

Federal Trade Commission and Banking Authorities Issues Identity Theft and “Address Discrepancy” Rules

D. REED FREEMAN, JR., AND ALYSA ZELTZER HUTNIK

The authors analyze recent federal regulations governing (i) obligations of financial institutions and creditors to develop and implement a comprehensive written program that prevents, detects, and mitigates identity theft; (ii) duties of card issuers regarding changes of address; and (iii) duties of users of consumer reports regarding address discrepancies.

The Federal Trade Commission (“FTC”) and the federal banking agencies have jointly issued final rules and guidelines on:

- Financial institutions’ and creditors’ obligations to develop and implement a comprehensive written program that prevents, detects, and mitigates identity theft;
- Duties of card issuers regarding changes of address; and
- Duties of users of consumer reports regarding address discrepancies.¹

D. Reed Freeman, Jr. and Alysa Zeltzer Hutnik are attorneys in the Advertising and Marketing Practice Group of Kelley Drye & Warren LLP. They focus on all aspects of consumer information law, including privacy, data security, and breach notification, online and offline advertising, and direct marketing. The authors can be reached at rfreeman@kelleydrye.com and ahutnik@kelleydrye.com, respectively.

These rules and guidelines implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act ("FACTA"). The final rules are effective on January 1, 2008. Covered financial institutions and creditors must comply with the rules by November 1, 2008.

Financial institutions and creditors subject to the rules will have approximately one year to develop policies and procedures that comply with these requirements. It can be anticipated that the FTC will initiate a compliance sweep shortly after the November 2008 compliance deadline.

If the FTC initiates an investigation into a company's failure to comply with these rules and concludes that the company violated the rules, the company could be exposed to injunctive relief, damages (if there are any), and civil penalties of up to \$11,000 per each violation (which the FTC often calculates for each day of non-compliance). A detailed analysis of each of the rules follows.

DUTIES REGARDING THE DETECTION, PREVENTION, AND MITIGATION OF IDENTITY THEFT

General Overview

The final rules require each financial institution and creditor that holds one or more "covered accounts" to develop and implement a written "Identity Theft Prevention Program" (the "Program") that is designed to detect, prevent, and mitigate identity theft² in connection with the opening of new "covered accounts" or activity relating to existing "covered accounts."³ The Program must be appropriate to the size and complexity of the financial institution or creditor, and the nature and scope of its activities.

A "covered account" is:

- An account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions (e.g., a credit card account, mortgage loan, automobile loan, cell phone account, utility account, checking account, savings account, etc.); or

- Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft (e.g., small business accounts or sole proprietorship accounts that may be vulnerable to identity theft).

The final rules also require financial institutions and creditors to periodically determine whether they offer or maintain a “covered account.” As part of this determination, a financial institution or creditor must conduct a risk assessment (and document such efforts) to determine whether it offers or maintains covered 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.

Designing An Identity Theft Prevention Program

Each financial institution’s and creditor’s written Program must contain “reasonable policies and procedures” that:

- Identify relevant patterns, practices, and specific forms of activity that indicate possible existence of identity theft (e.g., red flags) 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 from identity theft.

The rules also identify certain steps that financial institutions and creditors 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 the staff, and overseeing service provider arrangements.

Guidelines for Formulating and Maintaining and Identity Theft Prevention Program

To assist financial institutions and creditors in formulating and maintaining a Program that satisfies the legal requirements (e.g., detecting, preventing, and mitigating identity theft), the rules set forth detailed guidance.⁴ Each financial institution or creditor must consider the guidelines and include in its Program those guidelines that are appropriate. Further, while an institution or creditor 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. The guidelines are summarized below.

1. Incorporating Existing Policies and Procedures

When designing its Program, a financial institution or creditor may incorporate, as appropriate, any of its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

2. Identifying Relevant Red Flags

When identifying relevant red flags for covered accounts, the financial institution or creditor should consider, as appropriate, 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.

Financial institutions and creditors also should incorporate relevant red flags from other sources, such as incidents of identity theft that the financial institution or creditor has experienced, methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks, and applicable supervisory guidance.

In addition, the Program should include relevant red flags from the following categories, as appropriate:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account; and
- 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.

Examples of red flags from each of these categories are appended as a supplement to the rules' appendix, and are summarized in No. 8 below.

3. 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 obtaining identifying information about, and verifying the identity of, a person opening a covered account, and authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

4. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the red flags that the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft (e.g., 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:

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

5. Updating the Program

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

- The experiences of the financial institution or creditor with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that the financial institution or creditor offers or maintains; and

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

6. Methods for Administering the Program

Oversight of the Program should be performed by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. The responsibilities for such oversight should include assigning specific responsibility for the Program's implementation, reviewing reports prepared by staff regarding compliance by the financial institution or creditor in the detection, prevention, and mitigation of identity theft, and approving material changes to the Program as necessary to address changing identity theft risks.

In addition, the staff of the financial institution or creditor responsible for the development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on the financial institution or creditor's compliance with the Program. The report should address material matters related to the Program and evaluate issues such as the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for material changes to the Program.

Further, whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities, and to either report the red flags to the financial institution or creditor, or take appropriate steps to prevent or mit-

igate identity theft.

7. Other Applicable Legal Requirements

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

- For financial institutions and creditors that are subject to the USA Patriot Act, 31 U.S.C. § 5318(g), filing a "Suspicious Activity Report" in accordance with applicable law and regulation;
- Implementing any requirements under the FCRA, 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;
- Implementing any requirements for furnishers of information to consumer reporting agencies under the FCRA, 15 U.S.C. § 1681s-2 (e.g., to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate); and
- Complying with the prohibitions in the FCRA, 15 U.S.C. § 1681m, on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

8. Examples of Red Flags to Consider

In a supplement to the rules' appendix, each financial institution or creditor is encouraged to consider incorporating into its Program, whether singly or in combination, red flags from the following illustrative examples in connection with covered accounts. Consideration of each of these illustrative red flags is optional.

Alerts, Notifications, or Warnings from a Consumer Reporting Agency

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

response to a request for a consumer report;

- A consumer reporting agency provides a notice of address discrepancy (as defined in the rules); and
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as a recent and significant increase in the volume of inquiries, an unusual number of recently established credit relationships, a material change in the use of credit, especially with respect to recently established credit relationships, or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged;
- A photograph or physical description on the identification that is not consistent with the appearance of the applicant or the customer presenting the identification;
- Other information on the identification that is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
- Other information on the identification that is not consistent with readily accessible information that is on file with the financial institution or creditor (e.g., a signature card or a recent check); and
- An application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

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

- Personal identifying information provided by the customer that is not consistent with other personal identifying information provided by the customer (e.g., there is a lack of correlation between the SSN range and date of birth);
- Personal identifying information provided that is associated with known fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor (e.g., the address on an application is the same as the address provided on a fraudulent application, or the phone number on an application is the same as the number provided on a fraudulent application);
- Personal identifying information provided that is of a type commonly associated with fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor (e.g., the address on an application is fictitious, a mail drop, or a prison, or the phone number is invalid, or is associated with a pager or answering service);
- The SSN provided is the same as that submitted by other persons opening an account or other customers;
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
- Personal identifying information provided that is not consistent with personal identifying information that is on file with the financial institution or creditor; and
- For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account;
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud (e.g., the majority of available credit is used for cash advances or merchandise that is easily convertible to cash, such as electronics equipment or jewelry, or the customer fails to make the first payment or makes an initial payment but no subsequent payments);
- A covered account is used in a manner that is not consistent with established patterns of activity on the account (e.g., there is nonpayment when there is no history of late or missed payments, a material increase in the use of available credit, a material change in purchasing or spending patterns, a material change in electronic fund transfer patterns in connection with a deposit account, or a material change in telephone call patterns in connection with a cellular phone account);
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account;
- The financial institution or creditor is notified that the customer is not receiving paper account statements;
- The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account; and
- The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Duties of Card Issuers Regarding Change of Address

The final rules also require credit and debit card issuers to 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.⁵ Specifically, a card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account.

Under these circumstances, the card issuer may not issue an additional or replacement card, until, consistent with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

- Notifies the cardholder of the request at the cardholder's former address (or by any other means of communication that the card issuer and the cardholder have previously agreed to use); and
- Provides to the cardholder a reasonable means of promptly reporting incorrect address changes, or otherwise assesses the validity of the change of address in accordance with its policies and procedures the card issuer has established pursuant to these rules.

A card issuer may satisfy these requirements if it validates an address, as described above, when it receives an address change notification, which may be before it receives a request for an additional or replacement card.

In addition, any written or electronic notice that the card issuer provides to comply with these rules must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Duties of Users of Consumer Reports Regarding Address Discrepancies

The final rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of

address discrepancy from a consumer reporting agency.⁶ Under the rules, a “notice of address discrepancy” means a notice sent to a user by a consumer reporting agency 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. Under the rules, 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. Examples of suggested reasonable policies and procedures include:

- Comparing the information in the consumer report provided by the consumer reporting agency with information the user obtains and uses to verify the consumer’s identity pursuant to the requirements of the Customer Information Program rules,⁷ maintains in its own records (e.g., applications, change of address notifications, other customer account records, or retained CIP documentation), or obtains from third party sources; or
- Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

The rules further require a user to develop and implement reasonable policies and procedures for furnishing a confirmed address of a consumer to a credit reporting agency from whom the user receives a notice of address discrepancy if the user:

- Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
- Establishes a continuing relationship with the consumer; and
- 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.

The rules provide guidance to users on how to confirm a consumer’s

address is accurate, such as by:

- Verifying the address with the consumer about whom it has requested the report;
- Reviewing its own records to verify the address of the consumer;
- Verifying the address through third party sources; or
- Using other reasonable means.

These policies and procedures 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.

NOTES

¹ See FTC, Press Release, *Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy* (Oct. 31, 2007), at <http://www.ftc.gov/opa/2007/10/redflag.shtm>. Section 114 of FACTA, 15 U.S.C. § 1681m(e), amended Section 615 of the Fair Credit Reporting Act ("FCRA") and directed the agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances. Section 315 of FACTA, 15 U.S.C. § 1681c(h), added a new Section 605(h)(2) to the FCRA requiring the agencies to issue joint rules that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy.

² Section 111 of FACTA defines "identity theft" as "a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade] Commission may prescribe, by regulation." 15 U.S.C. § 1681a(q)(3). The FTC defines the term "identifying information" (mentioned in the "identity theft" term) 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:

(1) 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; (2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) unique electronic identification number, address, or routing code; or (4) telecommunication identifying information or access device as those terms are defined in 18 U.S.C. § 1029(e).

³ *See, e.g.*, 16 CFR § 681.2 (duties regarding the detection, prevention, and mitigation of identity theft).

⁴ *See* Appendix A to Part 681 Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.

⁵ *See id.* § 681.3 (duties of card issuers regarding changes of address).

⁶ *See id.* § 681.1 (duties of users of consumer reports regarding address discrepancies).

⁷ The Customer Information Program rule, available at 31 CFR § 103.121 and promulgated pursuant to Section 326 of the USA Patriot Act, require banks, savings associations, credit unions, and certain non-federally regulated banks to have a Customer Identification Program to help reduce financial crime.