

ID Theft Red Flags: Using risk assessment to improve your business

Kara Lamphere, CIA, CAMS

Chris Wetzel, CISA

Contineo

In the banking industry, regulations come with the territory. Financial institutions must find ways to adhere to those regulations by implementing programs, policies and procedures that guide their employees and business processes down the path of compliance. However, interpreting what the regulations specifically require the institution to do can often be a bigger challenge than actually implementing a program that leads to compliance.

Identity theft red flags rules, the regulation and guidelines that implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, appears to be no different. In a survey of 50 financial institutions conducted by Contineo in February 2010 that asked questions about performing a red flags risk assessment, the results showed once again that interpreting the law can be tricky. While some consistencies were found amongst the participating financial institutions, some of the survey answers also revealed inconsistencies in what those institutions may believe is required of them and their ID theft red flags program.

You get what you pay for...or do you? Slightly more than half of the respondents stated they purchased a template to develop the framework and documentation for their risk assessment. Yet we found that 40 percent of that group did not consider all risk factors required by the red flags rules. By contrast, of the institutions that either developed their own risk assessment or were given a sample from a peer or business partner, 80 percent considered all risk factors when conducting their assessments.

According to the red flags rules, risk factors that must be considered include:

- Methods of opening covered accounts
- Methods used to access covered accounts
- Previous experience with identity theft

Although a financial institution may not have previously dealt with instances of identity theft within its customer base, it is a factor that still must play into the discussion when determining its identity theft risks. And remember service providers play a role in the assessment, too.

Is reviewing my risk assessment once a year enough? While most of the respondents indicated they conduct an annual review of the identity theft red flag risk assessment, the guideline is simply to periodically update the program to reflect changes in risk associated with customers or the safety and soundness of the institution. When product offerings or services change within the institution it is best practice to re-address the risk assessment at that time, too.

Although the ID theft red flags law requires periodic assessment, best practice would dictate an annual review is probably the easiest way to ensure a periodic check is completed. As you are conducting your update of the program, a review of the risk assessment would be appropriate to ensure everything is still accurate.

While the requirement is to use the risk assessment as a means to determine if you hold covered accounts, the probable intent behind the law could arguably be larger than what is actually written. As a financial institution offering any product, you probably already know you have covered accounts, such as credit cards, demand deposit accounts, and savings accounts. So it seems likely the intent within the regulation is to approach the identity theft red flags program from a risk-based position.

So how should we proceed? Risk assessments are often completed “in a silo,” or without a strong regard to what it may mean to the various processes surrounding the particular area. In our survey results, we found only 52 percent of the institutions included business unit managers in the assessment process. That means that the people on the front lines of the business who are in charge of implementing the processes and training staff on the procedures are not involved in the identification of the risks and the development of the controls to mitigate those risks. The intent of a risk assessment is of course to identify risk. But once risks are identified, the people involved in the areas associated with the risks should determine the best and most cost effective means to mitigate them. Implemented the right way, the assessment can be used as an ongoing tool to aid management in monitoring the program throughout the year.

Assessments can also aid management in developing strong procedures. Your procedures govern the actions of your team members. So, understandably, these should be strong and built around inherent and residual risk allowances. By getting applicable departments together, rather than creating the assessments in silo by the designated officer, risks can be discussed in depth. Through these discussions concerning what risks are posed to the institution, you can determine the best way to mitigate those risks bearing in mind cost and the risk tolerance of the Board of Directors and management. And ta-da! By having these discussions about what risks are out there and the ways to mitigate you now have a basis to write strong procedures.

But don't let the risk assessment collect dust. As a banker, especially in these belt-tightening times, costs are constantly evaluated. But have you considered risk assessments as a tool to use in evaluating costs? As you begin to contemplate a new product or service, perform a risk assessment or simply add it to your identity theft red flag risk assessment. What are the risks? What is it going to cost to mitigate those risks? What is the value? As you begin to answer those questions, it adds to the pool of decision making factors in whether to actually implement the new service or product. If you decide to move forward, you have already updated your risk assessment and the only step left is to ensure it is added properly to your policies and procedures.

Executive management can also use risk assessments in the overall strategic planning process. As the strategic goals are developed, it could be beneficial to understand the risks associated with current and future products, programs, and services. For instance, if internet banking is fairly new for your institution and you have experienced some instances of identity theft, you may not want to bring on mobile banking until several years down the road. The institution could strategize on developing stronger relationships, tightening procedures to cut down on internet banking identity theft and perhaps strengthen customer service and reputation. At the appropriate time, mobile banking could then be brought into the mix.

Banking compliance, at times, can be difficult to stay abreast of and understand. As discovered through our survey, the requirements under the FACTA for identity theft red flags are no different. Risk assessments can be powerful tools to aid management in taking a bank to newer levels while maintaining

costs associated with risks. The key is to be involved in those assessments and use them regularly in managing your business rather than dusting them off once a year simply to see if anything has changed.

Kara Lamphere is an auditor and consultant at Contineo. She has been working in the financial industry for over 10 years, specializing in regulatory compliance and internal audit.

Chris Wetzel is Vice President and Senior Consultant at Contineo. He specializes in information security, information technology, and internal controls testing.

For more information, please contact Contineo at 866-847-0100, or visit us on the web at www.contineotech.com.

*©Copyright by Contineo Technologies, Inc. 2010
All Rights Reserved*