

Banking & Securities Issues Briefing

With deadline looming, now's the time to finalize a response to identity theft "red flag" provisions

Background

Identity theft has become a multi-billion dollar issue that continues to accelerate. Protecting against it has become a multi-million dollar business. A survey conducted by the Federal Trade Commission (FTC) in 2006 estimated that 8.3 million American consumers, or 3.7 percent of the adult population, became victims of identity theft in 2005. Reported incidents collected by the agency in its annual fraud analysis showed 258,427 cases logged in their databases.

Stepping into this foray is the U.S. Federal Government's Fair and Accurate Credit Reporting Act and its "Identity Theft Red Flags and Address Discrepancies" provisions. This Act defines specific "Red Flags" that organizations must monitor, act upon, and have a documented program in place to address. Some of these items may be addressed by existing policies and procedures, others may be new. Regardless, responding to this is not an option. The joint final rules and guidelines were effective January 1, 2008 with a mandatory compliance date of November 1, 2008.

The end victims of identity theft, the consumers, are rarely held responsible for fraudulent debts incurred in their name. Rather, creditors are frequently attempting to collect the bad debt, or simply writing it off. Compliance with the regulations can likely reduce the incidence of identity theft suffered by your organization, which, in turn, may result in lower end costs. With a compliance date only a few short months away, your organization's response should begin quickly. What can you do to be prepared?

Regulation overview

The regulation calls for the "Establishment of an Identity Theft Prevention Program" that is appropriate to the size and



complexity of the organization. Developing documentation for the program is a required element of the regulation.

The regulation, as the name implies, was originally intended to focus on address discrepancies between credit reporting agencies and creditors. This has broadened to look at many areas that can be indications of identity theft. Several of these areas overlap with existing anti-money laundering processes, as well as information security standards published as part of Gramm-Leach-Bliley Act and other regulations.

The regulations focus on individuals and the accounts they maintain — the usual victims of identity theft; however, this does not eliminate certain small businesses, especially sole proprietorships, from the mix. If you manage accounts that fit within the definition, it is imperative that you understand what is in this regulation and the actions that you should be taking.

The regulations were jointly published by six agencies:

- Department of the Treasury — Office of the Comptroller of the Currency
- Federal Reserve System
- Federal Deposit Insurance Corporation
- Department of the Treasury — Office of Thrift Supervision
- National Credit Union Administration
- Federal Trade Commission

As the FTC is involved, it is not just a banking regulation and covers anyone that offers credit or manages a “covered account”. Therefore, it potentially extends to millions of businesses.

The term “covered account” is divided into two parts. The first part refers to “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.” The second part of the definition refers to “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.”

The final regulations list the four basic elements that must be included in the identity theft program. It must contain “reasonable policies and procedures” to:

- Identify relevant red flags
- Detect red flags
- Respond appropriately to any red flags
- Ensure that the identity theft program is updated periodically

The regulations further define that the program must be documented and have oversight from the board of directors, a committee of the board, or an employee at a senior management level.

Finally, 31 specific red-flags in “Appendix J” are provided that should be reviewed by your organization. These are organized into the following major categories:

- Consumer reporting and account application
- Documentary identification
- Personal information
- Address changes
- Anomalous use
- Notices
- Other

One area of note is that in the management of service providers, the regulations state that organizations should take steps to ensure that service providers are also acting with appropriate policies and procedures.

Response

While the regulations may seem daunting, a prudent approach to developing a program need not be. A scalable approach to developing an identity theft program includes the following:

- Scope and impact assessment
- Requirements analysis and gap assessment
- Gap closure plan and execution

Scope and impact analysis

Developing documentation for the program is a required element of the regulation. A key element of this documentation is a clear analysis of the elements of “Appendix J.”

This analysis should begin with a review of existing policies and procedures and should be combined with a review of the red flag categories and specific items defined within the regulation to determine which types of accounts are currently being managed, which of those accounts are “covered accounts,” and, most important for those accounts, which activities defined are relevant to your organization.

A key element of this review should be the development of a repeatable process to conduct this assessment on a periodic basis. This will enhance your organization’s ability to periodically update the program. When reviewing the account categories and red flags for applicability, do not stop at what is defined in the regulations; review other areas where your organization has reason to believe there may be a risk of identity theft. This will enable your program to respond to new threats as they are identified.

When conducting the impact analysis, it is important to gain input from the personnel closest to the business to enhance the understanding of accounts being managed and the applicable risks.

Requirements analysis and gap assessment

After initial identification of accounts, relevant red flags, and existing policies and procedures, the next step is to determine how well your organization’s existing policies and procedures match the regulations. There are few prescriptive measures in the regulations; however, a careful review of them can provide useful insights and suggested actions that can be used as input for updates that will allow your organization to develop a program that responds appropriately. Generally, the gap assessment will reveal that the organization’s capabilities fall into three general categories:

- Inadequate process — there is no process or the process in place to identify, respond and mitigate the situation is inadequate
- Processes exist although documentation may be lacking
- Processes exist and are appropriately documented

Gap closure plan and execution

Once the gaps are identified within the program, developing a remediation plan should be straightforward. For processes that exist and are appropriately documented, noting these and incorporating them into the program documentation will be all that is required. For processes that are functioning, albeit without adequate documentation, appropriate update of existing policies and procedures can be completed and incorporated as part of program documentation. Finally, the item requiring the most attention is developing or enhancing processes. Defining or enhancing processes in a large organization can be a challenging endeavor; however, the sooner changes begin to be made, the sooner the process can begin to work effectively. The regulations contain a significant amount of information regarding detection and response to suspected identity theft. Determining which actions are appropriate for your organization is ultimately up to your team.

Documentation

As stated above, the program must be documented and appropriate to the size of the organization. This will require that the relevant red flags be identified, the reporting structure and oversight of the program be appropriate, and that reporting of the effectiveness of the program be defined. The reporting aspect of the program is a key element that should be considered as the program is developed; specifically, the program documentation should include the types of reports that will be created and the frequency with which they will be reviewed by senior management. The program documentation should further contain specific references to appropriate policies and procedures that are involved.

Training

As with any change, as new processes are put forward, it is critical that the people involved receive adequate training. Focused training for the individuals involved can be an effective way to help the process work effectively.

Conclusion

While some of this regulation may seem burdensome it is important to remember that its ultimate goal is to help prevent fraud. Each fraudulent identity prevented from entering an organization's system will prevent additional accounts from being created with the same fictitious information.

For more information, contact:

Mark Steinhoff

National Financial Services Lead
Security & Privacy Services
Principal
Deloitte & Touche LLP
+1 617 437 2614
msteinhoff@deloitte.com

Richard Baich

Principal
Deloitte & Touche LLP
+1 704 887 1563
jbaich@deloitte.com

Frank Bresz

Director
Deloitte & Touche LLP
+1 212 436 3030
fbresz@deloitte.com

This publication contains general information only and is based on the experiences of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.