GREAT AMERICAN & LOWERS RISK GROUP | ISSUE #43 | NOVEMBER 2018

# FIDELITY/ CRIME OBSERVER

# ELEMENT OF SURPRISE

## TABLE OF CONTENTS

## HOW TO CUT FRAUD DETECTION TIME IN HALF

When it comes to occupational fraud, the total loss an organization suffers is correlated with the length of time from when the fraud begins to the time it is detected. This is true for all types and circumstances of fraud even though some types lead to greater total losses, e.g., petty larceny vs. financial statement fraud. The Association of Certified Fraud Examiners' (ACFE) 2018 Report to the Nations finds that frauds that are not detected in 60 months are 20 times as costly as those detected within the first six months.

Therefore, there is substantial value for any policy or procedure that reduces detection time. Overall the most common form of detection is from tips, especially when a safe and easily accessed hotline is provided. Other common forms of active detection are internal controls and routine internal and external audits.

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*

# 7 KEY COMPONENTS OF SUCCESSFUL ITM RISK MITIGATION

Interactive Teller Machines (ITMs) offer new business opportunities to banks, and therefore to CIT carriers. A significant side benefit to the CIT carrier is the chance to take on an even bigger role in cash management in partnerships with banks. But with the larger role comes a larger responsibility to manage the risks that go with a deeper integration into the financial institution.

***Here are 7 key components of a program where CIT carriers evaluate risks and then develop and implement procedures to address them.***

## RISK ASSESSMENTS

The basis for a proactive strategy includes evaluation of the human and physical environments along the path of the ITM servicing crew. Every CIT carrier has to examine its own routes, responsibilities, and capabilities in creating a risk assessment.

## POLICIES & PROCEDURES

The risk mitigation policies a carrier sets up for ATMs may serve as a template for ITM policies, with additional or different elements incorporated as needed. These policies constitute best practices for the specific carrier to manage cash with security.

## INTERNAL AUDITS

The aim of internal audits is to implement a running account of transactions and cash balances at key points in a route to maintain control of the disposition of cash. In all cases, the policy should be communicated to affected staff to set expectations that the audits will occur.

## EXTERNAL AUDITS

Audits performed by external agencies give a strong, credible check on internal procedures, adding a strong layer of security. The value of an external audit is that it can find failures in the system where employees and/or accomplices have intentionally voided internal controls.

## PERSONNEL SCREENING AND TESTING

Working in CIT imposes demands on an employee's character and capabilities that are above and beyond most jobs, so screening has to be thorough enough to weed out applicants who are unfit. Employees on the front line have to be able to cope with threats appropriately as they arise. Selection and training help identify employees who can handle the threats.

## ACCESS CONTROLS

Access controls including keys, passwords, combinations and alarms should be monitored for operational effectiveness, and changed often enough to reduce the possibility of being defeated.

## PHYSICAL SECURITY

Hardening a target to protect physical security is a classical response to risk. However, it is in the spaces between these hardened targets, where cash is carried that a clever larcenist will look to find weakness. The ITM can exacerbate these weaknesses because of its relatively long service interval, putting a premium on how surveillance, environmental design, and communication can be used to supplement the physical security of the ITM.

For a more comprehensive introduction to managing risk in ITM servicing, download our latest whitepaper on the topic, A CIT Carrier's Guide to Building Your ITM Program.

# EXPENSE ACCOUNT FRAUD CAN ADD UP

*By: Tom Maloney*
*Vice President, Crime Claims*
*Great American Insurance Group*

Expense account fraud can be one of those easily overlooked schemes employees use to steal. It can be in the form of simple padding here and there, to more extensive abuse. It can be perpetrated by all types of employees, from the office assistant to upper management. Some do it out of a feeling of entitlement ('they should pay me more for all that I do for the company') or may rationalize 'it's only a few dollars and not a big deal'. Either way, the losses add up. Here are a few ways expense account fraud works.

Many companies have a monetary cut-off for receipts. Any expense below $25 does not require a receipt. Some employees earn "pocket" money off of phony meals, tolls, parking, supplies etc. It might not sound like a big deal, but over time it can become a big deal.

Taxi expense fraud is another easy way for fraudsters to cheat on an expense account. Let's say an employee travels for business. After landing at an airport he hops in a cab. When he gets to his destination, he pays the $35 fare in cash and asks for a receipt. The cabbie hands him a couple of blank receipts. When he submits his expense report, the cost of the taxi gets inflated to $60.

Let's say his trip was to Cleveland. He always wanted to visit the Rock and Roll Hall of Fame. During some down time, he had a great time exploring the museum and even purchased gifts for his wife and kids, all at the company's expense. How? When he returned to work, he submitted the other blank taxi receipts (now fraudulently filled in) for rides he never took.

There is also the scheme of airline ticket exchange. An employee books a flight with a major airline for a $750 round trip ticket. He prints the confirmation showing it was paid, then cancels the booking before any penalties are assessed. He rebooks the same flight on a discount airline for $250, yet submits the original cost on his expense report, netting himself $500.

Four colleagues who have not seen each other for a while meet up at a conference. They have a great time catching up over dinner and drinks at a celebrity chef's restaurant. When the bill comes, they each chip in an equal share. The total cost of the dinner with tip was $360. They each submitted for a reimbursement for the full amount on their expense report, even though they only spent $90.

Reimbursement for mileage on a personal vehicle is another method. An employee uses his personal car for business trips. The company reimburses him fifty cents per mile. One trip was 240 miles to attend an out of state meeting. On his expense report, he claims he drove 400 miles. It's only $80 this time, but the employee pads the mileage every trip he takes, costing the company thousands of dollars per year.

One employee used expense reports to support her catering business she has on weekends. What she claimed as equipment and supplies for the office, were actually items she used for her business.

Some jobs entail entertaining clients. An employee submitted receipts for professional sporting events and restaurants claiming he took clients out. In reality, he attended the events with old friends. The dinners he claimed were with clients, were actually with his spouse.

Lastly, some busy executives give access to their company credit card to their assistants as a convenience. The assistants can also be the ones who complete the expense reports without the boss ever seeing it. One assistant took advantage of this situation to use the card for personal expenses. She regularly used the card to shop on-line, ordering clothes, jewelry and other items. She was the one who opened the monthly statements, so the boss never saw what was being charged.

Employees can get away with abusing an expense account for several reasons. First, employees who embezzle, whether by expense account fraud or other schemes, are usually highly trusted employees. Supervisors generally don't expect them to steal so therefore, don't ask questions.

Many companies do not take the time to scrutinize the expense reports, particularly if they use a manual system. Those charged with reviewing paper reports may cut corners and not drill down to look at the details.

There are software programs that can produce invoices. Word processors and laser printers make it easier for employees to fabricate authentic looking invoices or credit card statements.

The "super star" salesman may not get the same scrutiny as others. As long as he brings in the business, some bosses will look the other way. It's not until his numbers drop, and they look more closely only to find he's been abusing his expense account.

Some managers may ignore red flags such as an employee who is months behind in processing his expense report. If someone is behind every once in a while it's no big deal. However, if the person is always months behind, the reason could be he's scrambling to cover his tracks on personal or fraudulent charges.

Companies need to be vigilant to ward off these schemes. Those charged with approving expense reports need to look closely at statements and receipts. A lot of times a fabricated credit card statement may seem ok, but after closer examination flaws can be detected revealing the fraud.

Instead of having employees charge expenses to personal credit cards, issue corporate cards. This way, the company will have access to the statements and won't have to rely on copies supplied by the employee. Copies can be altered.

Company credit cards can also reduce the cash expense out lay. For example, taxi cabs will now accept payment with a card. There is no longer a need to pay cash.

If possible, utilize the services of a designated travel agency. A company-wide on-line portal for booking travel can help.

When you look at the different schemes above, you may think it's only a hundred dollars here and there. Keep in mind that if an employee is someone who thinks it ok to submit bogus taxi receipts, he is probably inclined to engage in other fraudulent expense schemes as well. Over time, it could cost a company more than six figures.

# LATIN AMERICAN BANKS ARE FEELING THE IMPACT OF THE CYBERCRIME WAVE

In a [2018 study of cybercrime](#) by the Organization of American States (OAS), 92% of banks in the study reported some kind of digital security event and more than 1 in 3 banks reported falling victim to at least one successful attack.

The OAS report uses two kinds of data: on the behavior of banks, and on a sample of their customers. Regarding the banks, there are 3 top level results to frame the more detailed data:

- Cyber-attacks are ubiquitous. 92% of banks in the study reported some kind of digital security event, including both successful and unsuccessful attacks (65% of large banks reported successful attacks). If you are a banker, you've been hacked.
- Most banks, by a narrow margin, do NOT use advanced detection tools and controls based on big data or artificial intelligence. This problem is more severe for smaller banks, of course, but it exists across the system.
- Cyber-attacks work, and they are costly. The average cost of an attack in Latin America was US $1.9 million, with a region-wide loss in 2017 of US $809 million.

From the customer/users' point of view, digital services are desirable and widely utilized. This is reflected in the fact that customers are increasingly using the super-convenient smartphone as a banking platform.

- A large majority of customers,88%,use one or more digital service, and the percentages of various services are increasing. Of those who did not, 59% cited distrust of the digital environment as the reason.
- Customers are the weaker link in the chain. Though most of them understand the general threat and some of the methods of cyber-attacks, they do not use sophisticated methods to thwart them.
- 27% of customers had suffered some kind of attack, with 47% of these reporting a financial loss. About 70% of these were fully or partially compensated (at a loss to the bank or insurer). People who were attacked also reported reduced affect for the banks (reputational loss).
- Incident reporting was very low. Customers reported that their banks did not have visible reporting mechanisms, and few reported losses to the authorities.

From the detailed OAS report, a few lessons emerge. First, the digital security risks that warrant the most attention from banking entities are theft of a critical database; compromise of privileged user credentials; and data loss.

Second, defensive systems used by both the financial institution and its customers are probably behind the curve. Hackers on the other hand, are persistent and aggressive. Banks need to step up their efforts to adopt advanced controls and invest continuously in these tools. Banks might also improve efforts to educate customers and install security requirements that help to insulate the system from mistakes of relatively unsophisticated users.

Finally, both banks and customers are committed to the digital future. Customers report that even knowing the threats of digital services, they will not stop using them. Banks continue to adopt ever more digital services to satisfy customers and lower costs. So, the prize for fraudsters and criminals will remain.

# SURPRISE AUDITS ARE SURPRISINGLY EFFECTIVE

Where external audits reduce fraud losses by less than a third, unannounced audits were found to reduce median loss and duration by 51%. When unannounced audits were in effect, median losses dropped from $152k per fraud case to $75k. What's more, the use of unannounced audits was shown to cut the average detection time in half for fraud cases in the ACFE 2018 study. However, while superior in terms of effectiveness, unannounced audits are much less commonly used than external audits. Only 37% of the companies surveyed in the 2018 ACFE report, 'Report to the Nations,' used unannounced audits to detect fraud.

An unannounced audit would typically be performed by an external third party, but it doesn't have to be. The key thing is that it must truly be unanticipated by employees or contractors who have access to assets to prevent them from taking steps to conceal fraudulent activity. An unannounced audit might employ a different and unusual approach compared to routine internal audits as an added precaution to thwart the fraudsters' defensive tactics. Intuitively, an unannounced audit can disrupt fraud more effectively than an audit that is expected.

Unannounced audits can be used in many circumstances. Auditing cash on hand is one of the most important applications, which can cover activities ranging from skimming petty cash to concealing large cash thefts from CIT carriers. Numerous accounting functions like accounts payable and payroll, as well as routines like inventory are vulnerable to frauds that can be detected by unannounced audits.

Like any other audit, unannounced audits have to be planned. The planning will involve identifying the risk points in the system being evaluated and understanding the design of existing internal controls. These factors will be used to create an audit approach leading to reporting and policy revisions as needed.

Read more on *The Element of Surprise* here: [http://blog.lowersrisk.com/surprise-audits-cut-fraud-detection-time-in-half/](http://blog.lowersrisk.com/surprise-audits-cut-fraud-detection-time-in-half/)