

Michigan Banker

Reprinted with permission from
Michigan Banker Magazine
June 2007

Bankers Need to Maintain Vigilance To Eliminate Identity Theft

By ADAM ELLIOTT
President
ID Insight, Inc.
St. Paul, Minnesota

Identity theft is everywhere. The FTC estimates that in 2007, identity theft will be responsible for sucking about \$50 billion dollars out of the U.S. economy – most of which will come from banks and other financial institutions. Identity theft remains a chief concern for consumers as well, as it topped the FTC's consumer complaint list for the seventh straight year in 2006.

But in spite of these staggering figures, concerns among bankers about identity theft seem to have plateaued. In the 2002 ABA Fraud survey, 38 percent of bankers listed identity theft as the number-one issue threatening their banks. In the latest ABA Survey, that number dropped to 20 percent of bankers citing identity theft as their top concern, which was the third most common response. There are probably several explanations for the seemingly lessened concern, including varying definitions of identity theft and slowed growth in reported losses.

However, for a multitude of reasons, it is critical that the banking industry not become complacent in the fight against identity theft. A failure to keep identity theft out of the banking system can have devastating effects, not only measured by substantial dollars lost, but perhaps even more significantly, in the damage to a bank's brand. As evidenced by numerous consumer surveys, protecting customer data is now becoming just as important as protecting a customer's money. Maintaining customer trust not only preserves brand loyalty, but also expands a customer's willingness to utilize new and more profitable channels and products, such as online banking.

To fully realize the benefits of greatly decreased identity theft losses and real customer protection, an attitude of merely "containing" the identity theft problem needs to be replaced by one of actively taking measures to eliminate it. By effectively combating identity theft, an opportunity exists for very tangible and measurable benefits across all aspects of the bank.

Preventing identity theft first requires knowledge of how identity theft occurs, and where the current gap is in terms of detection and prevention. Identity theft happens in one of two ways: either the identity thief uses the victim's identifying data to open a new account in the victim's name, or they use that same information to take over an existing account. In both cases, the identity thief looks to change the address from that of the victim to that of the thief. They do this for the simple fact that they want the corresponding checks, debit cards, credit cards and financial statements going to an address that is accessible to the thief, and not the victim.

Because people legitimately change residence very commonly, thieves know that they can easily and inconspicuously gain access of someone's account by fraudulently changing the address held by the victim's bank. This explains the fact that virtually every identity theft situation involves an address change.

Now, it would be great if solving identity theft were as simple as looking for someone changing their address. However, it is not that simple, as approximately forty percent of all new demand deposit account applications feature a situation where the application address differs from where the bank "thinks" the consumer lives, and fifteen percent of all existing accounts change addresses annually in the U.S. In short, honest people move all the time, and finding the identity thief hiding within all these legitimate



ADAM ELLIOTT

address changes requires finding the proverbial "needle in the haystack." Until recently, there wasn't much available by way of a tool set to effectively seek out and uncover this fraud.

The good news is that there are new and emerging technologies that effectively smoke out the fraud in the stack of address-change transactions. By effectively determining which address changes are legitimate and which ones are fraudulent, identity theft can be eliminated and more legitimate customers can be protected.

For example, say a long-standing customer who lives in a 3,000-square-foot house in an affluent suburb abruptly changes his address to a seedy motel in one of the highest crime areas in the country. It's likely that the bank would only see this as a move from 123 Main Street to 456 Oak Street, without any additional knowledge of either address. But, with new technologies that utilize highly complex analytics and cutting-edge data mining techniques, banks can now learn everything about the address change in question, and then accurately assess the risk of fraud – in fractions of a second.

The implications of effective address risk management will only continue to pick up steam with the new Red Flag Guidelines included in the FACT Act. A flagship piece of these imminent regulations is the requirement for banks to form a true belief of identity when presented with an address change. But compliance aside, managing risk in address changes will open a tremendous opportunity for banks to truly squash the identity theft problem, better serve customers, and ensure their long term trust.