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

4. OTS Rules: 12 CFR Part 571, Chapter V, Subpart I, §571.82, Subpart J, §§571.90 and 571.91, Appendix J Guidelines. Applies to a savings association whose deposits are insured by the FDIC and certain federal savings association operating subsidiaries.

5. NCUA Rules: 12 CFR Part 717, Chapter VII, Subpart I, §717.82, Subpart J, §§717.90 and 717.91, Appendix J Guidelines. Applies to a federal credit union.

6. FTC Rules: 16 CFR Part 681, §§681.1, 681.2, and 681.3, Appendix A Guidelines. **Applies to all other creditors and financial institutions**. (***See attached FTC Enforcement Policy delaying enforcement of the Identity Theft rules in §681.2.***)

FINAL RULE SUMMARY

The following summary of the final rules is taken directly from the final rules and the Agencies preamble explanations published in the November 9, 2007 issue of the *Federal Register*.

I. Identity Theft Prevention Program

The final rules list four basic elements that must be included in the Program. The Program must contain reasonable policies and procedures to:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor or financial institution from identity theft.

The final rules also list certain steps that creditors and financial institutions must take to administer the Program. These steps include obtaining approval of the initial written Program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the Program, training staff, and overseeing service provider arrangements.

Scope. Each Agency identifies those creditors or financial institutions under its jurisdiction to which the final rules regarding identity theft apply.

Definitions. Contains definitions of various terms that apply to the final rules and guidelines regarding identity theft. To understand and comply with the final rules regarding identity theft, the following definitions are important:

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." (***Note:*** *Although this definition contains the words "continuing relationship," the final rules 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.*)

2. "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." (***Note:*** *The first part of this definition applies to consumer accounts, and the final rules require an Identity Theft Prevention Program to cover these accounts. The second part of the definition applies to business accounts, but the final rules allow creditors and financial institutions flexibility in determining which business accounts will be covered by an Identity Theft Prevention Program.*)

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

4. "Financial institution has the same meaning as in 15 U.S.C. 1681a(t) [***i.e.***, *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 person that, directly or indirectly, holds a transaction account (as defined in 12 U.S.C. 461(b)) belonging to a consumer*]."

5. "Identity theft has the same meaning as in 16 CFR 603.2(a) [***i.e***, *a fraud committed or attempted using the identifying information of another person without authority*]." (***Note:*** *Unauthorized use of <u>any</u> "identifying information," whether used alone or in conjunction with other information, to identify a specific person satisfies this definition.*)

6. "Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft."

7. "Service provider means a person that provides a service directly to the financial institution or creditor." (***Note:*** *Creditors and financial institutions who outsource a covered account activity are ultimately responsible for the detection, prevention, and mitigation of identity theft in connection with that activity, even when the service provider has access to the information of a person who is not yet, and may not become, a "customer" of the creditor or financial institution.*)

Periodic Identification of Covered Accounts. The final rules require each creditor and financial institution to periodically determine whether it offers or maintains any covered accounts. As a part of this determination, each creditor and financial institution must conduct a risk assessment to determine whether it offers or maintains those covered accounts that are other than consumer accounts (*e.g.*, business accounts), taking into consideration:

- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.

Establishment of an Identity Theft Prevention Program – Program Requirement. The final rules require each creditor and financial institution that offers or maintains one or more covered accounts to develop and 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. The final rules state that the Program must be appropriate to the size and complexity of the creditor or financial institution and the nature and scope of its activities.

Elements of the Program. (1) The first element of a Program is reasonable policies and procedures to identify relevant Red Flags for covered accounts offered or maintained by a creditor or financial institution. These relevant Red Flags must be incorporated into the Program of that creditor or financial institution. Policies and procedures are not required, however, for identifying which Red Flags are relevant to detecting a *possible risk* of identity theft.

(2) The second element of a Program is reasonable policies and procedures to detect the Red Flags that a creditor or financial institution has incorporated into its Program.

(3) The third element of a Program is reasonable policies and procedures to "respond appropriately" to any Red Flag that is detected to prevent and mitigate identity theft. In order to "respond appropriately," a creditor or financial institution must assess whether the Red Flag detected evidences a risk of identity theft. If a creditor or financial institution concludes that the Red Flag detected does not evidence a risk of identity theft, it must have a reasonable basis for its conclusion.

(4) The fourth element of a Program is reasonable policies and procedures to 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 creditor or financial institution from identity theft. This element only requires periodic updating. It does not require creditors and financial institutions to immediately and continuously update their Programs.

Administration of the Program. This section of the final rules describes the steps that creditors and financial institutions must take to administer the Program, including: obtaining approval of the initial written Program (board of directors or senior management); ensuring oversight, development, implementation and administration of the Program by the board of directors or senior management; training staff; and overseeing service provider arrangements.

- Initial Approval of the Program - The final rules require approval of the initial written Program by the board of directors or an appropriate committee of the board. Thereafter,

at the discretion of the creditor or financial institution, the board of directors, a committee thereof, or senior management may update the Program.

- Oversight and Administration of the Program - The final rules provide discretion to creditors and financial institutions to determine who will be responsible for the oversight, development, implementation, and administration of the Program. The rules state that a creditor or financial institution must involve its 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.

- Staff Training - Creditors and financial institutions must train their staff, as necessary, to effectively implement the Program. This provision, however, requires training of only relevant staff. Also, staff already trained, for example, as a part of the anti-fraud prevention efforts of the creditor or financial institution, do not need to be re-trained except "as necessary." There is no corresponding staff training section of the guidelines.

- Oversight of Service Provider Arrangements - The final rules provide that creditors and financial institutions must exercise appropriate and effective oversight of service provider arrangements, without further elaboration. This provision provides maximum flexibility to creditors and financial institutions in managing their service provider arrangements, while making it clear that creditors and financial institutions cannot escape their obligations under the final rules by simply outsourcing an activity in connection with a covered account.

- Guidelines - In explaining the relationship of the final rules to the guidelines, the final rules state that creditors and financial institutions must consider the interagency guidelines (*i.e.*, Appendix J to the OCC, FRB, FDIC, OTS and NCUA final rules, and Appendix A to the FTC final rules) and include in the Program those guidelines that are appropriate.

II. Interagency Guidelines Appendix on Identity Theft Detection, Prevention, and Mitigation

The interagency guidelines provide assistance to creditors and financial institutions in the formulation and maintenance of a Program that satisfies the requirements of the final rules to detect, prevent, and mitigate identity theft. Each creditor and financial institution must consider the guidelines and include in its Program those guidelines that are appropriate. While a creditor or financial institution may determine that particular guidelines are not appropriate to incorporate into its Program, the Program must nonetheless contain reasonable policies and procedures to meet the specific requirements of the final rules. Illustrative examples of Red Flags are listed in Supplement A to the guidelines.

1. Section I of the guidelines clarifies that creditors and financial institutions may incorporate into the Program, as appropriate, their existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the creditor or financial institution from identity theft, such as those already developed in connection with the fraud prevention program of the creditor or financial institution. This avoids duplication and allows creditors and financial institutions to benefit from existing policies and procedures.

2. Section II of the guidelines contains the following list of factors that a creditor or financial institution "should consider … as appropriate" in identifying relevant Red Flags:

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

3. Section III of the guidelines provides examples of how to detect Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by obtaining identifying information about, and verifying the identity of, a person opening a covered account and, in the case of existing covered accounts, by authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

4. Section IV of the guidelines states that a Program's policies and procedures should provide for appropriate responses to the Red Flags a creditor or financial institution has detected that are commensurate with the degree of risk posed. The final rules do not define Red Flags to include indicators of a possible risk of identity theft. Instead, section IV states that in determining an appropriate response, a creditor or financial institution should consider aggravating factors that may heighten the risk of identity theft, and section IV provides examples of such factors.

5. Section V of the guidelines elaborates on the obligation to ensure that a Program is periodically updated. It lists factors that should cause a creditor or financial institution to update its Program, such as its own experiences with identity theft, changes in methods of identity theft, changes in methods to detect, prevent and mitigate identity theft, changes in accounts that it offers or maintains, and changes in its business arrangements.

6. Section VI of the guidelines notes that oversight of a Program should include assigning specific responsibility for the Program's implementation; reviewing reports prepared by staff on compliance with the Program; and, approving material changes to the Program as necessary to address changing identity theft risks. Section VI also states that these staff reports should be prepared at least annually and describes the contents of a report.

7. Section VI of the guidelines states that, whenever a creditor or financial institution engages a service provider to perform an activity in connection with one or more covered accounts, the creditor or financial institution 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. Under this guideline, a service provider that provides services to multiple creditors and financial institutions may do so in accordance with its own Program to prevent identity theft, as long as the Program meets the requirements of the final rules. Section VI also provides an example of how creditors and financial institutions may comply with this guideline.

8. Supplement A lists examples of Red Flags. Thus, a creditor or financial institution may tailor the Red Flags it chooses for its Program to its own operations. A creditor or

financial institution will not need to justify to an Agency its failure to include in its Program a specific Red Flag from the list of examples in Supplement A.

III. Consumer Report Address Discrepancy Policies and Procedures

Section 315 of FACTA requires the Agencies to jointly issue final rules that provide guidance regarding reasonable policies and procedures a user of a consumer report should employ when the user receives a notice of address discrepancy from a consumer reporting agency. Specifically, these final rules (herein, the final regulations) must describe reasonable policies and procedures for a user of a consumer report to employ to (i) enable it to form a reasonable belief that the user knows the identity of the person for whom it has obtained a consumer report, and (ii) reconcile the address of the consumer with the consumer reporting agency, if the user establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the consumer reporting agency.

Scope. Each Agency identifies those users of consumer reports under its jurisdiction (‘user”) that receive a notice of address discrepancy from a consumer reporting agency.

Definition. Contains the following definition for an address discrepancy notice*:* “[A] *notice of address discrepancy* means a notice sent to a user [of a consumer report] by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency’s file for the consumer.”

Reasonable belief - Requirement to form a reasonable belief. The final regulations provide that a user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom the user has requested the report when the user receives *a notice of address discrepancy*. The final regulations do not limit this requirement solely to the establishment of a new account. It also applies to existing accounts.

Examples of reasonable policies and procedures. The final regulations provide the following examples of reasonable policies and procedures that a user may employ: (1) comparing information in the consumer report with information the user: (i) obtains and uses to verify the consumer's identity in accordance with the Consumer Information Program (CIP rules – 31 CFR 103.121), (ii) maintains in its own records, or (3) obtains from third-party sources; or (2) verifying the information in the consumer report with the consumer. If a user cannot establish a reasonable belief that the consumer report relates to the consumer about whom the user has requested the report, the user should not use that report (***Note:*** *If a user is a “creditor” or “financial institution,” a notice of address discrepancy may be a Red Flag and require an appropriate response to prevent and mitigate identity theft under the user's Identity Theft Prevention Program.*)

Consumer's address - Requirement to furnish consumer's address to a consumer reporting agency. The final regulations provide that a user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency when the following three conditions are present: (1) The first condition requires that a user form a reasonable belief that a consumer report relates to

the consumer about whom the user requested the report. (2) The second condition states that a confirmed address must be furnished if the user "establishes a continuing relationship with the consumer." It does not require the reporting of a confirmed address to the consumer reporting agency in connection with existing relationships. (3) The third condition provides that if the user regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which a notice of address discrepancy pertaining to the consumer was obtained, the consumer's address must be communicated to the consumer reporting agency as part of the information the user regularly provides. (**Note:** Because of the second condition, the above requirement to furnish a confirmed address for the consumer to the consumer reporting agency is applicable only to new relationships.)

Examples of conformation methods. The final regulations list the following measures that a user may employ to reasonably confirm the accuracy of the consumer's address: (i) verifying the address with the consumer; (ii) reviewing its own records to verify the consumer's address; (iii) verifying the address through third party sources; or, (iv) using other reasonable means.

Timing. The user's policies and procedures must provide that the confirmed consumer's address required to be provided to a consumer reporting agency will be provided as part of the information the user regularly furnishes for the reporting period in which the relationship is established.

CONCLUSION

The final rules that require credit and debit card issuers to assess the validity of notifications of changes of address are not covered in this memorandum, although they are cited in the above sections of the Code of Federal Regulations.

Because the final rules, the final regulations, and the interagency guidelines issued by each Agency are substantially identical (except for the sections identifying the persons to whom the rules apply), for ease of reference we have attached only the versions issued by the OCC. Please refer to theses attachments when reading this memorandum.

The mandatory date for compliance is November 1, 2008, except for the FTC Identity Theft Rules - *See attached FTC Enforcement Policy*.

Consumer Reports – Address Discrepancies

Sec. 41.82 Duties of users regarding address discrepancies.

(3) *Scope*. This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a national bank, Federal branch or agency of a foreign bank, or any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definition*. For purposes of this section, a notice of address discrepancy means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address (es) in the agency's file for the consumer.

I *Reasonable belief.*

(3) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.*

(3) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(3) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

I Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address*.

(3) *Requirement to furnish consumer's address to a consumer reporting agency*. A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(3) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods*. The user may reasonably confirm an address is accurate by:

(3) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing*. The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

Identity Theft Red Flags

Sec. 41.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope*. This section applies to a financial institution or creditor that is a national bank, Federal branch or agency of a foreign bank, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions*. For purposes of this section and Appendix J, 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 (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 J of this part and include in its Program those guidelines that are appropriate.

Appendix J --Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 41.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in Sec. 41.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of Sec. 41.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, 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.

II. Identifying Relevant Red Flags

(a) *Risk Factors*. A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(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*. Financial institutions and creditors 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; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags*. The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this 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; and

(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

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as 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

The Program's policies and procedures should provide for appropriate responses to the Red Flags 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, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor 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;

(d) Reopening a covered account with a new account number;

(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; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) 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:

(a) The experiences of the financial institution or creditor 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 the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

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

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with Sec. 41.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports*.

(1) *In general*. Staff of the financial institution or creditor responsible for 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 compliance by the financial institution or creditor with Sec. 41.90 of this part.

(2) *Contents of report*. 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.

(c) *Oversight of service provider arrangements*. 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 either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors 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.

Supplement A to Appendix J

[Examples of Red Flags]

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

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, as defined in Sec. 41.82(b) of this part.

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

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

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

8. 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.

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

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. 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.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

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

15. 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.

16. 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.

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

18. 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

19. 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.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. 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).

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

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

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

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

26. 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.

FTC Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.2

On November 9, 2007, the Federal Trade Commission ("FTC"), the federal bank regulatory agencies,[1] and the National Credit Union Administration, published a joint notice of final rulemaking in the Federal Register (72 FR 63718) finalizing the Identity Theft Red Flags regulations and guidelines. This rule, promulgated pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), requires financial institutions and creditors to develop and implement written "identity theft prevention programs." The programs must provide for the identification, detection, and response to patterns, practices, or specific activities - known as "red flags" - that could indicate identity theft. Although the final rule became effective on January 1, 2008, full compliance with the rule is not required until November 1, 2008.

During the course of the Commission's education and outreach efforts following publication of the rule, the Commission has learned that some industries and entities within the FTC's jurisdiction have expressed confusion and uncertainty about their coverage under the rule. These entities indicated that they were not aware that they were undertaking activities that would cause them to fall within FACTA's definitions of "creditor" or "financial institution."[2] Many entities also noted that because they generally are not required to comply with FTC rules in other contexts, they had not followed or even been aware of the rulemaking, and therefore learned of the requirements of the rule too late to be able to come into compliance by November 1, 2008.

Given the confusion and uncertainty within major industries under the FTC's jurisdiction about the applicability of the rule, and the fact that there is no longer sufficient time for members of those industries to develop their programs and meet the November 1 compliance date, the Commission believes that immediate enforcement of the rule on November 1 would be neither equitable for the covered entities nor beneficial to the public. Delaying Commission enforcement of the rule as to the entities under its jurisdiction by six months, until May 1, 2009, will allow these entities to take the appropriate care and consideration in developing and implementing their programs. It also will give the Commission time to conduct additional education and outreach regarding the rule. Therefore, the Commission has determined that it will forbear from bringing any enforcement action for violation of the Identity Theft Red Flags Rule, 16 CFR 681.2, against a financial institution or creditor that is subject to administrative enforcement of the Fair Credit Reporting Act by the FTC, for a period of six months following the mandatory compliance date of November 1, 2008. **(emphasis added)**

This delay in enforcement is limited to the Identity Theft Red Flags Rule (16 CFR 681.2), and does not extend to the rule regarding address discrepancies applicable to users of consumer reports (16 CFR 681.1), or to the rule regarding changes of address applicable to card issuers (16 CFR 681.3). **(emphasis added)**

For questions regarding this enforcement policy, please contact Naomi Lefkovitz or Pavneet Singh, Bureau of Consumer Protection, 202-326-2252.

---

[1] The Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

[2] Under FACTA, "creditor" is defined the same way as in the Equal Credit Opportunity Act ("ECOA"), as 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. The ECOA definition of "credit" includes a right granted to defer payment for any purchase. Thus, any person that provides a product or service for which the consumer pays after delivery is a creditor. A "financial institution" is defined by FACTA to include all banks, savings and loan associations, credit unions, and any other person that holds a consumer transaction account as defined by section 19(b) of the Federal Reserve Act.