



This article was featured on the Callahan & Associates website, www.creditunions.com, the week of August 4, 2008

The Red Flags Guidelines— Points for Consideration When Developing a Program

By Linda Moynihan Vance | Vice President, Financial Services and
Charles Deremer | Senior Business Consultant, Fraud and Identity Management Group

Identity fraud and identity management are quickly becoming critical operational concerns for the financial industry. In addition, with recent media news stories and headlines, the general public is becoming more and more concerned over the protection of their personal and account information. While recent reports by the Federal Trade Commission and the Department of Justice indicate a downward trend in identity theft, the overall perception and potential impact of identity theft and fraud can have far reaching and potentially costly consequences in both the perception and reputation management of a financial institution and the customers they serve.

The Red Flags Guidelines issued in October 2007, pursuant to the Fair and Accurate Credit Transactions Act, requires implementation of an Identity Theft Prevention Program by November 1, 2008. While the Red Flags Guidelines have raised the overall awareness and understanding of the importance of identity fraud management, it is important to note that an effective Red Flags compliance program is not a spot check, but rather a blueprint for identity management. Many organizations are using the regulation to assess and improve current practices. In addition, organizations are considering the future impact of the regulation and making key considerations now that will provide flexibility to and improve the performance of their Red Flags Identity Theft Prevention Program.

When designing a program or processes to comply with the Red Flags Guidelines, here are some suggestions to consider:

1. Execute an initial risk assessment and a schedule for future ones

A risk assessment may be the first comprehensive opportunity to review all areas of the organization with a focus on identity management. Many organizations may have not previously undertaken a complete end-to-end review of operations in terms of operational risks or how it relates to identity management. Mergers, acquisitions, new products and updated charters can all have a dramatic impact on the level of risk in current processes.

The risk assessment will identify the effectiveness of current procedures and tools. Many organizations will find minimal changes are required to develop an appropriate program to fill potential gaps. Those organizations that identify significant gaps in their current procedures will need to develop an implementation plan to ensure strong identity management procedures are in place and well tested prior to the compliance deadline.

2. Implement and use accurate, reliable external data

The effective use of accurate and reliable data, whether from an internal or external source, is paramount to effective identity management. Data use is critical to all stages of the identity management process and a significant element of an identity theft prevention program. The data reviewed will support the decision to open or continue business with a customer. Whether the program is manual or automated, the quality of the data used to make the identity decision will be the key factor in performance. It is highly likely that the organizations will become increasingly reliant upon quality external data as the customer base expands and/or new products are introduced.

3. Deploy a flexible approach

The program must be flexible to meet the current and future demands associated with identity management. All too often, point solutions are introduced to respond to a current fraud trend. Point solutions may effectively resolve the current identity management issues, but fail to address evolving challenges. The policies, processes and tools implemented as part of an Identity Theft Prevention Program should not be stagnant and must be able to evolve to meet future needs in identity management.

4. Automate the process

Currently, the overwhelming majority of identity verification processes deployed in the industry are manual, relying upon the personal expertise, discretion and supposition of the representative. While manual processes may have been sufficient to meet the basic identity verification requirements, they may not pass a compliance audit. Typically, manual processes include significant discretionary and subjective authority that can be exposed as a weakness in an audit.

Automating the identity verification process is one of the most effective ways to ensure that a consistent and objective process is followed, a key element in any program. Automation does not necessarily mean the implementation of a complex decisioning platform; however, it does mean that the key decision points in the identity process are governed by a consistent and auditable series of automated checks and balances.

5. Establish comprehensive reporting

Identity management reporting continues to be one of the most under-appreciated elements of the process. The Red Flags Guidelines elevate the issue of reporting and mandates that an organization implement an effective reporting structure to keep senior management aware of the current state of operations. Reviewing and responding to those reports should be one of the primary elements of the Identity Theft Prevention Program to evaluate and ensure its effectiveness.

And finally, when deciding how to best implement processes to comply with the new regulations, it is important to apply a customer-driven approach to identity management. This type of approach provides the customer with the reassurance that the financial institution has leveraged the technologies and information available to make this a streamlined and seamless process at every touch point and throughout the account lifecycle.