

 611

# FRAUD DETECTION TECHNIQUES

Because of the need to falsify accounting records, many fraud schemes leave a trail in the underlying accounting data that the forensic auditor can follow if he or she knows what to look for. For businesses with a large volume of transactions, however, finding the tell­tale trail using manual procedures may be impossible. Computer-based data extraction and analysis tools such as ACL are thus essential. To find the trail in the masses of data, the auditor first develops a “fraud profile” that identifies the data characteristics that one would expect to find in a specific type of fraud scheme. This identification requires an understanding of the enterprise's processes and internal controls (and their weaknesses). Once the fraud profile is developed, ACL can be used to manipulate the organization's data to search for transactions that fit the profile. In this section, we examine the operational and data characteristics

;)

of three common fraud schemes.

*;* /**1) PAYMENTS TO FICTICIOUS VENDORS**

The purchasing function is particularly vulnerable to fraud and, for many organizations,

represents a significant area of risk. A common fraud scheme involves making a pay ment to a fictitious company. A preliminary step in this scheme requires the perpetrator to create a phony vendor organization and establish it in the victim organization's re­ cords as a legitimate supplier. The embezzler then submits invoices from the fake ven­ dor, which are processed by the accounts payable system of the victim company. Depending on the organizational structure and internal controls in place, this type of fraud may require collusion between two or more individuals. For example, the purchas­ ing agent prepares a purchase order for items tl·om the fake vendor, and the receiving clerk prepares a fictitious receiving report for the items. Accounts payable receives these documents, which appear to be legitimate, and matches them to the phony invoice when it arrives. An accounts payable is recorded and payment is subsequently made. In smaller organizations, a single individual with the authority to authorize payments can hatch a simpler version of the scheme. The fraud profile describing the false-vendor scheme and the audit procedures are described next.

## Sequential Invoice Numbers

Since the victim organization is the only recipient of the invoices, the supporting invoices "issued" by the phony vendor may actually be in something close to an unbroken nu­ merical sequence. The audit procedure is to use ACL to *sort* the records of the invoice file by invoice number and vendor number. This will highlight records that possess series characteristics, which can then be retrieved for further review.

612 Chapter 12: Business Ethics, Fraud, and Fraud Detection

## Vendors with Employee Addresses

Rather than rent a P.O. box, the perpetrator may use his or her home address on the invoice. Although it is also possible that an employee's home-based business is a legiti­ mate supplier, this is not likely and should be investigated. The audit procedure is to use ACL to *join* the employee file and the invoice file using the address fields as the common key for both files. Only records that match should be passed to the resulting combined file. These records can then be reviewed further.

## Multiple Companies with the Same Address

To divert attention away from excessive purchases made from the same vendor, a perpe­ trator may create several phony suppliers that share the same mailing address. As an audit safeguard, use ACL's *Duplicates* command to generate a listing of mailing addresses that are common to two or more vendors.

## Invoice Amounts Slightly below the Review Threshold

Many organizations control disbursements by establishing a materiality threshold. A management review and signature is required for all checks that exceed the threshold. Those that fall below the limit are not reviewed. Knowing this, the perpetrator may

..........,\_ falsify payments that fall just under the t.hreshold to ma.'dmize his or her benefit from the

*i :i-* \. fraud. The audit procedure for this situation is to use ACL's expression builder to *create*

a value range around the control threshold. To highlight suspicious activity that warrants

further investigation, sort payments records that fall within this range *by* vendor.

## **2) Payroll Fraud**

:00!15''0,'•1:'

The two common forms of payroll fraud are overpayment of employees and payments to nonexistent employees. The first scheme typically involves inflating the number of hours worked and/or issuing duplicate payroll checks. The second approach involves entering fictitious employees into the payroll system. A supervisor, who then receives the resulting payroll checks, usually perpetrates this type of fraud. A variation on this scheme is to keep a terminated employee on the payroll. Suggested audit procedures for detecting

these frauds are described next

## Test for Excessive Hours Worked

Use ACL's *Expression Builder* to select payroll records that reflect excessive hours worked. The determination of what is excessive will depend on the nature of the organi­ zation and its policies. If moderate overtime is fairly common, then filtering records to identify instances where the hours worked field in in the payroll record is greater than 50 may uncover fraudulent situations. Using this filter to review employee records over time may disclose a pattern of abuse.

## Test for Duplicate Payments

Use ACL's *Duplicates* function to search payroll records for employees with the following characteristics:

* Same employee number, same name, same address, etc. (duplicate payments) e Same name with different mailing addresses

Techniques **613**

* + Same name with different checking accounts
	+ Same name with different Social Security numbers

e Same mailing address with different employee names

Some duplicate records detected in the search will be due to natural phenomena (i.e., unrelated individuals who happen to have the same name):' The results, however, provide the auditor with a basis for further review.

## Test for Non existent Employees

Use ACL's *Join* feature to link the payroll and employee files using Employee Number as the common attribute. The resulting joined file should contain only those records from the payroll file that do not match valid employee records. These records need to be re­ viewed with management.

## **3) LAPPING ACCOUNTS RECEIVABLE**

Lapping was described earlier in the chapter as the theft of a customer's check received in payment on his account The perpetrator then covers the theft in the following period by applying cash received from a second customer to the account of the first. The sim­ plicity of this fraud technique is key to its *success* because it presents a very obscure fraud profile. The only evidence of fraud in the underlying data is in the timing differ­ ence between when payment is received and when it is recorded. Depending on how the organization structures its accounts receivable, this may be difficult to detect. The prob lem is illustrated by comparing *tvvo* common methods of managing accounts receivable.

## The Balance Forward Method

The **balance forward method** is used extensively for consumer accounts. Total sales to cus­ tomers for the period are itemized and billed at the period end. Customers are requi\_red to pay only a minimum amount off the balance. The rest of the balance, plus interest, is carded forward to the next period.

Lapping is ditlicult to detect in this type of system. For example, assume the perpe­ trator embezzles a customer payment of $500. This amount would not be posted to t·he customer's account in the current period, and the balance carried forward to the next period would be overstated by $500. In the following period, cash taken from another customer would be used to cover this amount. Since balances carried forward are com­ monplace, an overstated amount does not draw attention internally. The customer, how­ ever, may complain that the payment was not recorded. If the embezzler himself deals with the complaint, he could explain that the payment was received too late to be reflected on the current statement but would show up in the next period.

## The Open Invoice Method

The **open invoice method** is often used to manage trade accounts receivable (sales to other business organizations). Each invoice is recorded as a separate item in the invoice file. Checks received from customers are usually in payment of individual invoices. Since good credit relations between customer and supplier are critical, payments tend to be on time and in full. Partial payments resulting in balances carried forward are the exception rather than the norm.

To illustrate lapping in this situation, assume that Customer A remits a check for

$1,523.61 in payment of an open invoice for the same amount. The perpetrator pockets the check but does not close the invoice. Therefore, the invoice balance is carried

614 Chapter 12: Business Ethics, Fraud, and Fraud Detection

Sales Invoice File

**Invoice Customer Invoice** Sales Due Closed **Remittance**

Number Number Amount Date Date Date Amount

--------------- ·- ·-·---·- ·-·

77885 23671 2,636.88 02/12/04 02/25/04 03/28/04 1,113.27

forward. In the next period, Customer B remits a check for $2,636.88 in full payment of an open invoice. The embezzler applies $1, 523.61 of this payment to Customer A's open invoice, thus closing it. The remainder ($1,113.27) is applied to Customer B's invoice, which remains open. The balance of $1,523.61 is carried forward into the next period. To go undetected, the perpetrator must actively continue the lapping fraud from period to period. This carry-forward characteristic provides the forensic auditor with a basis for constructing a fraud profile. To illustrate, refer to invoice record structure in Table 12.10.

The Invoice Amount Held in Table 12.10 is the accounts receivable amount due. The

Due Date field is calculated at the time of the sale, and the Closed Date field is entered when the payment is received. The Remittance Amount field reflects the amount of pay­ ment received from the customer.

The audit procedure is as follows: Assuming the organization follows proper backup

procedures, the invoice file will be copied frequently throughout the period under review.', thus producing several archived versions of the file. Collectively, these files reflect the invoice amounts carrled forward from month to month. If the auditor suspects lapping, he or she may employ the following ACL test"

E Use ACL's *expression builder* to select items from each file version whose Remit­ tance Amount field is ·greater than zero and less than the Invoice Amount field. These sets of records may contain legitimate items that are being disputed. by the customers. For example, damaged goods, overcharges, and refused deliveries may re­ sult in customers making only partial payment<>. The auditor will need to sift through these legitimate issues to identify lapping.

* *Aierge* the resulting carry-forward files into a single file reflecting activity for the en­

tire period.

* Create a *calculated\_ eld* of the amount carried forward (Invoice Amount-Remittance Amount).

o Use the *duplicates* command to search the file for calculated carry-forward amounts

That are the same, following the example just illustrated, a carry-forward pattern of

$1,523.61 will emerge.

# SUMMARY

This chapter examined the two closely related subjects of ethics and fraud and their im­ plications for auditing. It began by examining ethical issues that societies have pondered about for centuries. Good ethics is a necessary condition for the long-term profitability of a business. This requires that ethical issues be understood at all levels of the firm, from top management to line workers. In this section, we identified several ethical issues for auditors to consider in their fraud risk assessment.