



Fraud - Is it a Gordian Knot ... or Not?
By Bob Cofod, President, BANKDetect, LLC

The credit card industry made significant investments in fraud prevention technologies decades ago. It was clear to them that detecting the indicators of fraud were more valuable than waiting for the losses to occur. Today, credit unions continue to experience fraudulent losses from a growing array of methods, yet the actual defenses against these threats often remain anemic, or non-existent.

In its "2005 Global Economic Crime Survey," PricewaterhouseCoopers made a number of observations that are relevant to credit unions:

- "Results show that larger companies often have the ability to - and do - implement a greater number of controls and risk management procedures than smaller companies..." (Suggesting to criminals that smaller companies are increasingly softer targets.)
- "90 percent of companies that had no fraud to report thought it unlikely they might suffer it in the future. This declined to 67 percent for those that had already experienced fraud in their organization."
- "While quantifying the financial damage from fraud is hard, it can be even harder to estimate the 'collateral damage' (significant damage to their brand or reputation). Yet 40 percent of the respondents reported a decline of staff morale or impaired business relations. Each of these elements is critical to the success of any business and all can be undermined by the occurrence - or even the perception - of fraud."
- "Irrespective of the type of incident, smaller companies reported suffering greater 'collateral damage' than larger companies, with 51percent of them reporting significant intangible damage compared with 39 percent of larger companies."
- "In the past two years, the average financial damage to companies from tangible frauds (i.e., asset misappropriation, false pretences, and counterfeiting) was US \$1.7 million."

Rather than justifying current attitudes, these messages should tell every credit union manager that there is a real threat that can and will target every financial institution, of whatever size, at some time. That threat has the potential of inflicting severe, even catastrophic, financial damage on any unaware and unprotected credit union. The collateral damage may be the most severe threat, since the credit union concept of "people helping people" would be jeopardized to the fullest extent.

Make no mistake, "fraud and abuse" are not simple problems, and this may be the reason so many managers seem to ignore it. The often-heard comment, "It's just too complex, and it won't hit us anyhow" can be detrimental. While this attitude is inexcusable, it is understandable when we consider the complexities of check fraud (e.g., forged maker, forged endorser, counterfeits, stolen checks, kiting, new account, ID fraud, account takeover, etc.), as well as online fraud (e.g., ID fraud, phishing, pharming, key logging, man-in-middle scams and others), electronic fraud (e.g., hacking, intrusion, etc.), mortgage fraud, loan fraud and a few others. The array of threats permeates nearly every functional and organizational component of most credit unions.

In addition to these threats, we must also consider the Bank Secrecy Act compliance requirements for anti-money laundering/terrorism financing processes. While these requirements are separate from the traditional fraud problem, failure to comply may result in a variety of unwanted fines, penalties and other serious regulatory judgments.

The range and complexity of threats span the skills possessed by staff in operations, security, loss prevention, communications, computer, human resources, legal, risk management, compliance, audit, collections and probably a few other positions. The question begs, who is in charge? How do we prioritize the counter-measures needed for the different types of threats? What is the relationship between the potential threats and our real risks? How do we insure coordination of the individual processes and the overall management of the total detection-prevention effort?

Fingerprinting, IP address location, two-factor authentication, data encryption, intrusion detection, transaction-risk analysis, customer-risk detection and other technologies promise to solve fraud and abuse, money laundering and terrorism financing risk. But, which ones solve which parts, and what are the risk-priority relationships that guide decision-making and investment? These are problems with which the largest financial institutions in the world are struggling. How then is the average credit union supposed to solve them?

It is crucial that credit union managers and board members come to the realization that fraud is a real and growing problem; it has the potential to impact every credit union, regardless of size. The financial loss incurred from fraud can be devastating to smaller institutions and being the target of a major fraud event can produce collateral damage with the potential to destroy the credit union's public image and member confidence.

Senior managers need to form a risk-based strategy for their particular needs. Every credit union should already have a "Customer Identification Program" risk assessment function as part of the Anti-Money Laundering requirements of the Bank Secrecy Act. This can be used as a template from which

the risks of your membership can be assessed. The risks that reside in products, processes, policies and procedures of the credit union also need to be acknowledged.

After identifying the vulnerable areas, establishing a central focus for identifying and prioritizing fraud/loss prevention investments is essential. This requires an understanding of how the various solutions needed fit together in support of an integrated technical and operational strategy. Without such planning and control, duplication and poor coordination will waste resources and reduce the effectiveness of the resulting processes.

Fraud risks are continuously changing as credit unions expand their member-bases and product offerings. It becomes impossible for CEOs to manage all of these factors for growing institutions. In such cases, a distinct intelligence-like unit charged with the responsibility for understanding the threats, relating them to the specific vulnerabilities of the credit union, and assessing the daily level of protection and prevention may be required.

Change is slow, particularly when it is driven by proactive ideas. But pro-action is far better than the knee-jerk reaction that results from ignoring the problem until a major fraud attack occurs. There is no reason for credit unions to budget significant dollars to fraud losses when strategically implemented solutions can help protect an institution's integrity, its members and its money.

As Al Capone once said, "It's strange that men should take up crime when there are so many legal ways to be dishonest."

Bob Cofod is the president and founder of Churchton, Md.-based BANKDetect, LLC, 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.