Issue #27
July 2014

GREAT AMERICAN and LOWERS & ASSOCIATES

Fidelity / Crime Observer

Vow of Poverty, Life of Luxury

When you think of embezzlement, you may think of Wall Street and the business community. Much embezzlement takes place at banks, retailers, and manufacturers, however, religious organizations are not immune as evidenced by the story of one parish church.

Monsignor Douglas was the pastor of Corpus Christi Church (CCC). After being ordained he obtained a doctorate in classical languages, acted as a dean and president of a university, and became a monsignor. He was subsequently appointed pastor of CCC, a position he held for twenty years. He was described as very refined and cultured as well as an accomplished violinist. His parishioners thought very highly of him.

Although the monsignor attended to his pastoral duties diligently, he had a penchant for luxury vacations, including trips to Las Vegas with friends, dinners at fine restaurants, and Broadway shows. Because of his refined and cultured appearance, parishioners believed he either came from a wealthy family or his friends footed the bill.

The story unfolded shortly after the monsignor exhibited some odd behavior. He was seen having loud conversations with people not connected with the parish about cash. The controller for the diocese conducted a preliminary review of the Sunday collections. He found that collections were not being recorded correctly so he had an accounting firm conduct an audit. The audit revealed a discrepancy between what was collected and recorded in the Sunday bulletin and what was deposited. The monsignor explained that he used some of the money for church and operational expenses such as groceries and charity cases.

The diocese came up with procedures they wanted the monsignor to implement so that all cash collected at mass would be accounted for. In the following months, Monsignor Douglas refused to implement the procedures so they brought in Monsignor Burns to take over as pastor.

When a parish gets a new pastor, the diocese reviews the financial situation with the incoming pastor. Around this time one of the employees working in the rectory came across a bank statement that she gave to Monsignor Burns. He noted the bank account was not on the parish's financial statement. It turned out to be a dormant account that was used for a specific fund raising activity years ago. Their accounting firm looked into the account and discovered that for a ten year period, $2.6 million dollars was deposited and withdrawn.

The majority of funds going into the account were checks payable to the parish. Monsignor Douglas also moved funds from the parish's investment account to the fund raising account. Disbursements included checks made out to him, his friends, and cash. Some money was used for church business.

Continued on Page 4

Contact List

Great American Insurance Group

Dennis Burns, VP
Fidelity / Crime Division
212.513.4017
dburns@GAIC.com

Lowers Risk Group

Steve Yesko, ARM
VP, Bus. Development
540.338.7151
syesko@
lowersriskgroup.com

Inside This Issue

Are You Doing Enough To Protect Against Financial Fraud?

Yet more evidence of the prevalence of financial fraud against organizations has emerged from a recent poll by Kyriba. The poll found that almost 80% of organizations had been victims of fraud. The very high proportion of victims is startling in itself, but it is consistent with information we have presented in previous articles that organizational fraud is a global problem, costing 5% of top line revenue annually.

Almost 30% of the respondents to the Kyriba poll reported suffering financial losses, but we think this is a conservative number in this context. Organizational fraud is a hidden crime that sometimes is difficult to detect, even long after the fact. When organizations do detect fraud, they may have incentives to minimize publicity about the crime, so underreporting is probable.

Fraud Occurs, But Fraud Prevention Lags

Taken together, this information is a clarion call to executives and managers to implement rigorous anti-fraud controls. Yet the poll found that over one-third of respondents had not reviewed or updated their fraud prevention controls in over a year. In fact, 18% believed that their organization had *never* installed or updated a fraud prevention program.

Almost 80% of companies have been victims of fraud costing 5% of top line revenue annually.

Sometimes it seems like it should be easier for victims, many of whom are sophisticated individuals or organizations, to detect financial fraud. But the Bernie Madoff case has shown us how easily investors can be fooled by timing deposits, moving cash from one account to another, delaying responses to questions, or simply not providing requested information at all. All of these kinds of subterfuges should be detected by a fraud prevention program, but obviously the program has to exist in the first place.

A new range of threats has evolved in the rapid growth of extensively networked digital systems. We have seen the massive losses that external theft can cause, as in the Target case, but loss potential is also large for internal theft and fraud. The challenges in these cyber thefts involve both organization (comprehensive access control, for example) and continuous reviews of performance through audits of digital transactions.

Active Prevention Processes are Essential

We have long argued that systematic financial fraud prevention controls should be an integral part of every organization's risk management program. We cannot know with certainty, in advance, when unseen flaws in controls will be found, or flaws in software will come to light.

An organization's best defense against these possibilities is regular, rigorous audits and internal controls designed to detect irregularities in financial flows quickly.

By D. Mark Lowers,
President / CEO
Lowers Risk Group

How Are You Handling This Year's Emerging Risks?

The Edward Snowden case and the theft of Target customer data both drive home the point that cybersecurity is an emerging, and rising, risk issue for both companies and political entities. But there are other risks that emerge as rapidly-changing multi-market regulatory and business interactions redefine the landscape.

This year business consultant CEB (Corporate Executive Board) issued a list of ten specific emerging risks that they recommend managers address:

- → Compliance Management
- → Cybersecurity: Malicious Insiders
- → Risk Management
- → Cybersecurity: Malicious Outsiders
- → Emerging Markets
- → IT Governance
- → Third-Party Relationships
- → Project Management
- → Intellectual Property
- → Crisis Response Management

The main reason to review a list like this is that changes in the business environment can make companies' risk management plans obsolete or improperly targeted. Changes in regulation alone make compliance a major problem, not to mention the fact that multiple regulators issuing new rules may create unintended conflict that in turn increases the potential for compliance risk. Risk managers need to allocate resources to evaluate and respond to this new control environment.

Changes in the business environment can make companies' risk management plans obsolete or improperly targeted.

An Actionable Emerging Risk Agenda

To help move you toward an actionable plan to address these emerging elements, Friso Van Der Oord and Jeffery Ugbah at RM magazine have consolidated the 10 risks identified by CEB into four analytical themes. The themes are:

Businesses are increasingly entangled in networks of stakeholders, partners, clients, and suppliers who expose them to risks that are difficult to identify and evaluate.

The downside of business interdependence: Businesses are increasingly entangled in networks of stakeholders, partners, clients, and suppliers who expose them to risks that are difficult to identify and evaluate.

Balancing business control and value creation: The risks of many new business opportunities are opaque, such as in emerging markets. In these circumstances, managers have to make difficult decisions balancing risk against expected value.

Embedding compliance and risk discipline into the business: The increasingly complicated and sometimes conflicting regulatory demands require a higher and more sophisticated approach to compliance management. Formal full-scale enterprise risk management initiatives are part of the solution.

Blind spots inside our organizational perimeter: Dependence on digital technology creates new risks within the organization, as well as in the external networks it is connected to. IT security spanning everything from cyber spying to employee fraud becomes even more urgent.

The speed of change is not likely to slow down anytime soon. It will continue through good economic conditions and bad as governments, corporations, and businesses in general seek to gain advantages and control. Smart organizations will commit significant resources to identify these tendencies and develop policies to cope.

If you need help formulating your enterprise risk management strategy, let's talk.

By D. Mark Lowers,
President / CEO
Lowers Risk Group

Vow of Poverty, Life of Luxury

Continued from Page 1

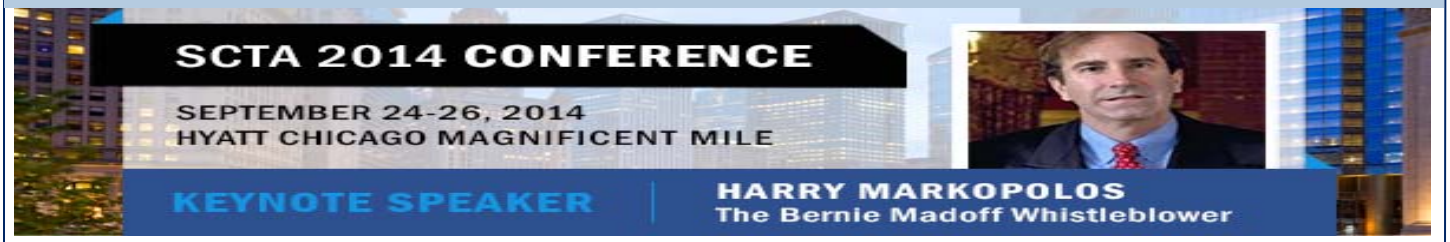
A full investigation disclosed cash shortages at the school, Sunday collections, and votive candle donations. Employees came forward to tell the investigators that Monsignor Douglas told them the cash was being used for church business. They thought it appeared suspicious but they never questioned his explanation or brought their concerns to other priests.

The monsignor got away with the theft for several reasons. First, he knew the dormant bank account was no longer on the books and it would never be audited. He was able to divert church funds to the account without anyone finding out. It is a sound practice to close any bank account at the time it is no longer needed. Secondly, for twenty years he was the most respected person in the parish. Monsignor Douglas was the last person anyone would have suspected of theft. Another sound practice is having an anonymous tip line for employees to report suspicious activity. Often times, employees feel intimidated when they suspect someone is stealing, especially when it's the boss, so they keep quiet. The tip line gives them an anonymous way to report their concerns.

As for the monsignor, he pled guilty to criminal charges and was sentenced to four years in prison. He was also removed from the priesthood. His life of luxury was over.

By Tom Maloney, Vice President, Crime Claims
Great American Insurance Group
Fidelity / Crime Division

Join Us in Chicago for the 2014 SCTA Conference



An Event for Professionals in Cash-In-Transit and Cash Servicing

We invite you to join us at the Hyatt Chicago Magnificent Mile on September 24-26, 2014 for the Secure Cash & Transport Association (SCTA) Conference. As founding members and Gold sponsors, Lowers Risk Group and Great American Insurance Group are pleased to support this powerful event and hope you'll make plans to attend.

HERE ARE A FEW HIGHLIGHTS:

- ☑ Attend a keynote address and seminar by Harry Markopolos, the Bernie Madoff whistleblower.
- ☑ Take part in more than a dozen informative sessions covering topics ranging from cash management in the new legal marijuana trade to ATM jackpotting fraud.
- ☑ Network with leading professionals representing a wide range of organizations in the cash servicing and CIT industries.
- ☑ Enjoy the Hyatt Chicago Magnificent Mile in the heart of Chicago, steps from Michigan Avenue, the Gold Coast neighborhood, and Lake Michigan.

FOR MORE INFORMATION—CLICK HERE