

ON-BOOK VS. OFF-BOOK FRAUD SCHEMES

By Thomas A. Buckhoff, Ph.D., CPA, CFE

(Published on October 10, 2005 in *Savannah Business Report and Journal*)

For obvious reasons, cash is the asset most often stolen by dishonest employees. Fraudsters will steal either the incoming cash receipts or the outgoing cash disbursements via a variety of fraud schemes. When conducting fraud investigations, one must first understand the controls and procedures in place for processing cash flowing through a business. If controls over incoming cash receipts are inadequate and those incoming cash flows are substantial, then dishonest employees will attempt to divert some of that cash flow into their own pockets. If controls over outgoing cash disbursements are inadequate, then dishonest employees will attempt to divert some of those cash disbursements into their own pockets. A thorough understanding of the controls over cash flows allows investigators to generate ideas concerning how someone could steal cash from the organization and not get caught. These ideas, called fraud theories, can be categorized as either *on-book* or *off-book* fraud schemes.

On-Book Fraud Schemes

Cash larceny, an on-book fraud scheme, involves the theft of cash after it has appeared on the victim company's books. For example, a teller stole \$15,000 from the night vault at the bank where she worked. Such schemes are called "on-book" frauds since an examination of the victim company's records could easily reveal the cash shortage. In these cases, the victim company typically knows that a theft has occurred. *On-book frauds* can usually be detected by a thorough examination of the books and underlying source documents of the company and generally fall into one of the following categories:

- Billing schemes
- Payroll schemes
- Expense reimbursement schemes
- Check tampering schemes
- Register disbursement schemes

Off-Book Fraud Schemes

Skimming, an off-book fraud scheme, involves the theft of incoming cash before its entry into the accounting records. Skimming typically occurs when an employee sells goods or services to a customer, collects the customer's payment, but makes no record of the sale. For example, a plastic surgeon pocketed patients' payments for surgeries performed, thereby cheating his employer out of \$200,000 in revenues. Such schemes are called "off-book" frauds since no record of the fraud exists on the victim company's books. In these cases, the victim company generally does not know that a theft has occurred. *Off-book frauds* cannot be detected by examining the books and records of the company and generally fall into one of the following categories:

- Skimming
- Unrecorded sales
- Understated sales and receivables
- Theft of checks through the mail

Case Example

For 12 years "Betsy Smith" managed Northern Exposure, a gentleman's club featuring exotic dancers. A recently-passed local city ordinance outlawed the type of entertainment offered by Northern Exposure. At the club owner's request, Betsy petitioned the city council to exempt any existing businesses from the ordinance. The city council granted the exemption and Northern Exposure was allowed to continue to operate in a 'competition-free' environment. The club generated huge amounts of incoming cash, no credit cards or checks were accepted and an ATM was on site for any customer who needed more cash. The profit potential for the club was enormous, if only the incoming cash could find its way to the bank every day.

"Larry Swenson," the owner of Northern Exposure, was not satisfied with the 10% after-tax profit margins being generated by the club. Given the volume of customers and the lack of competition, Larry thought the club should be earning at least a 35% after-tax profit margin. Consequently, he engaged a certified fraud examiner (CFE) to determine if the club's employees were diverting some of the incoming cash flow. After obtaining an understanding of how cash flowed through the club, the CFE developed the following fraud theories:

1. The employee collecting the \$6 cover charge could either pocket some of the money or allow free admission to friends or acquaintances.
2. Servers and bartenders could get drinks for customers, not ring them into the cash registers, and pocket the entire amount received from customers.
3. The manager could perpetrate any of the schemes available to the employees and could steal part of the deposit.
4. Anyone with access to the cash registers (i.e. servers, bartenders, and the manager) could simply take cash directly from the registers.

Off-book frauds such as theories one and two above are typically called “skimming” schemes and are essentially unrecorded sales. The manager stealing part of the deposit or others taking cash from the cash register would be considered on-book frauds (i.e. cash larceny) since the cash stolen had been rung into the cash register. Consequently, the fraud could be detected by reconciling the cash register tapes to deposits listed on the bank statements. However, in this particular case, cash register printing ribbons were not replaced on a timely basis resulting in illegible cash register tapes.

To test the fraud theories, the CFE employed the following investigative methods: financial statement analysis, undercover surveillance, interviews, and invigilation. The purpose of an invigilation is to establish a baseline for what cash flows ought to be. This was accomplished at Northern Exposure by sending in a team of six investigators who conspicuously monitored the handling and depositing of cash for an entire week. Since the employees knew they were being closely watched during that week, they did not steal. The cash receipts deposited during the invigilation set a record for the most cash the club had ever deposited in one week, which was counterintuitive since the volume of customers that week had been unusually low.

Based on the evidence collected, the CFE estimated that internal theft was costing the club at least \$350,000 per year, or about 25% of total revenues. The undercover surveillance and interviews of employees indicated that about 90% of the club’s employees were stealing, and that the manager, Betsy, was the primary thief. When confronted with the evidence in an interrogation, Betsy admitted she had stolen almost \$100,000 over three years. Larry was shocked when he found out Betsy had been stealing from him. He had trusted her completely. Larry misconstrued her efforts during the petition drive as loyalty to him. Instead, Betsy was

motivated by a selfish desire to protect her own cash flow. The CFE filed an employee dishonesty insurance claim on behalf of Northern Exposure for the maximum coverage amount provided for in their policy, which in this case was \$50,000. As required by the insurance provider, the evidence collected during the fraud examination was turned over to local law enforcement for prosecution.

Summary

Businesses are especially vulnerable to fraud at the points where cash enters or exits the business. Dishonest employees will seek out and exploit weaknesses in internal controls over cash and divert some of that cash flow into their own pockets. Cash intensive businesses can take steps to both detect and prevent fraud schemes involving cash. Despite a lack of direct evidence, off-book fraud schemes—such as the skimming prevalent at Northern Exposure—can be detected and thwarted through various investigative techniques and careful control over the cash flow a business generates.