The State of Affairs Regarding Employee Embezzlements

STEPHEN A. PEDNEAULT

In this article, the author discusses how companies can prevent, detect, and protect against employee embezzlement.

The recent uptick in employee embezzlement is only the tip of the iceberg. While employee theft and embezzlement have always been a risk, in today's environment it is more significant than ever, even in the smallest organizations.

Even the San Francisco Giants became victims. This summer, the team discovered that a former payroll clerk, Robin O'Connor, may have stolen over $1.5 million dollars from the team over a 12-month period. Her case provides a great example of how an employee can steal a large sum of money from their employer and go undetected because of a lack of sound internal controls within the organization.

According to news reports, Ms. O'Connor received an annual salary of $80,000 and was entitled to bonuses. During the 12-month period June 2010 through June 2011, Ms. O'Connor allegedly diverted in excess of $1.5 million dollars to herself.

How did the team discover this alleged theft? Was it the Giants organization's internal controls, or management and board oversight over the financial operations? An internal or external audit? An anonymous tip? Management's recognition of a lavish lifestyle? None of the above. The

---

Stephen A. Pedneault is the principal and founder of Forensic Accounting Services, LLC, a public accounting firm. He is also a certified fraud examiner, certified in financial forensics, and a forensic certified public accountant.

Published by A.S. Pratt in the November/December 2011 issue of the *Financial Fraud Law Report*

discovery of Ms. O'Connor's $1.5 million diversion is being credited to her own actions when she applied for a personal loan in June 2011.

As part of the due diligence commonly performed within today's lending environment, the bank requested a letter explaining why she received several large payments. The letter, described as being written by Ms. O'Connor on Giants' letterhead, explained that two six-figure payments were additional compensation in response to her outstanding contributions, and included a phone number for confirmation purposes that was reported, in fact, to be Ms. O'Connor's direct line.

The case has received much coverage, in part because it involves the San Francisco Giants, 2010 World Series Champions, and also because of the staggering dollar amount this one employee was able to divert without any detection in such a short period of time.

WHAT CAN WE LEARN?

This case illustrates several significant and common issues. The most significant issue pertains to the lack and maintenance of quality internal controls. Clearly, no one independent of payroll processing was reviewing the amounts paid to Ms. O'Connor.

Embezzlement schemes committed by those with access and responsibilities for processing payroll are common and well-known. In many cases the theft simply involves those who process payroll issuing additional unauthorized payroll to themselves, or paying themselves amounts in excess of their approved compensation level. A basic control against such abuse is for someone independent of payroll to review the registers and reports on a regular basis, with specific attention to those who have access to or responsibilities for processing payroll. That would make it easy to spot such a scheme.

There is no end to the creativity of some employees. Consider the case of a payroll clerk who stole more than $400,000 over a four-year period, diverting and concealing funds within payroll while maintaining an "as expected" W-2.

The clerk figured out that the miscellaneous deduction fields used to withhold amounts from employees' payroll could be easily converted into

fields that would actually add amounts to her net compensation. She used this bit of knowledge in her own favor. Instead of putting positive numbers in the fields for after-tax deductions from "net" pay, she entered negative numbers. The software recognized the negative amounts, and in place of subtracting the amounts from her paycheck, it added them back to her net pay. Week after week her gross compensation, federal, and state tax withholdings were accurate, but her "net" compensation on average doubled her gross pay. At year-end, the W-2 issued to her properly reflected gross compensation as well as the required tax withholdings. The fields she manipulated were not fields reported on Form W-2, and each year her W-2 was accurate for tax reporting purposes.

How was her scheme discovered? Much like Ms. O'Connor's case, the internal controls within the organization did not identify the theft, nor did internal and external audits conducted during the four-year period. An odd statement uttered by the payroll clerk to a co-worker initiated a specific review into her payroll history, leading to the discovery. Had the clerk not made the statement, the scheme might never have been detected.

TRENDS

If these two cases seem like anomalies, they are not. Forensic accountants and fraud professionals report that the number of such incidents is escalating. Whether it's the economy, the rising unemployment figures or an increased reliance on software-based systems, the trend shows no signs of slowing down. And a Google search of news articles about employee embezzlement cases yields over 175 stories of these cases. They include:

- A 62-year-old transportation supervisor who was charged with embezzling $900 in public funds from the county.
- The former assistant to the head of the Washington (State) Medical Center who is accused of stealing more than a quarter of a million dollars.
- The Sparks, Nevada, office manager who was accused of embezzling nearly $750,000 from the construction company where she worked to pay for her gambling addiction over a five-year period.

- A Vermont municipal utility's former office manager who pleaded guilty to embezzling $1.6 million.

WHY IS THIS HAPPENING?

The increase in the number of these cases is due to a number of factors. Those in this field point to the decline in the economy as a primary reason. A recurring theme is that these employees are acting out of desperation to make ends meet under considerable personal financial pressure. Certainly many individuals are living day-to-day under significant pressure, trying to make their mortgages, credit card, and car payments, along with health care costs and all their other living expenses. Even in households with two wage earners, times are tough. Unemployment continues to be a major issue fueled by significant layoffs. The loss of employment by even one earner can add even more stress on a household budget. Such pressures can cause an otherwise law-abiding person to "rationalize" their need to "borrow" just a little to make ends meet, with the understanding that they will put it right back without anyone noticing. No harm, no foul, and no victim. It would be an interest-free personal loan, albeit unauthorized, that no one will miss anyway.

And then there are the more "traditional" stressors — people living a lifestyle way beyond their means, with no desire to reduce or change the "high life" they lead. In a disturbing number of cases, this is the explanation of why a trusted employee chooses to divert funds for their own personal gain. Cases involving individuals who used the stolen funds to satisfy personal addictions such as gambling, drinking or drugs also round out some of the excuses, but most forensic accountants will point to the number one leading motivation they have encountered as entitlement — the "Big E" as it is known. No matter the cause of the embezzlement, it is vitally important for companies to learn to prevent it.

IMPORTANCE OF INTERNAL CONTROLS

The major point here is that every organization that has employees, regardless of size, needs to design, implement, and maintain an adequate

system of internal controls, checks, and balances. They need to do all they can to ensure their funds are not easily diverted by any one of their employees. Some embezzlement schemes are complex, involving the creation of shell companies or fictitious vendors to fraudulently obtain payments for non-existent goods or services. Some involve collusion between two or more individuals or departments. In these cases, for example, an individual initiates a fraudulent transaction and a second co-conspirator approves it. Then, they divide the proceeds. These can be difficult to detect and often result is a significant financial loss when they are discovered. Others are downright basic but effective. However, in many instances basic internal controls could have either prevented or detected the problem early on, precluding or minimizing the loss.

The size and complexity of the organization will determine the level of controls needed, as well as the level of capacity needed to ensure the integrity and accuracy of each financial transaction. Understandably the largest organizations possess the greatest number of opportunities and also require a larger capacity than smaller employers. However, the financial impact of an employee theft or embezzlement is often greater to the smaller organizations. These smaller companies have less capacity to properly implement the required level of internal controls to safeguard the business from all the risks. Downsizing at all companies has also made things more challenging. Companies now have fewer employees in financial and internal audit roles. This often leads to one individual having too much access and opportunity to both divert funds and conceal their theft with little to no risk of being detected.

Regardless of size, every employer should identify many of the common, easily committed schemes, and put in place controls to minimize their occurrences. Some of the more common schemes are: diversion of cash receipts (checks as well as cash), paying personal invoices through an organization, submitting fictitious or fraudulent expenses for reimbursement, and processing inappropriate payments through payroll. If practical controls cannot be implemented due to capacity limitations, then companies need to implement measures that ensure a problem is detected as early as possible. A payroll clerk earning $80,000 per year should not be able to divert over $1.5 million in the course of 12 months, unless someone is not

reviewing the payroll activity and reports.

As we approach the paperless office, expect these incidents to increase. As employers strive to eliminate the waste and storage issues of paper transactions, they also lose the "paper trails" that often tripped up embezzlers in the past. Banks no longer offer or return cancelled check images, and most offer online access to review images. The problem is that few people, if any, have the time or inclination to go online and review every cancelled check. Unfortunately, unethical employees are banking on this. The same holds true for those organizations that accept credit card payments. Monthly merchant statements, once received in the mail, are now available online for review. Here, too, no one is printing and reviewing the statements to ensure an employee is not reducing his or her personal credit card debt through his or her employer's merchant account.

Payroll has become the latest entrant into the paperless category. Outside payroll services historically delivered printed payroll packages containing the registers and reports from each payroll period. Most, though, have shifted to either electronic delivery (CD-ROMs) or online access to the same information via their "cloud." This facilitates thefts through payroll because the reports and registers are never printed and reviewed.

These changes have caused more and more employers to rely on automated "controls" and systems, and simply trust that their employees are not abusing the system. That is, until something bad is discovered, and then it is back to the basics.

BOARD'S ROLE IN PREVENTING EMPLOYEE FRAUD

Internal controls start with the Board of Directors, and flow down, layer-by-layer, throughout the entire organization. Individuals occupying positions within each level need to be responsible for authorizing and approving the transactions and activity of those employees below their level. This includes the Board members reviewing and approving the activity of senior management.

Board members need to play a significant role in ensuring that proper controls and procedures are implemented and maintained throughout their organizations. The Board is often the only oversight over the senior

management team. In the case of the largest, publicly traded companies they must play a crucial role in corporate governance and compliance with Sarbanes-Oxley and other internal control oriented regulations. They must also make sure that both internal and external auditors are constantly testing the design, operating effectiveness and adherence to such controls within their organizations.

For all the other private companies, nonprofit organizations and government entities that exist (and there are many more of them than publicly traded entities), much less stringent requirements apply, so the oversight role of the board is much more important. These Boards (sometimes called Boards of Commissioners) should take their roles of providing oversight and direction very seriously.

Sadly, this is often not the case. In far too many cases, a victim organization had such Boards in place and yet a significant theft or embezzlement occurred. In these cases, investigations find that these Boards were not reviewing the controls or finances, or worse, were not maintaining adequate records of the Board's activities. When Board approvals are required for expenditures, compensation increases, and similar transactions, their discussions and approvals must be memorialized within the minutes. If this is neglected, it is much harder to determine approved activity versus that which was unauthorized. Often the matter becomes a "he said, she said," and proceeding with those aspects becomes difficult if not impossible to successfully resolve.

INVESTIGATING THE FRAUD

The three key goals when investigating a potential incident of employee theft or embezzlement are: 1) keeping the circle of trust to the ultimate minimum number of individuals; 2) maintaining the integrity of the individuals potentially involved as well as the integrity of the investigation; and 3) securing as much information as quickly as possible before it is gone.

Let's first address keeping the circle of trust to a minimum. Fraud investigators are often surprised at how easily information regarding an inquiry about a potential crime is leaked beyond those who need to know,

and even to the media. The risks and exposure to an organization from these leaks can often outweigh the losses experienced from the actual theft or embezzlement itself. It is critical that only those individuals who need to know are informed, and each one is reminded about the confidentiality of the matter.

Now to the need to maintain the integrity of the individual potentially involved. As with leaks, acting rashly, accusing employees, and lashing out can be dangerous to the victim organization. Backlash lawsuits and complaints filed by the accused employee are common. Expect them even when it is clearly shown that the individual stole from the organization. The safest way to ensure the integrity of both the individuals and the investigation is to place the potentially involved individuals on immediate paid administrative leave. It is best if this is done with as little attention as possible. In addition, make sure they are supervised as they remove their personal belongings, to ensure that they do not leave with company property. The person supervising them should be appropriate and knowledgeable of the investigation. This process should be done as quickly as possible, and should be done after consulting counsel and discussing options.

When it comes to securing information quickly, chances are that this will be a challenge. Ironically, it is very common for embezzlers to track their thefts, supporting their rationalization that the diverted funds are actually a loan to be repaid down the road. Yet once the theft comes to light, they will likely destroy, discard, or remove that information from the premises, in the hope that there will be no evidence remaining to show what they have done. Once this happens, the organization will be faced with the costly and sometimes impossible task of replacing that information. It is particularly difficult to get new copies of bank statements and cancelled check images, when the originals have been destroyed or discarded. Long delays and large invoices from the banks to support the needed research time are common. In some cases, getting the information may not even be possible. Merchant statements, for example, can often be retrieved online and printed. However, individual credit card numbers are no longer printed because transaction numbers are used for privacy purposes. Even when the victim organization is the one that processed the credit cards, merchant banks may refuse to help. When they contact the

bank to obtain the credit card numbers for identified transactions, the merchant bank often refuses, citing privacy and secrecy laws and regulations. With the new transaction number system, it is nearly impossible to detect unauthorized credits or reductions to an employee's personal outstanding balance if it is done through their employer's merchant system.

PROSECUTING AN OFFENSE

Once you've investigated the theft and confirmed that there is a significant issue, it may feel like you've reached the finish line. You did the work and now it is just a matter of bringing it to law enforcement, right? Wrong. In fact, the journey is only just beginning. Prosecuting the individual is not automatic. The success in having an embezzlement case investigated and prosecuted depends on a variety of factors, including:

- The jurisdiction in which the crime occurred;
- The form and capacity of law enforcement for that area;
- The dollar amount involved;
- The area of the country in which prosecution is sought; and
- Whether the crime will be prosecuted at the federal, state, or local level.

Fraud investigators know it all begins with a good case, good records, and the willingness of law enforcement and the prosecutor's office to pursue the case. Cases that move forward are those that can be investigated and compiled into reports that are easily read and adequately supported with original evidence. However, even a well-documented case may not be investigated or prosecuted due to the dollar amount involved, the level of resources available, or other more significant crimes that warrant law enforcement's attention. In some jurisdictions, thefts and embezzlements are welcomed and prosecuted, and result in jail time for the suspect. However, in other jurisdictions, financial crimes rank towards the bottom of the priority, and only receive attention if the dollar amount is extremely large, or if other factors or issues are present within the case.

Of course, most fraud professionals would like to see each and every

individual who has been shown to steal be prosecuted and appropriately punished for their actions. Unfortunately, the reality is that it depends on the case, and each case stands on its own. Successful prosecution is often based on the ability to put together a complete case, bolstered by a written report describing the details of the crime. That report needs to be supported by sufficient reliable evidence that has been appropriately preserved to better ensure its admissibility. Even a package with a bow on it is no guarantee of a prosecution, but anything less is often a sure-fire way to lose their attention.

That said, not every victim organization desires criminal prosecution as a means to resolve the theft or embezzlement. In fact, only one in nine cases ever makes it to the light of day. Many are quietly resolved without law enforcement's knowledge or involvement. Once an organization has information about a possible theft or embezzlement, it is best to consult counsel to discuss investigative and other options. This discussion needs to include, among many other things, possible outcomes to the organization if news of the crime goes public.

RECOVERING THE LOSS THROUGH INSURANCE

More often than not, an organization's best option to recover from this kind of loss is to file a claim with their insurance company. Recovering any of the diverted funds from the suspect is highly unusual. Chances are, the organization's funds have already been spent on the motivating factor for the theft in the first place. Even if the suspect owns real estate, it is almost always fully encumbered, leaving no means to realistically recoup any funds.

Insurance coverage for employee theft (historically called fidelity bonding) is commonly found today in an organization's commercial insurance package. While fidelity bonding still exists, it is usually found only in specific circumstances requiring it, such as with an individual who is responsible for an employer's retirement plan administration. Bonding is specific to each individual and has become very expensive as well as difficult to maintain administratively. Therefore, blanket coverage covering all employees has become the norm. Unfortunately, too few organizations

ever address the adequacy of their coverage until after a loss has been suffered. Fraud investigators will review a client's policies after a potential theft has been discovered and often find the organization has minimal to no coverage for this type of loss.

Organizations need to consider their options carefully within employee dishonesty coverage. Often there is an important option that covers investigation costs to assemble the records and file a claim that should not be overlooked. Professional costs to investigate a claim can run into the thousands and even tens of thousands of dollars. An organization that has been victimized may already have strained cash flows, especially a smaller entity, and using any remaining funds to complete an investigation could be a leading reason why the victim chooses not to pursue the details of the crime.

Recovering through insurance is also getting more difficult. Insurance companies are looking harder at these claims, and attempting to deny coverage more frequently than ever before. In the past, insurance companies would review a claim, often enlisting the assistance of forensic accountants to evaluate it. Once they were satisfied with their procedures, they would send the victim organization a check settling the claim, minus the policy deductible. Not anymore.

Today, insurance companies will often take a good hard look at the personnel file of the person accused of embezzlement. They will be seeking anything in the employee's file that implies that the employer knew, or should have known, that the individual was dishonest and not trustworthy. In one recent claim, the policy stated that it would not provide coverage if the insured knew of anything in the individual's background that could make the person dishonest. The insurance company took the position that there was no coverage from the point in time they knew (or should have known) that the employee was not trustworthy. For this reason alone, it is critical for every employer to consider how he or she will handle minor employee issues prospectively. Even a minor non-financial issue that is documented within an employee's personnel file could be interpreted by an insurance company as showing the person to be less than trustworthy. Those employers willing to give an employee a second chance after discovering a small loss will want to seriously reconsider their policy because

of this risk and potential lack of coverage. While it is often human nature to want to "do right for the employee" it could be very expensive if that person doesn't live up to an employer's trust during their second chance.

GOING FORWARD

Every employer should be thinking about the risks associated with an employee stealing or embezzling from his or her organization. The frequency of occurrence has risen to the level that it is no longer a matter of "if" but rather "when" embezzlement will occur. Implementing sound yet practical controls is the best defense in preventing fraud schemes from occurring. That defense needs to include limiting access or opportunity in each financial area to the least number of individuals. Prevention alone will not suffice as often perpetrators will circumvent the controls and conceal their diversions from discovery. Therefore, detection measures are equally critical in minimizing the risks associated with theft and embezzlement. The goal should be to ensure that someone who is independent of each financial process reviews transactions and activity regularly to detect a potential problem as early as possible. Preventive controls are designed to prevent unauthorized activity to occur, while early detection procedures minimize the loss.

Beyond prevention and detection, every employer needs to maintain adequate employee dishonesty insurance coverage to have a means of recovery in the event of a loss.

In the future, the potential for dishonest employees to steal and conceal their thefts will only increase as more transactions are processed through new means such as wireless and cellular technology. This trend of departing from traditional paper reports and audit trails will ensure improprieties are easier to accomplish. Every employer needs to regularly consider how changes will create new opportunities and new schemes.

In the words of the late Ronald Reagan, "trust, but verify," and, as always, remain vigilant.