The Cost of FACT Act Compliance:
New Research Study Finds that Financial Institutions Are Underestimating Cost

By Adam Elliott, President, ID Insight

Red Flag compliance seemed to be ***the*** compliance topic of 2008, culminating with the November 1, 2008, compliance deadline. As we enter 2009, it has quickly diminished from the front page as the economic crisis is in full swing and most financial institutions have put their Red Flag Plan into action at some level. However, a new Fraud Management Institute Report sponsored by ID Insight suggests that the costs associated with Red Flag compliance are still largely unknown by those affected, and are being underestimated by more than half.

What You Don't Know, Can Hurt You

In the study, hundreds of banking industry fraud and risk managers representing all geographic areas and institutional sizes were surveyed regarding topics of Red Flag readiness and fraud prevention strategy. When asked questions about very pertinent issues with respect to the new Red Flag compliance requirements and the impacts to their institution, an alarming number of respondents reported they "didn't know." At a time when banks and credit unions are desperately looking for ways in which to reduce operational costs, the survey shows that many are still largely unaware of where these costs actually reside and the impact they have on the institution.

If you're a part of this group and not up to speed on the Red Flag requirements—and how your institution is responding—you could be missing out on opportunities to become compliant, streamline your processes and cut costs.

One of the most prominent new requirements included in the FACT Act Red Flag rules is the practice of mitigating identity theft risk in the event of a bank or credit union customer changing their address; or, in situations where a new account application features an address that varies from the address on record for that applicant.

As seen from a sampling of survey questions in the table below, a substantial percentage of survey respondents didn't have an estimate of how prevalent address change situations are in their institution, or how much the common methods of compliance will cost in light of the new requirements.

Question	Respondents reporting "don't know"
What percentage of your customers change their address annually?	31%

What is the average cost of sending an address change confirmation letter to two addresses?	34%
What is the percentage of new account applications with an address that differs from the address of record?	36%

Additionally, many survey respondents who answered these questions and did provide an estimate may very well have underestimated the true impact of the Red Flag requirements and address change requirements. When comparing the answers from survey respondents against numbers provided the United States Postal Service and other proprietary research, we see a fairly significant disparity.

Here are some of the key inconsistencies observed:

Question	FMI Survey Respondents	Independent Statistics	Difference
What percentage of your customers change their address annually?	Average = 9%	Average = 13% *	- 56%
What is the average cost of sending an address change confirmation letter to two addresses?	Average = $0.92	Average = $1.30 **	-41%
What is the percentage of new account applications with an address that differs from the address of record?	Average = 7%	Average = 20% ***	-186%

* Source: U.S. Census Bureau, Current Population Survey, 2007 Annual Social and Economic Supplement
** Source: ID Insight Inc. Survey, 2009
*** Source: ID Insight Inc. Consortium Study, 2008

As with many new compliance measures, it can take time to fully understand the overall impact and cost, and these impacts tend to span across the entire organization, which makes them even more difficult to measure. Still, these gaps seem to be rather large considering that the live date for compliance with the Red Flags requirements was nearly six months ago, and the requirements have been known for much longer than that.

One possible explanation for this disconnect is simply that not enough time has been spent on fine-tuning a compliance strategy and fully vetting out solution options. Another key finding from the survey was that the anticipated effort involved with getting into Red Flag compliance was largely underestimated. When asked about the accuracy of the original figure from the federal regulators of 41 hours to develop and implement an Identity Theft Prevention program, 57 percent of survey respondents said that this estimate was either "a little low" or "way too low."

When we consider this along with the fact that many banking institutions are trying to survive in the midst of what is widely regarded as a crisis, it is easy to see how these matters may have been put on the proverbial back burner.

The Silo Effect?

The survey responses present evidence that many of the operational burdens and costs associated with Red Flag compliance may be overlooked. The reason? The associated costs fall to different organizational areas within the institution. The spirit of the Red Flag rules is to prevent identity fraud from penetrating the banking system. As such, much of the survey focused around the current fraud experience of the respondents. The survey was distributed primarily to individuals who serve in fraud, risk and compliance roles at their respective institutions.

When asked about their top business objectives, 42 percent of survey respondents put fraud reduction at the top of their list while 31 percent reported that compliance was their most important objective. In addition, 60 percent of survey respondents reported being a member of the Red Flag compliance team at their respective institution. Improving the customer experience, minimizing operational expense and growing revenues scored at the bottom of the priority list. Given the population of respondents, these findings certainly make sense.

When it came to the cause-and-effect relationship between address changes and fraud, the understanding was fairly well defined. More than half of survey respondents (54 percent) said that an address change was the most important indictor of account takeover. This figure is in line with much of ID Insight's proprietary research, as well as other industry reports.

When asked about the common practices chosen by survey participants to counter the threat of address-related fraud, the most common strategy was to either send an address change notification letter in the event of a customer address change, or require some type of physical ID document. In fact, 63 percent of the survey respondents reported using at least one of these methods. Again, this is not surprising, given the audience and focus of the survey.

Here is where the survey findings get particularly interesting: What is lying beneath these numbers is that fraud and compliance professionals definitely see and understand the relationship between fraud risk and address changes, and what is needed to get into

compliance. The potential problem, however, is that fraud and compliance decision-makers don't necessarily fully realize the impacts with respect to other areas of the institution such as customer service and operational efficiency. For example, because the budget for sending out notification letters in the event of an address change likely resides somewhere else within the banking organization, the cost impact isn't as prominent to the risk and compliance team. This is evidenced by the large number of "don't know" responses described earlier.

Because of this lack of cross-functional awareness, it is very possible that opportunities to not only meet compliance, but to "do it better" may be missed.

A Better Way

Most institutions that we worked with prior to the Red Flag deadline did assemble cross-functional teams to identify their chosen solution. However, we found that most of these institutions put much more of an emphasis on being compliant by the deadline, and not nearly as much of an emphasis on efficiency and effectiveness. This ended up in more costly manual processes. For those that did put more of an emphasis on cost and effectiveness, we have observed these institutions to be much better off.

In working closely with these institutions, we have observed a marked difference in the outcomes after the compliance date. By deploying an enterprise-wide approach with a risk-based focus, many institutions are not only achieving compliance today, but they are doing it for substantially less cost and interruption to their customers. It is important to understand that without cheapening the letter of the law from a compliance standpoint, there are ways to be compliant without resorting to the very manual and document-centric methods that are so common.

In whole, the key finding of the survey is that the industry as a whole is still in the early stages of fully understanding of the overall impact of Red Flag compliance. Further compounding this issue is the often felt state of panic within the industry. This can be dangerous. As we are learning with the current financial crisis, not knowing where everything resides on the balance sheet can result in some ugly surprises.

In a time when financial institutions are searching for dollars under every rock, there are considerable opportunities to save organizational time and expense. When you ask the very pointed questions about costs and impacts to the right people, we usually get that "ah-ha" moment. It is at this point that you can begin to have some meaningful conversations about doing things better. In doing so, compliance solutions can be thought of not just as merely a cost of doing business, but rather something that can be a strategic competitive advantage and vital to the institution.