Fundamentals of Computer and Internet Fraud
II. THE USE OF COMPUTERS IN OCCUPATIONAL FRAUD

Occupational fraud refers to the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets. Simply stated, occupational frauds are those in which an employee, manager, officer, or owner of an organization commits fraud to the detriment of that organization.

This discussion will examine how employees might use technology to commit occupational fraud schemes.

In general, there are three major types of occupational fraud—corruption, asset misappropriation, and fraudulent statements—but an examination of each of the three types is beyond the scope of this material. Instead, this discussion focuses on the most common type of occupational fraud—asset misappropriation.

Following the discussion on asset misappropriation, this chapter examines some common control weaknesses that give rise to this type of fraud.

Asset Misappropriation

Asset misappropriation involves the theft or misuse of company assets. The asset misappropriation schemes to be discussed here are:

- Cash schemes
- Non-cash schemes (inventory and other assets)

According to the ACFE’s 2010 Report to the Nations on Occupational Fraud and Abuse, frauds that target cash are more common than those that target non-cash assets. In fact, approximately 85 percent of all asset misappropriation cases in the study involved the theft or misuse of cash.

Cash Schemes

Cash schemes involve the theft of money in any form (e.g., currency or checks). Some common asset misappropriation schemes involving the theft of cash include:

- False invoicing schemes
- Expense reimbursement schemes
- Payroll schemes
- Skimming schemes
False Invoicing Schemes
False invoicing occurs when an employee generates a false payment by submitting a fraudulent invoice for products and services never delivered or rendered. To carry out these schemes, the fraudster must generate a fictitious invoice, and with the help of computers, there are various ways to do this. For example, an employee might use images downloaded from the Internet, scanners, printers, desktop publishing software, and other computer-based tools to generate false invoices.

A common type of false invoicing scheme involves the use of shell companies—business entities that typically have no physical presence (other than a mailing address), contain no employees, and generate little, if any, independent economic value. Essentially, in these schemes, the fraudster will submit a fraudulent invoice, which is from a nonexistent company, to the victim company for products and services never delivered or rendered.

The growth of technology has made it increasingly easy for employees to create legitimate-looking shell companies. After registering the fictitious entity, an employee can easily obtain a phone and fax number through a VoIP provider, set up a company e-mail account, and establish a website for the nonexistent company. Such activities lend credibility to the shell company and draw attention away from it.

False invoicing schemes are most common where weak controls allow a single employee to approve the requisition, receipt, and payment for goods and services, but through the use of computers, an employee can obtain approval for a fraudulent invoice in a number of ways. For example, the employee might obtain the authority to approve payments by increasing his computer system privileges. Alternatively, an employee might use his supervisor’s stolen account to approve unauthorized payments.

Expense Reimbursement Schemes
Expense reimbursement schemes occur when employees falsify information about their business expenses and cause their employers to overcompensate them in the form of inflated expense reimbursements.

Expense reimbursement schemes can be categorized based on the method employees use to falsify their expense reports and by the nature of the fraudulent expenses. The four most common types of expense reimbursement schemes are:

- **Mischaracterized expenses**: In a mischaracterized expense reimbursement scheme, the perpetrator falsifies an expense report and seeks reimbursement for ineligible personal (non-business) expenses (e.g., claiming reimbursement for expenses incurred on vacation).
- **Overstated expenses**: In overstated expense reimbursement schemes, employees inflate legitimate business expenses to obtain larger cash reimbursements.
The Use of Computers in Occupational Fraud

- **Fictitious expenses**: In fictitious expense reimbursement schemes, fraudsters seek reimbursement for expenses that were never incurred or were paid by others.
- **Multiple reimbursements**: In multiple reimbursement schemes, the perpetrator is reimbursed two or more times for the same expense. That is, the perpetrator seeks multiple reimbursements for a single expense.

Variations of the same technologies that can be used in false invoicing schemes can also be used in expense reimbursement schemes to generate false receipts and obtain approval for a fraudulent expense. Moreover, there are numerous websites that a fraudster can use to generate custom receipts.

**Payroll Schemes**

Like the perpetrators of false invoicing and expense reimbursement schemes, the perpetrators of payroll fraud schemes produce false documents that cause the victim company to unknowingly make a fraudulent disbursement. But in payroll fraud schemes, the fraudster alters payroll records, causing the company to make overpayments in payroll.

The most common payroll frauds involve the use of ghost employees and the falsification or overstatement of reported work hours.

**EXAMPLE**

*John Smith, an employee in the payroll department of ABC Inc., had the authority to enter new employees into ABC’s payroll system, correct payroll information, and distribute paychecks. Because Tim Roberts, Smith’s manager, trusted Smith, he gave rubber-stamp approval to Smith’s actions. The lack of separation of duties and the absence of review allowed Smith to add a ghost employee into ABC’s payroll system.*

**Skimming**

*Skimming* is the theft of cash that has not yet been recorded in the accounting system. Skimming occurs before the cash is recorded as received on the accounting records—thus, it is known as an off-book scheme. The most common places for skimming schemes to occur are in sales and accounts receivable.

**SALES SKIMMING**

The most basic skimming scheme occurs when an employee sells goods or services to a customer and collects the customer’s payment, but makes no record of the sale. The employee simply pockets the money received from the customer instead of turning it over to his employer.
SKIMMING RECEIVABLES
In general, it is more difficult to conceal the skimming of receivables than the skimming of sales because receivables payments are expected. That is, the victim organization knows the payments are due, and it is waiting for the payment to arrive. When receivables are not received, the absence of the payment appears on the books as a delinquent account. Thus, when a customer’s payments are skimmed, that customer’s account becomes delinquent, making the scheme vulnerable to discovery. Moreover, as long as a customer’s payments are being skimmed, his account will continue slipping further and further past due.

Therefore, the perpetrator must take some action to conceal the skimmed receivables. There are a number of techniques fraudsters use to conceal the skimming of receivables, including:

- Forcing account balances
- Lapping
- Stealing or altering account statements
- Destroying transaction data

FORCING ACCOUNT BALANCES
If an employee is in charge of collecting and posting payments, he can falsify records to conceal the theft of receivables payments. For example, the fraudster might post the customer’s payments to their receivables accounts, even though the payments will not be deposited. Although this keeps the receivable from aging, it creates an imbalance in the entity’s cash account.

To address the imbalance, the fraudster may attempt to conceal it by forcing the total on the cash account, overstating it to match the total postings to accounts receivable.

LAPPING
Lapping is a method used to conceal the theft of incoming accounts receivable payments. After the perpetrator skims a customer’s payments, he must take some action to prevent the customer’s account from becoming delinquent. Lapping covers the fraud by crediting the customer’s account with money from some other account. That is, in lapping schemes, the stolen funds are shifted from one customer to another.

EXAMPLE

_XYX Inc. has three customers: A, B, and C. When A makes a payment to XYX, Roger, an employee at XYX, takes it for himself instead of posting it to A’s account. A expects that his account will be credited with the payment he has made, but his payment was stolen. When XYX sends A his next_
statement, A will see that the payment was not applied to his account and will notify XYX. And to avoid this, Roger must take some action to make it appear that A’s payment was posted.

After Roger steals A’s payment, XYX receives B’s payment. And when B’s check arrives, Roger takes the payment and posts it to A’s account. As a result, the payments on A’s account are up-to-date, but B’s account is short.

After Roger posts B’s payment to A’s account, XYX receives a payment from C. And when C’s payment is received, Roger applies it to B’s account. This process continues indefinitely until one of three things happens: (1) someone discovers the scheme, (2) restitution is made to the accounts, or (3) some concealing entry is made to adjust the accounts receivable balances.

A fraudster might be able to use his company’s accounting software to conceal any accounts receivable payments through lapping. For example, he could shift the stolen funds from one customer to another by altering customer account and transaction information in his employer’s database.

Moreover, a computer-savvy fraudster could alter the programming logic behind the report production process, allowing him to conceal evidence of his crime without altering transaction data. He could, for example, perform “manual” general ledger transactions to move money from one account to another while reprogramming report queries to eliminate any manual transactions from appearing on the company’s monthly reports.

STEAL OR ALTER CUSTOMER ACCOUNT STATEMENTS

In some cases, employees who skim receivables let the targeted accounts age rather than attempting to force the balances. This keeps the victim organization’s cash account in balance because the stolen payments are never posted, but the customer’s account will become past due. And if the customer receives notice that his account is past due, the missing payments will likely be discovered. Therefore, the fraudster must keep the customer from realizing that his account was not credited with the payment, and if this is accomplished, the customer will not complain about the missing payment.

To prevent the customer from becoming aware of his account’s status, the perpetrator might steal the customers’ account statements or late notices. Some perpetrators will intercept the customer’s account statements or late notices by changing the customer’s address in the billing system. The fraudsters might have the statements sent to a mailbox they can access. Similarly, some perpetrators will change the customers’ addresses so that the statements become undeliverable, causing the statements to be returned to the perpetrator.
And once the fraudster has intercepted the real statement, he will usually alter it or produce a counterfeit statement to indicate that the customer’s payment was properly posted. This leads the customer to believe that his account is up to date and keeps the customer from complaining about stolen payments.

But even though these methods will keep the customer in the dark about the status of his account, the account is still becoming more and more past due. Therefore, the perpetrator must do something to bring the customer’s account back up to date. He may do this by lapping or making false entries in the victim organization’s accounting system.

DESTROY TRANSACTION RECORDS
Rather than attempt to conceal the skimmed receivables, some perpetrators will simply destroy all of the records that might evidence their illegal actions. Although destroying records en masse will not prevent the victim organization from realizing that it has been the victim of fraud, it might help conceal the perpetrators’ identities.

Non-Cash Schemes
Non-cash schemes involve the theft or misuse of inventory, equipment, supplies, and other physical assets of the victim company. Non-cash frauds are not nearly as common as cash schemes, but they can be just as costly.

**Methods of Stealing Non-Cash Assets**
Some of the most common methods of stealing non-cash assets are:

- Falsified receiving reports
- Fraudulent shipments
- Fraudulent write-offs

FALSIFIED RECEIVING REPORTS
Personnel in charge of receiving incoming shipments may steal delivered goods on arrival. To conceal this type of theft, the fraudster will falsify the receiving report, listing the shipment as “short” or indicating that some goods in the shipment were defective. The fraudster only falsifies the copy of the receiving report that is used to maintain inventory records. He will not falsify the receiving report that is sent to accounts payable; this report will show a complete shipment to ensure that the vendor is paid in full.
FRAUDULENT SHIPMENTS
Employees may also steal non-cash items by creating fraudulent sales orders or shipping documents that direct certain items to be shipped to themselves or an acquaintance. The fraudulent documents represent “sales” to fictitious persons or companies, and they cause the victim company to ship merchandise as if it had been sold. But, in reality, there is no sale.

From the fraudster’s perspective, the problem with creating fake sales orders or shipping documents is that no one will ever pay for the shipped merchandise. As a result, someone at the victim company might try to determine where the items went. To avoid this, the perpetrator may destroy the sales records, after the items are shipped but before an invoice is generated. Alternatively, the perpetrator might do nothing and allow the fraudulent sale to be processed, knowing that it will be written off as a bad debt.

FRAUDULENT WRITE-OFFS
Often, fraudsters will write off inventory and other assets to make the items susceptible to theft. By doing this, the fraudsters remove assets from the books, making them easier to steal. For example, a perpetrator can enter data into his company’s inventory system to show that certain items have been scrapped. Once the items are marked as scrap, the fraudster can remove them.

Theft of Computer Hardware and Software
In addition to using computers to steal non-cash assets, employees may steal computer hardware or software. Under federal law, prosecutors typically prosecute theft of computer hardware under the Interstate Transportation and Receipt of Stolen Property or Goods statute. This statute, which is found in Section 2314 of Title 18, United States Code, regulates interstate transportation of stolen property. But prosecutors can only prosecute the theft of stolen computer software under Section 2314 if the stolen software is located on computer hardware.

Control Weaknesses
Internal controls play an important role in fraud prevention. Although a system of weak internal controls does not mean that fraud exists, it does foster an environment for fraud. Therefore, fraud examiners should understand the effect internal controls have on an organization.

According to most studies, employees represent the largest threat to a company’s computer system. That is, many computer crimes are committed by an insider who has gained knowledge of an organization’s IT system, enabling him to exploit any control weaknesses.
For example, employees often find themselves in positions of extraordinary privilege in relation to their organizations’ key functions and assets. And as a result of such circumstances, these employees are frequently exposed to temptation.

Likewise, management has a tendency to tolerate less stringent supervisory controls over information system personnel in many cases. Often, this occurs because that type of work is highly technical and specialized, and it is difficult for many members of management to understand and control. What’s more, information system personnel are often permitted, and sometimes encouraged, to perform these duties during non-prime shift periods, when demands on computer time are light. And if this occurs, many of the most critical software development and maintenance functions are performed in an unsupervised environment.

As the above examples illustrate, any entity that uses technology in its operations must strive to ensure that its technology is securely managed. That is, organizations must implement adequate administrative, physical, and logical security controls to restrict access by unauthorized users to system data and deter alteration, theft, or physical damage to their information systems.

The following discussion examines a number of recurring internal control weaknesses that give rise to fraud. At a later point, the text will discuss some controls, computer security considerations, and security auditing and testing procedures to help ensure that an entity’s computing assets are safe.

**Internal Control Weaknesses**

Common internal control weaknesses that might expose an organization to losses from computer and Internet fraud include:

- Lack of segregation of duties
- Inadequate policies
- Weak or nonexistent change controls
- Lack of education and awareness
- Lack of independent checks on performance
- Lack of proper authorization and documentation
- Ineffective accounting system

**Lack of Segregation of Duties**

Good internal control demands that no single employee be given too much responsibility. Weaknesses with regard to segregation of duties are often brought about by excessive access privileges granted to
users. Often, to simplify privilege management and to reduce the complexity of access control systems, IT administrators are tempted to grant additional rights to users.

And because any person who has too much access to an entity’s system, its programs, and its live data has the opportunity to perpetrate and conceal fraud, organizations must segregate the duties within the information system functions to prevent fraud. That is, authority and responsibility must be clearly divided among the following functions:

- **Authorization**: Approving transactions and decisions
- **Recording**: Preparing source documents; maintaining journals, ledgers, or other files; preparing reconciliations; and preparing performance reports
- **Custody**: Handling cash; maintaining an inventory; receiving incoming customer checks; and writing checks on the organization’s bank account

If a single person is responsible for more than one of these functions, problems can arise.

**Inadequate Policies**
Companies must establish effective fraud-related information and communication practices, including documentation and dissemination of policies, guidance, and results; opportunities to discuss ethical dilemmas; communication channels; training for personnel; and considerations of the impact and use of technology for fraud deterrence, such as the use of continuous monitoring software.

Moreover, policies should be drafted so that they can adapt to the organization’s technological evolution. Many organizations do not draft their policies to allow for evolution, however, and this causes their policies to become outdated when new technology emerges.

**Weak or Nonexistent Change Controls**
Briefly stated, change control refers to the process used to request, review, specify, plan, approve, and execute changes to an entity’s information technology system. These processes help guarantee that unplanned changes do not occur and that planned changes are successfully administered.

Unsanctioned and untested changes can prove costly. They can introduce errors or software bugs that could lead to fraud and system availability issues.
Lack of Education and Awareness
Education and awareness are at the base of any good information security program. But constraints placed on human and financial resources often lead to inadequate user training, which can lead to errors and other system irregularities.

Therefore, organizations must conduct information technology awareness training, which should be based on each organization’s operations and needs. This can be done as part of employee orientation, or it can be accomplished through memoranda, training programs, and other inter-company communication methods.

Additionally, the training programs should be designed to inform employees about the company’s stance on fraud. They should also inform employees about what kinds of acts and omissions are prohibited by the law and by the organization. The training should be designed to help employees identify and avoid situations that could lead to criminal conduct.

Furthermore, the training should vary among employees. General training, which should be appropriate for the majority of personnel, should include the basics of the system. Conversely, specific training, which should be geared to those employees who are in higher-risk positions, should provide more in-depth information.

Training, however, should not be a one-time event. Simply handing out a copy of the company’s compliance policy at the beginning of an employee’s tenure is insufficient.

Lack of Independent Checks on Performance
Independent checks serve as a deterrent to fraud because people that know their work is being watched are less likely to commit fraud.

Lack of Proper Authorization and Documentation
Proper authorization and documentation is, and has always been, a deterrent to fraud because these processes establish audit trails. And once a system becomes lax, it is opened up to fraud.

Ineffective Accounting System
An effective accounting system will impede fraud because it provides an audit trail for discovery and makes it more difficult for a fraudster to hide his actions. Accounting records consist of documents, journal entries, and approvals, and all of these items can point to a fraudster. With a weak accounting system, however, identifying fraud or determining if a fraud occurred is more difficult.
Control Activities
Companies should establish and implement effective control practices to help deter and prevent fraud. These control practices should include actions taken by management to identify, prevent, and mitigate fraudulent financial reporting or misuse of the organization’s assets. Additionally, they should include safeguards to prevent management from overriding the controls.