GREAT AMERICAN & LOWERS RISK GROUP | ISSUE #44 | JANUARY 2019

FIDELITY/ CRIME OBSERVER

BENCHMARKING FRAUD

TABLE OF CONTENTS

HOW DOES YOUR ORGANIZATION COMPARE?

The Association of Certified Fraud Examiners 2018 Report to the Nations on Occupational Fraud and Abuse offers a treasure trove of data you can use to assess how your organization's fraud profile stacks up against other organizations in terms of industry, size, and location.

The Report is based on case data reported from Certified Fraud Examiners (CFEs) from all over the world. It lends itself to benchmarking your organization because it allows you to compare your own experiences against the medians reported from broadly similar organizations. Perhaps most important, you can learn about how other organizations responded to fraud.

Continued on Page 4

ABOUT US

Lowers Risk Group
provides comprehensive enterprise risk management solutions to organizations operating in high-risk, highly-regulated environments and organizations that value risk mitigation.

Great American Insurance Group
understands the importance of choosing a financially strong company. We are an organization built for the long term and are committed to giving you that strength. For nearly 150 years, Americans have trusted us to protect them. Our innovative insurance solutions and specialization serves niche marketplaces that we know well. This expertise gives us a successful foundation that spans generations.

CONTACT

GREAT AMERICAN INSURANCE GROUP

Dennis Burns, SVP
Fidelity / Crime Division
212.513.4017
dburns@GAIG.com
greatamericaninsurancegroup.com

LowersRiskGroup®
Protecting People, Brands, and Profits

Brad Moody
EVP Operations
540.338.7151
bmoody@lowersriskgroup.com
lowersriskgroup.com

HOW ORGANIZATIONS RESPOND TO FRAUD

You discover your erstwhile trusted employee has been skimming funds to support a gambling habit. What do you do?

Your first response is possibly unprintable, and understandably so. Your cooler head will prevail, and look at a small series of options for recovery, and maybe a dollop of justice. If there are losses, especially substantial losses, you will look at the circumstances of the fraudster carefully and evaluate the alleged crime for prosecution. You will look into the possibility of recovery and what the sources of recovery might be. The disruptive impact of being the victim of a crime might very well turn your thoughts away from revenge to the more practical goal of remediation.

The case studies analyzed in the 2018 Report to the Nations on Occupational Fraud and Abuse suggest a range of options organizations choose in the wake of a fraud. The Report, a study published every other year by the Association of Certified Fraud Examiners (ACFE), includes actions both through internal mechanisms and through external legal channels.

HOW ARE FRAUDSTERS PUNISHED?

It will come as no surprise that 65% of the fraudsters were simply terminated. 12% of organizations agreed to a settlement with the perpetrator and 11% of organizations say the perpetrator was no longer with the organization. What you might not expect is that 6% of organizations took no action and another 8% put the perpetrator on probation or suspension. The methodology of the study asks participant organizations about their biggest fraud case in the recent past, so a no action result suggests there are some very complicated circumstances below the surface. At the least, these widely disparate outcomes imply that organizations conduct an investigation of the fraud, and the evidence might point to a prudent course of action other than termination.

THE PERPETRATOR'S POSITION IN THE COMPANY IMPACTS THEIR PUNISHMENT.

The perpetrator's role in the organization clearly modifies the organization's response. An owner or executive is much less likely to be terminated (44% compared with 65% overall), and also much more likely to receive no punishment (12% compared with 6% overall). 72% of ordinary employees who committed a fraud were terminated.

LAW ENFORCEMENT IS NOT ALWAYS INVOLVED.

In the legal realm, uncertainty is increased by the fact that the alleged fraudster is innocent until proven guilty. The outcome of a civil action or criminal prosecution is not a given. Still, in 2018, 58% of frauds were referred to law enforcement and 23% resulted in a civil suit—the majority of these legal actions were resolved favorably to the victim.

LEGAL UNCERTAINTY ABOUNDS.

Yet the legal uncertainty is reflected in the fact that 12% of fraud cases are settled by agreement even before any legal action is taken (18% of owner/executive cases). In the group of civil cases, 27% are settled by agreement. And, fully 15% of civil cases result in a judgment for the alleged perpetrator.

The risks deter some organizations from taking legal action. 38% of these organizations cited bad publicity as the main reason, and other risks might also impose costs. Compounding the reasons to avoid legal action is the fact that in 53% of cases the victim recovered nothing, zero dollars. The more victims lose, the smaller the proportion they recover.

It is clear that organizations look at the cost-benefit value in deciding on what course of action to take in response to a fraud. Revenge may feel good, but it doesn't serve the organizations' interests.

A BREAKING & ENTERING CRIME LEADS TO DISCOVERY OF A THEFT

Tom Maloney – Vice President, Fidelity / Crime Division

A cosmetic company felt they had excellent controls over their warehouse operation. They conducted yearly inventory counts and monthly cycle counts of product randomly chosen by an outside CPA firm. The warehouse had cameras and a security guard from an outside firm.

The year-end inventory count conducted in January was clean. During the subsequent months, Peter Larkin, the warehouse manager, was sporadic with his cycle counts. He came up with excuse after excuse as to why they were late. When they were finally completed, a discrepancy was revealed. One reason for such discrepancy might be that the product could have been moved from the location in the warehouse where it should be to another location of the building. Larkin was ordered to search the warehouse.

It was around this same time that the police received a 911 call regarding break in at Larkin's home. When the police arrived, they found Larkin's live-in girlfriend standing outside. She was visibly shaken. The officers found signs of forcible entry on the back door. The house was ransacked.

She told the officers that Larkin worked in a warehouse for a cosmetic's company and that he was involved in stealing product. She said that he kept a large amount of cash in the house that could have been what the burglars were looking for. The girlfriend said she feared for her life.

She led the police to a closet where they found $100,000 in cash. She gave them the names of Larkin's associates who she knew helped him steal.

As a result of the information, a second investigation into the warehouse thefts was established.

The police provided the names of all employees believed to be involved in the theft to the company. The names included Steve Davis, Larkin's boss. Davis was in charge of the operation as the director of distribution. They also mentioned Robert Lucas, a security guard.

The CPA firm was brought in to conduct a count of the entire warehouse. They found 60,000 bottles of perfume, worth $580,000, missing. There was a hot black market for the perfume. As part of the investigation, the company reviewed security tapes. The tapes confirmed that on numerous occasions, employees moved pallets of product to a bay normally used solely for garbage. A van, driven by Larkin, pulled in. The pallets were loaded into the van. Another employee drove out.

Employees were interviewed. Two lower level employees admitted that Larkin paid them $300 to move certain pallets to the garbage bay and load them into the van. They also admitted to cutting the bottoms of cartons, removing the product then resealing the boxes and placing the empty cartons back in inventory. Lucas admitted that Larkin "slipped him a few bucks" to turn a blind eye to what was happening. After being confronted with the video evidence, Larkin admitted to the scheme. He implicated Davis as well. Davis apparently discovered the thefts and demanded a cut to keep quiet. Davis denied any knowledge of the thefts. He was fired from his job. The company found $30,000 in cash in his desk. He said he didn't know how it got there.

Although the company had good controls in place, several factors enabled Larkin to steal product. First, the security guard took payments to ignore the thefts. The company cancelled the contract with the security company. Second, although the CPA firm randomly chose the items for the cycle count, it was Larkin's minions who did the count. The counts should have been conducted by an independent third party, not those who are in a position to steal. The minions gave the numbers to Larkin, who adjusted the count to match the book inventory. He should not have had the ability to adjust the count in the system. Third, nobody reviewed the tapes from the security cameras. Cameras act as a potential deterrent to theft but also provide evidence if product is stolen. The video should be reviewed as a routine security measure. Lastly, Larkin's boss did nothing to stop the thefts as long as he collected a cut of the proceeds.

BENCHMARKING FRAUD CONTINUED

YOUR RISK OF FRAUD

Industry sector makes a big difference in the incidence and cost of fraud. Private, for-profit companies have the highest incidence and the highest median loss, where not for profits have much smaller losses and fewer frauds overall. In between are publicly traded companies and government agencies. An interesting comparison is between private vs. public for-profit businesses, with the private ones suffering higher losses. In general, private businesses face less scrutiny than public ones.

One counter-intuitive finding is that defrauded small organizations (less than 100 employees) suffered losses almost twice as high as large organizations (100 or more employees) in absolute terms. It's not likely that the difference is attributable to the amount of money available—larger organizations offer fatter targets.

Among all types of fraud risk, corruption is one of only two types of fraud that is significantly more likely in large organizations (the other being non-cash fraud), perhaps because size offers more opportunities for small organized cliques to penetrate weak points, or due to a larger network of connections. Corruption is prevalent in almost every industry type, with the lone exception of professional services.

YOUR FRAUD PREVENTION MEASURES

The presence of anti-fraud controls, such as surprise audits, proactive data monitoring/analysis, codes of conduct, etc. is shown by the ACFE Report to reduce the medial losses associated with fraud. It is perhaps predictable that small organizations in the study were far less likely to have a full range of anti-fraud controls in place. They tend to have only the basics, such as internal audits, management review, and external reviews of financial statements. Right on cue, 42% of frauds in small organizations were caused by lack of internal controls, compared with only 25% for larger organizations which tend to have a far more complete and robust set of controls in place.

One important anti-fraud control is the presence of a tip line. This was present in a little over 20% of small organizations, but fully 80% of large ones. The reason the disparity is important is that tips are the most common way a fraud is detected.

Fraud is a threat to all types and sizes of organizations, but two tendencies in the data stand out.

- First, large organizations deploy more controls, and ACFE finds that every type of control tends to depress fraud.
- Second, large organizations are more likely to experience fraud by corruption, which is an intentional organized attack at the weak points in an organizations' links between units, internal or external.

The good news is that controls do work. Small organizations that may not have enough control due to cost or scale need to find ways to implement variations of these controls. The potential payoff from fraud averted or detected quickly is too large to not implement the controls.

What can the lessons and benchmarks embedded in the ACFE's Report to the Nations on Occupational Fraud and Abuse teach you about your own organization's risks? How can you become better protected?

WHO'S PUTTING YOUR ORGANIZATION AT RISK OF FRAUD?

Many times, occupational fraud is committed by an employee or third-party partner who is experienced and trusted. Which of your employees—or leaders—is likely to flip over to the dark side? And why?

Here are a couple of key takeaways about the question of "Who?" in the fraud equation:

- Anyone and everyone is a potential fraudster, but organizations must be aware that those in long-tenured, high authority positions can present a greater risk. Fraud prevention programs have to recognize this fact and plan extensive monitoring and controls to mitigate the risk.
- Identifying a potential fraudster can be difficult. Background checks can help, but some previous fraudsters may not have bad information in the public record. The fraud triangle of "red flag" factors on issues of motivation and opportunity may help to identify risks.

LONGER-TENURED, HIGHER-AUTHORITY = GREATER RISK.

Owners and executives have the most access to the organization's assets, and also have authority over some of the controls and processes established to deter fraud. They are also more likely to collude with others, and their frauds are more likely to be discovered by an external auditor or law enforcement. This argues for putting a risk management plan in place before fraud occurs, and to make sure the plan includes provisions for monitoring executive behavior as well as extensive controls on regular operations.

47% of occupational frauds reported were perpetrated by people with six or more years tenure with the organization. These long-term employees also stole far more money. In aggregate, the long-term employees caused much higher total losses than those who were with the organization less than six years. The length of tenure increases loss in all types of jobs, but the higher the authority the greater the loss. Both authority and tenure operate to increase the losses.

FOLLOW THE MONEY.

By department, the data tends to say, 'follow the money'. The two biggest threats come from upper management and accounting (with the high authority individuals by far the bigger threat). The single most common type of fraud is corruption, which strikes hardest in executive/upper management, and purchasing. Both of these departments are likely to be linked to both internal and external networks, which may foster systematic (often collusive) corruption.

Occupational fraud is estimated to have cost over $7 billion dollars in 2017. The warning to organizations is clear. There is no absolute certainty about the likelihood of any given employee committing a fraud. The organization's best response is systematic fraud prevention aimed at all levels and functions of the organization.