Potential threats may be on the rise

Facing Up to Fraud

There are plenty of reasons not to think about fraud. Maybe it hasn’t affected one’s institution in any meaningful way. Maybe the pressures of tight profit margins or increased regulatory responsibilities are more top of mind. Maybe it’s just no fun to think about such an unpleasant thing.

The truth is that any or all of the above factors may be conspiring to cause many institutions to pay less attention to the threat of fraud than they should be. But that’s the thing about fraud – the greatest risk comes from not being aware of it, and not thinking about it won’t make it go away. Therefore, the first step in addressing potential fraud threats within an institution is often simply identifying what those threats are and where they might exist.

External Threats

For all of the new risks associated with technological advancements and mobile banking, one of the most prevalent fraud threats to come from outside an institution’s walls may, in fact, be a pretty old-fashioned con game.

“What’s kind of surprising is that check fraud is still so substantial,” says E. Michael Thomas, a partner in the Financial Institution Risk Consulting division of Crowe Horwath LLP in Atlanta, Ga.

“Check fraud as a category, in terms of dollars lost, has continued to increase year over year at a pretty good clip. So con men are still making good money with these types of things.”

Check fraud can run the gamut from simple bounced checks and forgery to other timeworn schemes such as check kiting and new account fraud. Yet while institutions have long been on the lookout for these types of fraudulent activities, the steady-or-rising number of incidents suggests that many may not be paying as close attention as they should be. Further, while many larger institutions have set up sophisticated software programs and monitoring systems to keep an eye out for suspicious checking maneuvers, smaller community banks may not have the luxury of such advanced methods, leaving them at greater risk as criminals simply move down the line to more vulnerable targets.

Another “classic” scheme that has shown new life in recent years is mortgage fraud. Thomas says that after surging prior to 2008 amid loosened standards and lax due diligence, mortgage fraud receded considerably during the recession, as lenders tightened internal controls and became much more selective in considering applications. However, as the mortgage market has continued to climb out of its doldrums during the recent recovery, so too has the specter of potential fraud, especially for institutions that didn’t learn the lessons of the pre-2008 frenzy firsthand.

“We’re definitely seeing pockets of mortgage fraud starting to come back amid the recovery,” Thomas says. “Smaller institutions are now trying to get in the mortgage game to follow the trend and boost their earnings, and a lot of them don’t have the experience of having been through this before. So banks with the proper controls in place will be turning away a lot of the potentially fraudulent loan applications because they can screen them out, but smaller, less experienced lenders will be more susceptible to this type of thing.”

Even so, while their reemergence is certainly unwelcome, many institutions may at least have experience in dealing with schemes like check and mortgage fraud, and therefore likely have some semblance of internal controls in place to confront them. When it comes to external cyber threats, however, the rapid ascent of technology continued on page 2
– and the equally swift ability of criminals to capitalize on its exploitation – makes it exceedingly difficult for the industry to stay on top of the risks. Thomas says that many smaller community institutions probably dodged the cyber fraud bullet for a while, but with the adoption of more technology comes the potential for more fraud as well.

“Cyber fraud and identity theft didn’t really affect community institutions for a long time simply because those places didn’t offer a lot of the products that were susceptible to this type of threat, such as Internet banking and mobile banking,” he explains. “But the world has changed, and now even the smaller community banks can offer these services.”

Thomas also thinks that for all of its potential upside, a greater reliance on technology can undermine one of the biggest advantages that community institutions have long relied upon and open them up to a bigger risk of fraud.

“Community banks also knew their customers better than the bigger banks, which can be a significant deterrent to potential fraud,” he says. “I do see some of the smaller institutions becoming vulnerable now because one of the great controls that they always had was this ‘know your customer’ rule, and now they’re doing so much by email and the Internet, they might not have that close relationship anymore. Once you start layering technology between you and your customer, you’re opening the opportunity for con men to steal your customers’ identities or come to your bank pretending to be your customer and commit a number of fraud schemes.”

Internal Threats

In addition to the threats that exist on the outside, institutions need to be just as concerned about potential internal fraud opportunities as well. A recent McGladrey survey targeting specialty lenders found that half of the respondents had experienced some sort of internal fraud within the preceding twelve months, ranging from cash thefts to loan fraud.

Angela Morelock, a partner with BKD Forensics in Springfield, Mo., says that most internal fraud schemes are related to loans, with insider lending, undisclosed relationships and links to insiders comprising the bulk of the trouble. But she’s also seen an uptick in a fairly bold and straightforward brand of employee crime recently as well, directed at both customers and the bank itself – the cash scheme.

“Cash schemes often involve direct theft from customer accounts by tellers or branch managers, and these are usually high net worth and elderly victims,” she says. “But we’ve also seen a lot of vault shortages in the last two to three years – some in the $1 million to $2 million range. These are situations where not every part of the vault is being counted every day, or coins or mutilated money bags are not being accounted for.”

The Cost of Fraud

As one might expect, the McGladrey survey found that in most instances of fraud, little or
none of the losses were recovered – the money is often long gone by the time the incident comes to light. Although the financial cost of fraud may be fairly easy to calculate (if not so easy to swallow), in many instances the dollar loss is only the beginning.

Thomas recounts a story from a few years back of a small community bank in suburban Atlanta where the CEO made $1 million in phony loans before the FBI finally came in and brought it to light. In the end, the bank could have weathered the financial hit of the fraud, but it couldn’t survive the reputational damage of having the head of a community institution in a small, close-knit town involved in such a thing.

“The hardest thing for a community institution is to recover from the reputation hit and to regain the confidence of its community,” he says.

Managing the Threats

Both Thomas and Morelock agree that the key to preventing external and internal fraud is to have strong controls in place. For something like loan fraud, for example, simple steps such as verifying third-party collateral and documentation and conducting a strict review of origination procedures can be augmented by more rigorous data mining and pattern recognition practices to help detect suspicious activity. But whatever the underlying fraud, procedures on the books are only as good as the ongoing attention they’re given, and that’s where things can slide amid the day-to-day issues of running the business.

“You can have the best risk procedures in the world, but unless everybody is actually following them and they’re actually operating effectively, you don’t get the control that you think you might be getting.”

Angela Morelock
Partner, BKD Forensics
Springfield, Mo.

“Where I’m seeing the biggest risk is where small institutions especially are buying various technology solutions like mobile and Internet applications and letting the salesmen from those vendors tell them what they need for internal controls instead of bringing in the right people who are actually experts in internal controls, who actually understand the risks,” he explains. “Institutions absolutely have to embrace technology and offer these products and services in order to stay competitive, but they don’t have to do it blindly. It’s a matter of getting beyond the sales pitch to really understand where these new technologies might make the institution vulnerable.”

So the fraud risk today is a combination of both old (check fraud) and new (technology threats), and both internal and external, but Thomas believes that the biggest risk by far is actually much more a matter of mindset than anything else.

“The biggest risk in community institutions is the belief that it won’t happen here,” he says. “Institutions that believe fraud won’t happen to them are the most vulnerable, because it means they trust people over internal controls. It’s not that they shouldn’t trust people, of course, but they need to look at the notion of keeping honest people honest. A lot of times, it takes the big fraud actually happening for a bank to believe that they’re at risk, and then they’re very adamant about putting the right controls in place, but it’s too late to prevent the damage.”