



Identity fraud, front office or back office, where is the best place to catch it?
By Bob Cofod, President, BANKDetect

We often think that screening identities at the teller line and using an identity verification service for new account opening are viable stop gaps for identity fraud. There is no 'holy grail' when it comes to catching motivated criminals, and we often forget the value of a good account activity monitoring program for catching identity fraud at the point of its actual attack – the account. The truth is, you need both.

Just in case you still harbor the belief that only large financial institutions are targets for fraud, consider the recent fraud attack on Baltimore County Savings Bank, FSB in Maryland. A long established customer was discovered kiting. The estimated losses of \$6.9 million represent almost ten times annual net profit!¹

Theoretically all credit unions now have comprehensive new customer screening programs. This function was an optional precaution against fraud in the past, but it is now a requirement for Bank Secrecy Act and Anti-Money Laundering (AML) compliance. Such a program should include a combination of functions like: banking history search; verification of identity factors; searching databases for OFAC entities and Politically Exposed Persons (PEPs); and assessing the overall risk of the customer, the foreign country influences on the account, and the products and services used.

Recently regulators published a New Proposed Rule Making to require financial institutions to screen for identity theft “Red Flags.” It’s likely that in the next year or so you will need to add another compliance process to combat identity fraud.

So, with all this “screening” going on, we should stop fraud and money laundering in their tracks, right? Well, not necessarily, there are some chinks in the armor.

First of all, identity fraud (falsifying an identity) is only the first part of the problem. It is the means by which access to a new account or another’s account is gained. Then the real attack occurs and funds are stolen from either the credit union or its members.

Secondly, good customers can change. Some of the most difficult types of threats to detect are those that are conducted by employees or customers who establish a reliable level of trust before they change. Sex, drugs, health or relationship changes and a variety of other reasons can alter the behavior of

¹ http://www.baltcosavings.com/content/Press_Release/PR%2006-30-06.pdf

someone who has already gained our trust. Aldrich Aimes, was a highly trusted CIA employee for 31 years and actively spied for the Soviets for nine years before being caught in 1994. The CIA's identity screening was impeccable and repetitive, but the change in Aimes' behavior became a disaster for national security.²

The third reason identity screening is fallible is that Americans are passionate about their privacy and consequently we have no standardized and authoritative national identification program. The Social Security Number we commonly use for this purpose is, according to the Social Security Administration, intended only to allow individuals to track their social security benefits. While we can use credit reporting services and investigative sources to track SSN use, the reality is that the number itself is poorly constructed and controlled, allowing its manipulation for many types of identity fraud.

Finally, security in our world of proliferating data remains poor. Despite government regulations for maintaining privacy, each year identity data for millions of citizens is lost or stolen. Often the destination and disposition of this information is never learned. "Lost" identities may be held for years before they are used in a crime.

Aldrich Aimes was subjected to unimaginable "privacy invasion"(e.g., polygraphs, updated personal and financial statements, health screening). None of these uncovered his espionage.

Aimes' behavior finally did him in. And this is the lesson. Too often we set up a process designed to solve a specific problem. But the world is continually changing and old processes become obsolete. Once initial screening is completed, our attention must shift to monitoring an individual's behavior..

Credit unions, no matter the size, must continually monitor account activity for risk behavior in addition to performing new customer screening. AML compliance requires that high risk accounts be monitored with "enhanced due diligence." Also for fraud protection, all accounts need to be monitored on a daily basis for indications of suspicious activity.

Most financial institutions have relied on "exception" reports generated from the core processor as a means of detecting high risk activity. But these reports are also obsolete for assessing risk and defending against the wide range of fraud methods that are operating today. Modern automated transaction analysis systems have become more cost-effective and offer insights into a variety of risks that cannot be detected by traditional reports.

Briefly, whereas exception reports are paper based single focus views of activity (e.g., high dollar, new account, kiting, etc.) modern account activity analysis systems screen for many different dimensions of

² <http://www.time.com/time/magazine/article/0,9171,980263,00.html>

behavior simultaneously. For instance, they can analyze single transaction risks (of any kind) or they can analyze them as a group for inter-relationships. They can create a historical profile for the account and monitor a variety of potential variances from the profile. They can monitor for known patterns of activity that suggest high risk, including transactions over several days, or more. And, most important, these systems can produce a risk score for every transaction processed that dramatically aids in prioritizing work flow and filtering out false positives.

No financial institution can afford the type of loss experienced by the Baltimore savings bank. The threat has been moving toward smaller institutions for several years and even the smallest credit unions are potential targets.

Because credit unions are bound more closely to their members than banks, the responsibility of guarding against fraud losses is even more critical. Understanding how much front-office screening and back-office analysis are appropriate is not simple. But make no mistake about the need for both – they are required for BSA/AML compliance and they are a critical part of defending your members assets, as well as the credit union's reputation and future.

Bob Cofod is the President and founder of BANKDetect, which provides loss prevention and anti-money laundering compliance services to financial institutions. He has over thirty-five years experience developing and operating advanced analytical systems for the U.S. military/intelligence, healthcare and financial communities. He has been a speaker and author in various banking venues on the topic of loss prevention and anti-money laundering analysis. He may be reached at bob.cofod@bankdetect.com.