STRATEGIC TREASURER
Consultants in Treasury

Insider Fraud: More Prevalent Than You Think

When individuals think of fraud, the image that typically comes to mind is of a dark, shady figure hunched over a computer in a dimly lit room. Often, the corporate viewpoint on fraud is that it originates from obscure parties that operate remotely on the far side of the world. While some fraud does occur in this manner, what many firms might find surprising is that over one-third of fraud originates internally - from either current or former employees. While insider fraud doesn't always receive the media attention that more sophisticated system-level hacks get, it poses a major threat to companies and can result in severe losses if the proper precautions are not taken. In this article, we'll examine four common mistakes made by organizations that have allowed insider fraud to occur, as well as discuss some viable techniques for proactive prevention.

NO FINANCIAL OVERSIGHT

For smaller organizations, too much power given to the treasurer or financial officer, who in some cases is the sole employee responsible for making payments, can easily result in exploitation. This is an issue that has plagued many charities and small public offices, as the treasurer siphons off funds to personal accounts and simply forges or falsifies documents to cover their tracks. Often, it is because no other employees have the knowledge or financial prowess to recognize the signs of fraud that allows perpetrators to avoid discovery. Although some companies may not have the capacity to hire multiple financial professionals, everyone needs oversight and those responsible for initiating funds transfers and other payment activity need accountability. If a single individual is left to chaperone themselves, all it takes is one bad apple to defraud the company.

To protect against this risk, dual controls should be put in place so that all payment activity must pass through at least two individuals (i.e. one employee to initiate a payment and another to approve it). This simple tactic goes a long way in preventing rogue employees from stealing funds and provides much needed oversight for a vitally important business function.

IMPROPER RECONCILIATION CONTROLS

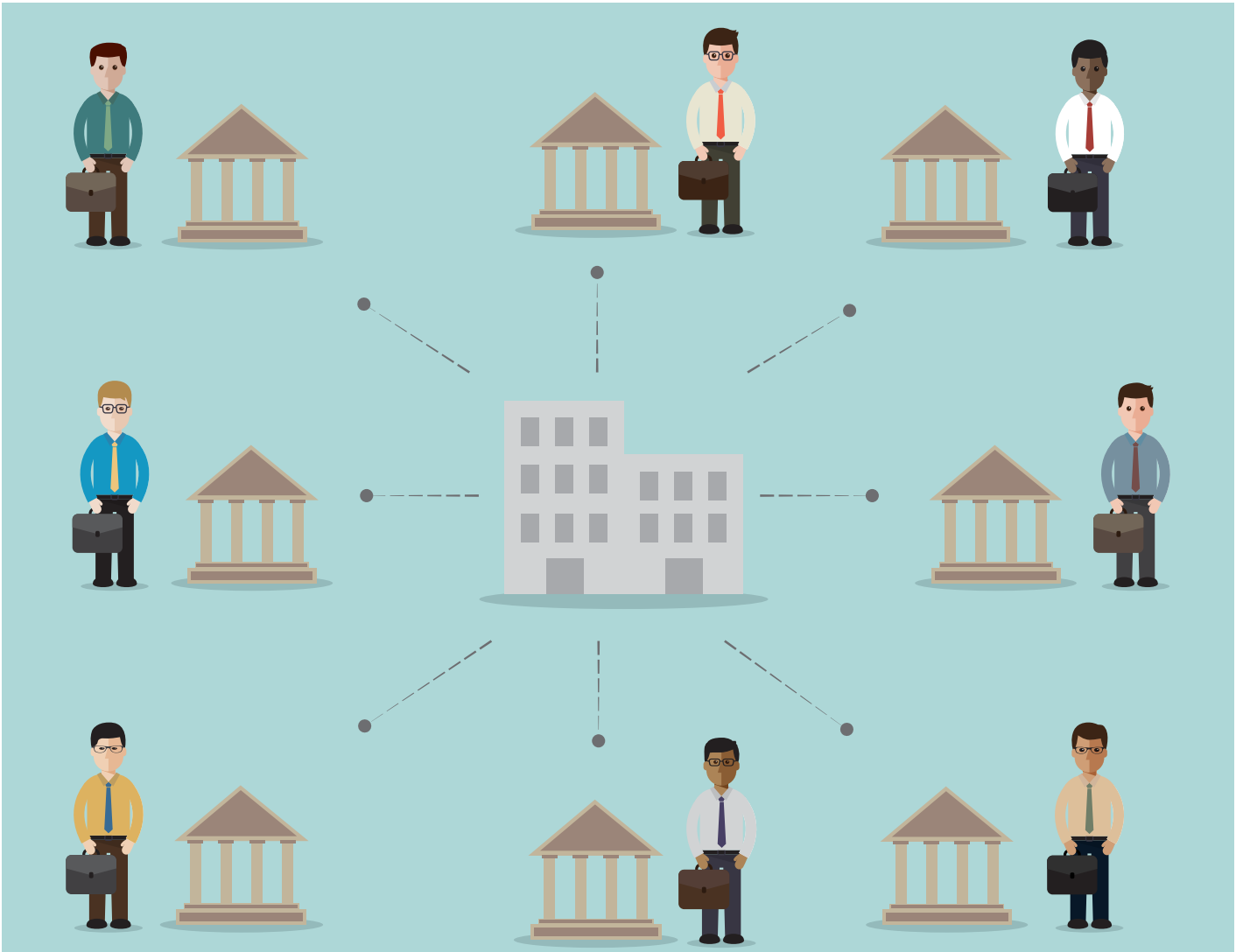
Another obstacle faced by many firms is a lack of proper controls to accurately reconcile accounts. While this can be a problem for companies of all sizes, it particularly affects those that are faced with a heavily manual reconciliation process and that do not have the resources to purchase reconciliation software. Rather than spend large amounts of time reconciling accounts, some companies elect to only partially reconcile their accounts or to only reconcile on a periodic basis. While this might save time, it also opens the door for fraud.

Such was the case for the Kern County School District in Bakersfield, California, who recently lost $19 million dollars in a multi-year fraud scheme that is still under investigation. The problem? Some of their accounts had not been properly reconciled in over 12 years! Had these accounts been reconciled more frequently, the fraudulent transactions being initiated through them would have been caught much sooner.

For rogue employees, knowing that their firm's reconciliation process is lacking may be all the motivation needed to initiate fraud, especially if they know that certain accounts are not reconciled at all. The simple truth is that ALL statements need to be reconciled regularly, preferably by a third party, to verify transaction amounts and destinations. Failing to reconcile even just one account opens the door for fraudulent activity to occur.

INADEQUATE BAM PROTOCOLS

For larger organizations, those operating with a plethora of accounts and multiple signers



For large organizations, it can be difficult to track and manage all bank account information, especially for those operating with numerous bank accounts and multiple signers.

over those accounts need to ensure that their bank account management (BAM) system is updated immediately when a signer leaves the company. This is because outdated signers that are still registered in the system represent a major area of exposure. As was the case at several firms in recent years, employees with access to their company's signer list were able to use the credentials of former employees who were still registered as active signers to initiate and approve fraudulent transactions. In many cases, the perpetrator was an individual in Treasury who did not have the authority to approve wires on their own, but who could use the credentials of former employees to approve the wires they initiated. Since these outdated signer profiles were still listed as valid, the use of their credentials did not trip any security alerts. In some cases, it was even the perpetrator's responsibility to manage the signer list, meaning they could keep old signers active on accounts for as long as they wanted, and there was no second employee to check the activity.

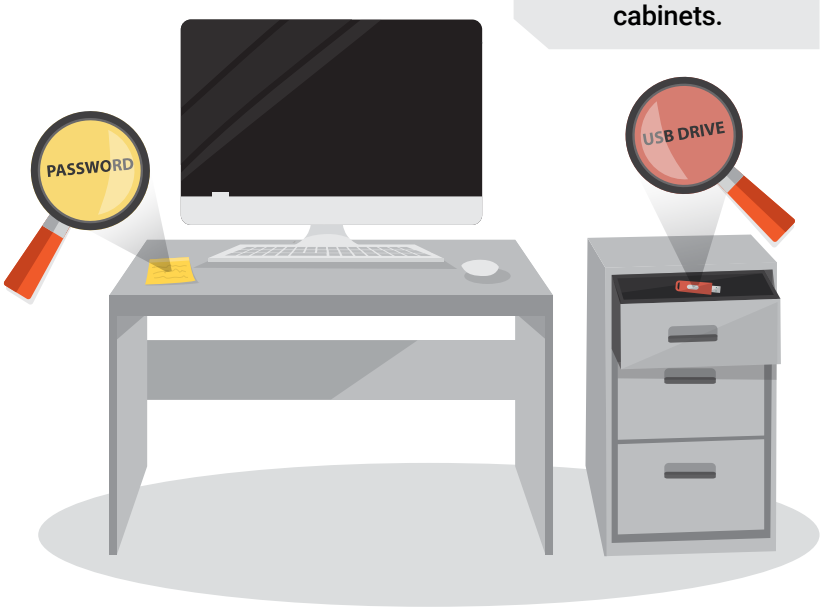
As stated previously, oversight is key and the task of managing and updating signer lists is one that that needs dual controls and clear segregation of duties. The eBAM tools that are available through many TMS platforms today allow for signer credentials and other bank account information to be updated regularly and stored securely. These tools also allow for activity logs to be installed that can track the actions of all users on the system to provide full reporting and audit trails. These audit trails are then managed by an independent administrative team to protect against misuse.

EASILY OBTAINED PASSWORDS

Even if rogue employees don't have the authority to make or initiate payments, they can often figure out the credentials of authorized employees fairly easily. In many cases, it's as easy as looking in their file cabinet, under their keyboard, or in a notebook they have on their desk to locate a piece of paper or a sticky note with usernames and passwords written down. Even if there isn't a password, the USB or key fob used to access the payments system is sitting in a nearby desk drawer. In these cases, it's a naïve and careless mistake that results in fraud.

A password does no good if it is available to everyone; keeping your password information stored in your phone or in a locked file cabinet is a simple, yet vitally important step that can help prevent incidents.

In many cases, an employee's passwords and credentials can be obtained easily by looking through their desk drawers and file cabinets.



FINAL THOUGHTS

While many organizations are aware of the threat that external fraud poses, they are less proactive in protecting against insider fraud, which makes them more susceptible. The bottom line is that insider fraud is occurring regularly against organizations. Furthermore, many of these attacks could be easily prevented through security steps that are regularly overlooked or ignored. To help stave off future attacks, it is imperative that firms:

- Recognize the threat that insider fraud poses;
- Develop a security framework that is just as effective at protecting against insider fraud as external fraud.

For many companies, this may involve allowing an independent team of treasury security experts to perform an assessment of their existing security structure. This process can help identify exposures that were previously unrecognized, and is a crucial step for firms to develop a security framework that addresses all areas of exposure. Once organizations are aware of the exposures they face, they can begin constructing a multi-layered security framework that addresses both internal and external threats and that will better protect them from fraudulent activity in the future.


Over Half of Corporates Experienced Fraud Attacks in 2016
Benefit from our senior consultants' 100+ years of combined corporate treasury experience to guide you in your next treasury security project.
Payment Security Assessments
Treasury Security Processes
Staff Training
Security Benchmarking
Strategic Treasurer
Consultants in Treasury
TREASURY SECURITY

TREASURY RESOURCES

Advise
TREASURY CONSULTING

- Management
- Technology
- Security
- Connectivity

Inform
MARKETING INTELLIGENCE

- Surveys
- Benchmarks
- Webinars
- Reports

ANALYST REPORTS

- Treasury + Risk Management Systems
- Teasury Aggregator

WEBINARS

- Quarterly Treasury Landscape Webinar
- Quarterly Compliance Webinar

SURVEYS

- B2B Payments & Working Capital Management
- Global Payments

EBOOKS + WHITEPAPERS

- Transforming A/P Into Profit Center
- Running Corporate Treasury

ABOUT STRATEGIC TREASURER

Since 2004, Strategic Treasurer has helped hundreds of corporate clients face real world treasury issues. Our team of senior consultants is comprised of former practitioners with actual corporate treasury experience who have "hopped the desk" to support their former peers from the consulting side. Strategic Treasurer consultants are known not only for their expertise in the treasury space, but also for their responsiveness to client issues, thorough follow-through on each project, and general likability as temporary team members of your staff.

Our focus as a firm centers on maintaining true expertise in the treasury space. Through constantly refreshing our knowledge and intentionally learning about leading solutions, we ensure that our understanding is both global in scope and rich in detail.

525 Westpark Drive, Suite 130
Peachtree City, GA 30269
+1 678.466-2220
strategictreasurer.com
info@strategictreasurer.com

STRATEGIC TREASURER
Consultants in Treasury

