Cover & Rossiter
Certified Public Accountants

Skimming and Check Tampering - Don't Let This Happen to You

By: Wendy Rafferty, Cover & Rossiter

There are many ways that employees are able to steal money from the businesses they work for. Cash-theft schemes are typically divided into three categories; skimming, cash larceny, and fraudulent disbursements. This article gives a general overview of these fraud schemes, and offers ways to SPOT them or STOP them before they happen.

Skimming

Skimming, also known as "off the book" fraud, is defined as the theft of cash from a business prior to the cash entries entering the accounting system. This type of theft is very difficult to catch because it does not leave an audit trail; which is why it is so enticing to the fraudster.

Any person who handles the process of receiving cash is in a position to perpetrate a skimming fraud; think salespeople, bank tellers, waitstaff, or employees who manage incoming mail. The most basic form of skimming is when an employee makes a sale of goods or services, but never makes a record of the transaction, and then pockets the money.

Employees whose duties include receiving and logging payments, working in mail rooms where checks are received, or working on remote or off-site locations are most likely to be employees who skim funds. Some cash receivable clerks have implemented complex frauds by manipulating customer payments and receivables by voiding or reversing transactions, or simply never recording a customer's payment and setting up fake bank accounts to deposit customer payments.

The best way to prevent skimming fraud is to maintain an oversight presence at every point where cash enters the business. A person is much less likely to steal if there is a good chance they will get caught.

Here are a few examples of controls you can implement to prevent skimming fraud:

- Separation of duties and internal controls
- Video surveillance
- Signage, in full view of customers, offering discounts if the customer does not receive a receipt
- All cash registers should require a log-in and log-off feature for each user.
- Independent salespeople should be required to keep activity logs accounting for all sales visits that include customer name, address, phone number, time of meeting, *and* those visits should be verified by another department.
- All incoming mail should be opened and processed in an open area free of blind spots

Check Tampering

Check tampering is defined as the conversion of a business's funds either by 1) fraudulently preparing a check from the business bank accounts for their own benefit, or 2) intercepting a check drawn on their employer's bank account that is for the benefit of a third party and converting that check for their own benefit.

Check tampering schemes are different than most frauds because the perpetrator steals a company check and makes it payable to themselves, oftentimes forging a check signature. They are then able to record the check in the accounting system as though it was sent to another vendor. Or, the perpetrator could pay personal bills using company funds, i.e., paying their credit card, cell phone or utility bill through their employer's bank account. This can work fairly readily if the business and employee have the same utility carrier. This fraud often goes unnoticed, especially when the perpetrator has access to the company's check book, signature stamps, and bank statements.

Fraudsters sometimes work with an accomplice, who submits a fraudulent bill for payment, and the employee makes a payment for that bill; the two then split the proceeds.

Another example of check tampering is when there are concealed check schemes, where the perpetrator prepares a fraudulent check and sneaks it into a batch of legitimate checks to be signed; the signer trusts the employee, so checks are signed without thorough review.

Check tampering is often an ongoing fraud that can result in thousands of dollars of theft and continue for years before being detected.

The best way to prevent check tampering is to have separation of duties in place. For example,

- ✓ Assign different employees for entering bills, processing payments, and printing checks. This may not be possible for very small businesses, so it is especially imperative for the business owner to be familiar with all aspects of their business's finances. This includes reviewing all financial reports with their bookkeeper on a regular basis and not assigning check-signing authority to anyone other than themselves.

- ✓ Bank statements should only be opened by owners or managers, and be thoroughly reviewed, including review of cancelled check copies.
- ✓ Checkbooks should be in a locked location, and require 2 people to access.
- ✓ All checks over a certain amount should require 2 signatures.
- ✓ Check signers should always review all checks and the underlying backup for each check before signing.

Please reach out to marketing@coverrossiter.com if you would like a consultation about how to detect and prevent fraud in your organization. If you suspect fraud is occurring in your business, Cover & Rossiter can assist you with the forensic accounting needed to uncover it.

(Note: Information for this article was adapted from the book, Principles of Fraud Examination*, by Joseph T. Wells)*

Wendy Rafferty is a supervisor in Cover & Rossiter's Diverse Accounting Services department at Cover & Rossiter. She is committed to providing expert services to organizations in need of outside assistance with accounting processes and day-to-day compliance. Wendy, a former business owner herself, joined Cover & Rossiter in 2013.