

Login

About FMS

Membership

Join Mailing List

Calendar of Events

Education

FMS Bookstore

Career Center

Web Resources

Member Resources

FMU, 8-5-08**Fraud vulnerabilities***High-level managers, execs represent significant risks, says expert*

Anti-fraud programs at financial institutions must effectively monitor senior managers and executives, since those individuals represent major potential risks in the current environment, a fraud specialist warns.

"This is where your real risk is—at the top of the organization," says fraud expert Angela Morelock, accountant and partner, BKD, LLP, Springfield, Mo. "These folks are going to get you for the big dollars."

The impact of fraud on the financial services industry is huge, and it's imperative for institutions to have effective fraud prevention programs, said Morelock, who made her comments at the recent FMS Finance & Accounting Forum in Orlando, Fla.

Such programs must ensure that the institution:

- Reviews personal accounts of employees and officers.
- Performs electronic analysis of the institution's loan master file.
- Trains tellers not to accept unusual transactions from insiders.
- Encourages questioning and reporting of unusual transactions.
- Has in place a confidential hotline.
- Is aware of relationships between insiders and loan customers.

Morelock said that data from a 2006 report on occupational fraud by the Association of Certified Fraud Examiners (ACFE) shows that instances of internal fraud within financial institutions are committed by all levels of employees.

Perhaps surprisingly, the study indicated that managers were responsible for 41.2% of reported cases, owner-executives for 19.3%, and employees, 39.5%. "And that sends a pretty important message to us," Morelock said. Supervisory and management-level employees perpetrate more fraud than employees at the line level.

However, Morelock noted that institutions usually do their best job of fraud prevention by setting up checks and balances at the bottom echelons. "We can build a great internal control structure at the bottom of the organization in our sleep—we're really good at that," she said.

But if one considers the control of an institution's supervisors, department heads, management, and senior management—then it's much more difficult to have effective checks and balances, she explained. "There is nothing harder than controlling 'up' in an organization."

"It's the area where we do not do the greatest job of building internal controls," she said.

Median losses

While research data indicates that the median fraud loss at institutions rises in correlation with the perpetrator's age and education level, not surprisingly it also rises with the position of the fraudster within the institution. The median losses, when separated by position, are: employees, \$78,000; managers,

\$218,000; and owner/execs, \$1 million, she said.

The data also indicates that in comparison with other industries, banking and financial services have experienced the greatest frequency of fraud, with a median loss of \$258,000 per case.

National fraud researchers normally describe the typical perpetrator as a college educated white male who is intelligent, married, and usually a loyal employee. "And those types of employees are really the most difficult for us to accuse, because their dedication is usually so highly valued by an organization," Morelock noted.

Significantly, however, she expressed a view that contrasts with the perspective taken by the national researchers.

"I disagree with the college-educated white male profile a little bit," she said, pointing out that large national cases like Enron and WorldCom have tended to slant the profile to that demographic. Based on the cases she typically investigates, the fraudsters are both male and female.

And although the demographics for various employee positions at institutions are changing, she said that if a fraud probe focuses on the clerk level, line level, or bookkeeper level in the accounting department, then it "seems like we are investigating a lot of females." But in the cases involving investigations of chief lending officers, CFOs, CEOs, or senior managers, frequently those individuals are males. "That's frankly the way we see the gender split," she added.

National data also shows that less than 8% of fraudsters have prior criminal backgrounds. "They're incredibly well liked by co-workers—often times the most popular people in the organization, she said. "They are very good at reeling you in over time."

Typically, those who perpetrate fraud are long-term employees, many with their institution for 15 to 25 years. Since these employees usually are trusted by others and have built up a certain amount of "informal authority" over the years, other people in the organization will do what they tell them to do.

"And we do see a lot of long-term employees take advantage of that," Morelock said. Usually the person starts fraudulent activity in small ways, perhaps by rationalizing that the fraudulent act is just "borrowing."

She advised CFOs and others: don't wait for an official fraud investigator to show up before you begin to look into what you think is a case of criminal fraud. "Don't feel bad about it, don't feel guilty about it, and don't be afraid to go look into something that goes contrary to that gut instinct," Morelock said. "Don't be afraid to be suspicious—especially in this industry."

Lifestyle clues, such as a \$45,000-a-year trusted employee who purchases a \$390,000 house, are usually some of the best early warnings of a serious embezzlement problem, she said.

Another lifestyle clue might involve compulsive shopping. "One big category that we see are collector items," Morelock pointed out. "Not only are they ordering this stuff—they are having those packages delivered to the office."

Fraudsters sometimes are lavish gift givers, including "spreading that money around in the office" as gifts to co-workers. "So the next time somebody gives you a really expensive Christmas gift, that's going to throw up a red flag for you as well," she warned.

Fraud schemes

While there are many types of fraud schemes, the most frequent types include cash larceny, skimming, billing, and check tampering. Other reported fraud cases involve wire transfers, expense reimbursements, payroll schemes, and register disbursements.

Within financial institutions, some common areas of concern to watch for include personal credit problems, NSF in personal accounts; unusual transactions in personal accounts; management override of

internal controls; or a second person signing off on transactions based on trust.

As for "non-cash" cases, the most commonly reported scheme involves the theft of proprietary information from bank customers.

Typically, certain risk areas at institutions get more attention from risk managers than others. "We pay a lot of attention to cash, and we pay a lot of attention to loans—we know those are two big risk areas," Morelock said.

But certain areas involving fraud that often don't get enough attention include payroll and accounts payable. "Those kind of fall to the back burner in this industry and don't get as much emphasis in terms of fraud prevention and internal control," she said. And they should.

Common accounts-payable and purchasing schemes include: paying personal bills; fictitious suppliers; kickbacks; ordering personal items; stealing from petty cash funds; fudging employee expense accounts; and the misuse of corporate credit cards.

Check tampering

Morelock also noted the ubiquity of problems involving check tampering, wire transfers and expense reimbursements. "That's a problem everywhere we go."

She said that institutions should consider ways to strengthen their fraud prevention and detection. One approach not used frequently enough involves utilizing commercial data-mining software, enabling bankers to look for anomalies in databases. Such data-mining can provide added protection in various areas, including payroll, accounts payable, expense reimbursement, loans, sales, and inventory.

But in toughening up fraud prevention programs, institutions especially need to remember to keep an eye on senior management and officers, Morelock said.

"You can't review everybody every year—but at least get senior managers, lending officers and personal-accounts personnel," she said.

Additional Resources

[Managing the Business Risk of Fraud: A Practical Guide.](#)
[New guidelines for fighting fraud have been released jointly by three leading professional organizations](#)

 Print Version