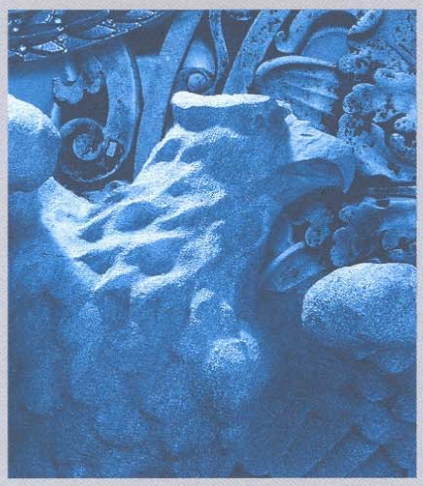


HERRICK

New York Office
2 Park Avenue
New York, New York 10016
Phone: (212) 592-1400
Fax: (212) 592-1500

Princeton Office
210 Carnegie Center
Princeton, New Jersey 08540
Phone: (609) 452-3800
Fax: (609) 520-9095

Newark Office
One Gateway Center
Newark, New Jersey 07102
Phone: (973) 274-2000
Fax: (973) 274-2500

www.herrick.com

FINANCIAL INSTITUTIONS ALERT MARCH 2008

Identity Theft Program Requirements Under the Fair and Accurate Credit Transactions Act

Financial institutions and creditors are required to implement anti-identity theft programs for certain types of accounts. The requirements went into effect at the beginning of this year, and if you're covered, you have until November 1, 2008 to get into compliance. This alert will help you determine if you're covered and, if so, what you need to do.

The rules

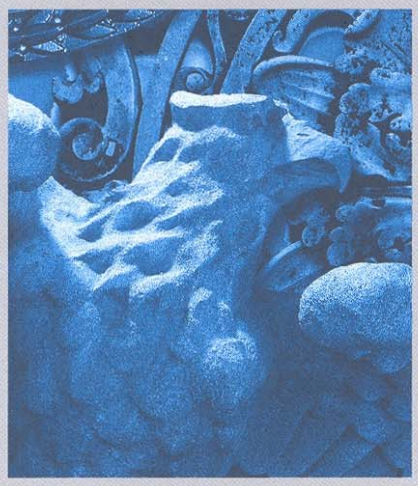
The Federal Trade Commission and the federal financial institution regulatory agencies published rules on identity theft procedures under the Fair and Accurate Credit Transactions Act of 2003 ("FACT"). The rules require each financial institution and creditor that maintains certain types of consumer accounts—those for which there is a reasonably foreseeable risk of identity theft—to develop and implement an Identity Theft Prevention Program. The agencies also issued guidelines to help financial institutions and creditors develop and implement a program. Here's what you need to know:

What is identity theft?

Identity theft is defined as a fraud committed using the identifying information of another person without authority. Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

What kind of accounts trigger the requirement to establish an identity theft program?

You must establish identity theft procedures for what FACT defines as "covered accounts": (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, or (2) any other account 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. FACT requires that each financial institution and creditor periodically determine whether it offers or maintains any covered accounts by conducting a risk assessment.



HERRICK

www.herrick.com

What's an identity theft program?

Each financial institution and creditor that offers or maintains covered accounts must develop and implement a written program that is designed to prevent, detect and mitigate identity theft in connection with both the opening of covered accounts and the maintenance of existing covered accounts. The program must contain reasonable policies and procedures that will enable a financial institution to:

- Identify relevant identity theft red flags for covered accounts;
- Respond appropriately to any red flags that are detected to prevent and/or mitigate identity theft; and
- Ensure that the program is periodically updated to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

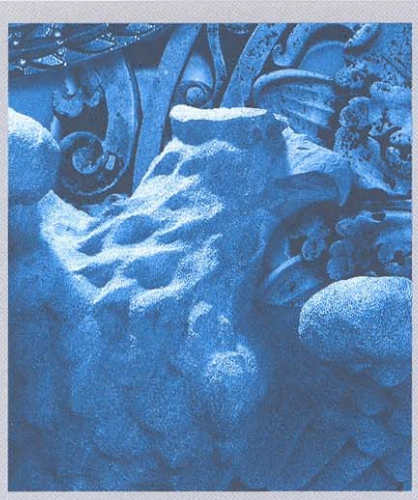
What's a "red flag"?

There are numerous red flags that may indicate identity theft. What they are will depend on the types of covered accounts the financial institution maintains, the methods it provides for customers to open and access its covered accounts, and its previous experiences with identity theft. Examples include:

- The presentation of suspicious documents, such as suspicious personal identifying information or documents that appear to have been altered.
- Personal information provided that is inconsistent when compared against external information sources or is associated with known fraudulent activity.
- A suspicious address change.
- Any particularly unusual or inexplicable use of a covered account, such as an unusual pattern of large withdrawals that quickly empty out an account that has consistently maintained significant balances.

Financial institutions should also have policies in place to quickly follow up on complaints from customers who have been victimized by identity theft. You also need to respond promptly to alerts, notifications, or other warnings received from law enforcement authorities, consumer reporting agencies or service providers such as fraud detection services.

Special rules for card issuers for "change of address" red flags



HERRICK

www.herrick.com

If a card issuer receives a notice of change of address for an existing account, and within 30 days or more receives a request for an additional card or replacement card for the same account, the issuer must assess the validity of the change of address through one of the following three methods:

- Notify the cardholder of the request at the cardholder's former address, and provide the cardholder with a means to promptly report an incorrect change of address;
- Notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder (e.g., notice to the customer's e-mail address); or
- Use of any other means of evaluating the validity of the address change in accordance with reasonable policies and procedures established by the card issuer.

The card issuer may not issue an additional card or replacement card until it has implemented one of these three procedures.

Conclusion

Identity theft is a rapidly growing financial fraud problem, and FACT and its rules are the government's way of ensuring that financial institutions and card issuers are taking steps to protect their customers.

For more information on these issues or other bank compliance or regulatory matters, please contact: **David Rosenfield at 212.592.1513 or drosenfield@herrick.com**.