



## ID Theft Red Flags: Essential Elements of Customer Awareness

### With New Focus on Prevention, Examiners Will Be Looking Beyond Statement Stuffers

Linda McGlasson, Managing Editor

September 2, 2008

As financial institutions scramble to meet the Nov. 1 deadline for Identity Theft Red Flags Rule compliance, the operative word is "prevention" - as in Identity Theft Prevention Program.

And the key to making prevention work, observers say, is a sound customer awareness program that goes beyond statement stuffers and television ads.



Regulators have raised the bar on identity theft prevention, says Sai Huda, CEO of Compliance Coach, an industry risk management and compliance services company. "The ID Theft Red Flags Rule has created an affirmative obligation on financial institutions and creditors to take proactive steps to prevent identity theft," he says.

Regulators expect to see evidence that institutions took their obligations seriously and methodically performed an inventory of all accounts; a risk assessment to determine covered accounts; [considered the 26 red flags](#) in Appendix J to the Rule; its own historical experience and other credible sources; mapped red flags to appropriate detection and response procedures; and developed a risk-based, written Identity Theft Prevention Program.

Also, Huda says, regulators will ask 'Did the institution obtain board approval and provide appropriate employee training to effectively implement the program?' Additionally, is the financial institution periodically updating the program to address new risks or operational changes, and is it overseeing vendor and business partners to mitigate identity theft?

While there is no legal requirement to provide a notice to or educate consumers in the rules, "such proactive efforts will reflect positively on the financial institution that undertakes a consumer awareness effort and to invite the consumer to join the fight to deter identity theft," Huda says.

Huda also points out that other forces come into play when considering how much customer awareness plays a part in the institution's security program. "One should note that due to the affirmative obligation created by the Rule, the other enforcer will be plaintiff attorneys." He expects an increase in lawsuits against non-compliant financial institutions. "Failing to comply with the Rule will be alleged to be unfair or deceptive acts and practices violation under federal and state laws," Huda says. "So before the regulators uncover non-compliance, the plaintiff attorneys will more likely identify the targets and go after the deep pockets. Financial institutions must proactively

comply with the Rule to mitigate the risks."

### **Elements of Awareness**

What are some of the things that financial institutions should be educating their customers on when it comes to identity theft?

**Tell Them What You're Doing** -- Speaking with several industry thought leaders, they all concur that awareness begins with telling customers what you're doing to protect their information. Not doing this creates the "enemy within," says Tom Wills, Senior Analyst of Risk, Security, Fraud and Compliance at Javelin Strategy and Research. "For customer-facing security awareness and education, the enemy comes from within, as institutions are sometimes reluctant to talk about security for fear of giving too much knowledge to the bad guys." The good news is, "It's not necessary to give away your methods in order to communicate to customers and to the public about security," he adds.

**Explain the Real Risks** -- What institutions will want to tell their customers is that more than 8.3 million consumers fall victim to identity theft each year, and over \$15.6 billion in losses are caused by fraudsters, according to the Federal Trade Commission. Fifty percent of the time it is a business that provides the point of vulnerability to thieves to steal consumer information due to poor controls, procedures or employee training, according to the U.S. Secret Service. Identity theft is a growing crime and consumers are very concerned. "Added to that, due to the current economic conditions, banks are suffering financial losses and some are even failing," says Huda. "Consumers are becoming concerned not only about the safety of their money, but also their personal information and beginning to question the trustworthiness of their financial institution that has both their money and information."

**Offer Reassurance** -- Financial institutions should be proactive and clearly communicate to consumers a simple message: It recognizes that these days the consumer may have concerns about the safety of their money and personal information, and that the financial institution has taken appropriate steps to protect both their money and personal information to maintain the consumers trust. This message will reassure existing customers, but also serve as a competitive differentiator and attract new business.

### **Additional Points**

The following are some key points that a financial institution should cover in an Identity Theft awareness program for consumers:

Identity theft harms both the consumer as well as the financial institution. It is a joint fight;

The financial institution cares deeply about the consumer's financial well-being and has taken steps to protect both their money as well as personal information;

Just as the financial institution has taken steps to do its part to fight identity theft, customers should also do their part by being alert at all time and not allow points of vulnerability for thieves;

The financial institution should list common methods of how thieves steal information and certain steps consumers should take to deter identity theft;

The customer should contact the financial institution if at any time their identity is stolen, and also a non-profit resource such as the Identity Theft Resource Center (ITRC) or the Identity Theft Assistance Center (ITAC) for counseling and assistance.

### **Crunch Time Before Nov. 1**

With fewer than 60 days to go before institutions must comply with the new regulation, there are things that an institution can do to promote more customer awareness. One problem that Dr. Markus Jakobsson, Senior Research Scientist at the Palo Alto Research Center, sees with many customer awareness programs (not just those honing in on identity theft) is that they don't explain the problem.

"Most security education by financial institutions shows examples only -- they do not teach the underlying principles," he says. "That is like teaching kids how to recognize the 100 most common words -- but not teach them how to read!" Jakobsson, a noted information security researcher, points to the hardest hurdle - motivating customers. "Most security education fails to motivate the recipients. It is hard or boring, and as a result, only people who already have problems (and want to avoid getting phished again) bother to use the material."

Material needs to be easily accessible, and in bite-sized portions. "People buy security textbooks if they want to become security experts," Jakobsson says. "Very few people are going to buy a fat textbook about security in order to be more secure online."

Wills encourages institutions to engage their marketing and PR talent, "to treat security awareness like a marketing campaign. If done well, this can be a great brand builder for your institution because trust (which follows largely from sound security) is a key value element that customers look for in their financial institution."

Develop a set of key messages around your security program, which can be reused across different media, print, audio, even the call waiting feature while a customer is on hold.

Try something different from the usual statement stuffers. Use the full range of media available to the institution: print, broadcast, and online media, financial institution-specific media such as messages on ATM screens and signage in branches. Don't overlook "new media" especially to reach the more youthful portion of your audience. Post a series of security awareness videos on YouTube, says Wills. "Because security is basically a dry subject, make your materials entertaining and concise to maximize learning retention. Don't be afraid to use plenty of humor in your messaging ... the point is to make it stand out and make it stick - not sound like every other institution in the world."

Reward good security practices by customers. "If you offer user-controlled alerts on your online banking website, waive account fees for a month when they first activate the alerts," Wills suggests.

Remember to think like your average customer. "Most security experts design countermeasures that would help them, but fail to recognize that they may not help the average bank customer and Internet user," says Jakobsson. "Remember the 'Average Joe' doesn't care about URLs and SSL...he wants to do his banking online, buy some stuff, search for fun and useful stuff, not spend a lot of time looking at certificates and worrying. It is important to know your audience."

[Close Window](#)

---

**BankInfoSecurity.com is your source for bank information security news, regulations, and education.**