Concealed Liabilities and Expenses

Understating liabilities and expenses is one of the ways financial statements can be manipulated to make a company appear more profitable than it is. Because pre-tax income will increase by the full amount of the expense or liability not recorded, this financial statement fraud method can significantly affect reported earnings with relatively little effort by the fraudster. It is much easier to commit this scheme than to falsify sales transactions. Missing transactions can also be harder for auditors to detect than improperly recorded ones because the missing transactions leave no audit trail.

There are three common methods for concealing liabilities and expenses:

- Omitting liabilities and/or expenses
- Improperly capitalizing costs rather than expensing them
- Failing to disclose warranty costs and product-return liabilities

Liability/Expense Omissions

The preferred and easiest method of concealing liabilities or expenses is to simply fail to record them. Large monetary judgments against a company from a recent court decision might be conveniently ignored. Vendor invoices might be thrown away or stuffed into drawers rather than posted into the accounts payable system, thereby increasing reported earnings by the full amount of the invoices. In a retail environment, debit memos might be created for chargebacks to vendors, supposedly to claim permitted rebates or allowances, but sometimes solely to create additional income. Whether these items are properly recorded in a subsequent accounting period does not change the fraudulent nature of the current financial statements.

Often, perpetrators of liability and expense omissions believe they can conceal their frauds in future periods. They frequently plan to compensate for their omitted liabilities with visions of other income sources, such as profits from future price increases.

Just as they are easy to conceal, omitted liabilities are probably one of the most difficult schemes to uncover. A thorough review of all post-financial-statement-date transactions, such as accounts payable increases and decreases, can aid in the discovery of omitted liabilities in financial statements, as can a computerized analysis of expense records. Additionally, if the auditor requested and was granted unrestricted access to the client's files, a physical search could turn up concealed invoices and unposted liabilities. Investigative interviews of accounts payable and other personnel can reveal unrecorded or delayed items as well.

Current accounting standards require entities to record provisions for contingent liabilities on their financial statements if a present obligation has arisen as a result of a past event, the amount of the liability can be reasonably estimated, and the likelihood of payment is probable.[1]

EXAMPLE

In July 2002, the U.S. SEC filed suit in the United States District Court for the Southern District of New York, charging major cable television producer Adelphia Communications Corporation ("the Company" or "Adelphia"); its founder John J. Rigas; his three sons, Timothy J. Rigas, Michael J. Rigas, and James P. Rigas; and two senior executives at Adelphia, James R. Brown and Michael C. Mulcahey, in one of the most extensive financial frauds ever to take place at a public company. The SEC charged that Adelphia, at the direction of the individual defendants, (1) fraudulently excluded over $2.3 billion in liabilities from its consolidated financial statements by hiding them in off-balance sheet affiliates; (2) falsified operations statistics and inflated Adelphia's earnings to meet Wall Street's expectations; and (3) concealed rampant self-dealing by the Rigas Family, including the undisclosed use of corporate funds for Rigas Family stock purchases and the acquisition of luxury condominiums in New York and elsewhere.

With respect to the concealed liabilities, the complaint alleged that between mid-1999 and the end of 2001, John J. Rigas, Timothy J. Rigas, Michael J. Rigas, James P. Rigas, and James R. Brown, with the assistance of Michael C. Mulcahey, caused Adelphia to fraudulently exclude from the Company's annual and quarterly consolidated financial statements over $2.3 billion in bank debt by deliberately moving those liabilities onto the books of Adelphia's off-balance sheet, unconsolidated affiliates. Failure to record this debt violated financial reporting requirements and precipitated a series of misrepresentations about those liabilities by Adelphia and the defendants, including the creation of (1) sham transactions backed by fictitious documents to give the false appearance that Adelphia had repaid debts when, in truth, it had simply moved them to unconsolidated Rigas-controlled entities, and (2) misleading financial statements by giving the false impression through the use of footnotes that liabilities listed in the Company's financials included all outstanding bank debt.

[1] Under U.S. GAAP, a company's potential liability must only be disclosed in the notes to the financial statements if it is reasonably possible that a change in an entity's estimate of its probable liability could occur in the near term. Under International Accounting Standard (IAS) 37, *Provisions, Contingent Liabilities and Contingent Assets*, contingent liabilities are disclosed unless the possibility of an outflow of economic benefits is remote.

In November 2002, in exchange for his testimony against the Rigas men, James Brown was released from prosecution by consenting to an entry of a permanent injunction against him for U.S. securities law violations. Additionally, Brown has been permanently barred from becoming an officer or director of a public corporation.

In July 2004, after a three-month trial, a federal jury convicted John and Timothy Rigas of conspiracy, securities fraud, and bank fraud. John Rigas received a 15-year prison sentence and was fined $2,300, and Timothy Rigas was sentenced to 20 years in prison. James Rigas was never criminally charged by the Court. In November 2005, Michael Rigas pleaded guilty to a charge of making a false entry in a financial record.

In April 2005, the SEC filed permanent injunctions against John, Timothy, Michael, and James Rigas, as well as James Brown, Michael Mulcahey, and Adelphia Communications Corporation. The defendants were charged with violating anti-fraud, periodic reporting, recordkeeping, and internal control provisions of U.S. securities laws. In addition, the Rigas family members were barred from ever holding officer or director positions in a public company.

Improperly Capitalized Costs

All organizations incur costs. How to record these costs on the books, however, is not always clear. Suppose ABC Company has a piece of property in need of some repairs. If the work performed simply fixes any problems and brings the property back to its original state, then the costs associated with the repair would appear as an expense on the income statement in the year they were incurred. Net income would be reduced by this amount, and the balance sheet would remain unaffected.

However, suppose work is done that not only repairs but increases the value of the property. Any expenditures made that increase the book value of the property would need to be capitalized. In other words, these costs would be added to the asset value on ABC's balance sheet and then depreciated as an expense over time.

Either way, the costs associated with repairs or improvements are on ABC's income statement as an expense. The difference is in the timing. Capitalizing an expenditure and depreciating it over a number of years makes a significant difference in the bottom line of the financial statements in the year the work was done. Conversely, expensing the same amount of costs in the same year results in a much lower net income that year.

Improperly capitalizing expenses is another way to increase income and assets and make the entity's financial position appear stronger. If ineligible expenditures are capitalized as assets and not expensed during the current period, income will be overstated. As the assets are depreciated, income in following periods will be understated.

EXAMPLE

In November 2002, the U.S. SEC filed an amended complaint against WorldCom, Inc., broadening its charges to allege that WorldCom misled investors from at least as early as 1999 through the first quarter of 2002. The complaint stated that the company had acknowledged that during that period WorldCom materially overstated the income it reported on its financial statements by approximately $9 billion, mainly using two methods. First, WorldCom reduced its operating expenses by improperly releasing as a credit to operating expenses certain provisions previously established for line costs and for taxes. Second, the company improperly reduced its operating expenses by reassigning certain expenses as capital assets. Much of the $9 billion related to improper accounting for "line costs," which were among WorldCom's major operating expenses. The SEC complaint alleges that, in a scheme directed and approved by members of senior management, WorldCom concealed the true extent of its "line costs." By improperly reducing provisions held against "line costs" and by transferring certain "line costs" to its capital asset accounts, WorldCom falsely portrayed itself as a profitable business when it was not and concealed large losses. These improper accounting practices were designed to inflate income to correspond with estimates by Wall Street analysts and to support the price of WorldCom's stock.

In March 2005, former WorldCom chief executive officer (CEO) Bernard Ebbers was convicted of one count of conspiracy, one count of securities fraud, and seven counts of false regulatory filing, and was later sentenced to 25 years in prison. He also agreed to forfeit nearly all of his personal assets to settle a civil suit filed by angry WorldCom investors.

Scott Sullivan, the former CFO under Ebbers and "the architect" behind the fraud scheme, pled guilty to fraud charges and agreed to testify against Ebbers. Due to his cooperation during the investigation, he was sentenced to only five years in prison. He also agreed to forfeit the proceeds from the sale of his $10 million home, along with his investment holdings, to settle the civil suit brought by shareholders.

Former WorldCom Controller David F. Myers and former Director of General Accounting Buford "Buddy" Yates, Jr., pled guilty to criminal charges prosecuted by the U.S. Attorney's

Office for the Southern District of New York. Myers received a sentence of one year and one day in prison. Yates was also sentenced to one year and one day in prison and ordered to pay a $5,000 fine. Additionally, each man was permanently enjoined from acting as an officer or director of any public company and was suspended from practicing before the SEC as an accountant, under Rule 102(2) of the Commission's Rules of Practice.

The SEC also brought civil actions against Betty L. Vinson, certified public accountant (CPA), and Troy M. Normand, former members of the WorldCom General Accounting Department. Both were permanently charged with securities violations. Vinson was suspended from appearing or practicing before the SEC as an accountant. In addition, she pled guilty to one count of securities fraud and one count of conspiracy to commit securities fraud, which led to a sentence of five months in prison and five months of house arrest. Normand pled guilty to similar charges and received three years of probation for his role in the fraud.

EXPENSING CAPITAL EXPENDITURES

Just as capitalizing expenses is improper, so is expensing costs that should be capitalized. The organization might want to minimize its net income due to tax considerations or to increase earnings in future periods. Expensing an item that should be depreciated over a period of time helps to accomplish that—net income is lower and, therefore, so are taxes.

Unrecorded and Undisclosed Warranty Costs and Product-Return Liabilities

Improper recording of warranty and product-return liabilities occurs when a company fails to accrue the proper expenses and related liabilities for potential product returns or warranty repairs. It is inevitable that a certain percentage of products sold will, for one reason or another, be returned.

The accounting treatment for warranties and product-return liabilities differs globally. When products are returned at public companies in the United States, management must record the related expense as a contra-sales account, which reduces the amount of net sales presented on the company's income statement. In countries governed by International Accounting Standards (IAS), management must recognize a provision for the best estimate of the costs of making goods under the warranty products sold before the end of the reporting period. The provision may be estimated based on an analysis of historical data (relation between types of products sold and warranty expenses) or on a subsequent review of quality issues around the reporting date.

Likewise, when a company offers a warranty on product sales, it must estimate the amount of warranty expense it reasonably expects to incur over the warranty period and accrue a liability for that amount. In warranty liability fraud, the warranty liability is usually either omitted altogether or substantially understated. Another similar area is the liability resulting from defective products (product liability).

What Red Flags Are Associated with Concealed Liabilities and Expenses?

The following red flags are indicators of concealed liabilities and expenses schemes:

- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to support
- Nonfinancial management's excessive participation in or preoccupation with the selection of accounting principles or the determination of significant estimates
- Unusual increase in gross margin or margin in excess of industry peers
- Allowances/provisions for sales returns, warranty claims, etc., that are shrinking in percentage terms or are otherwise out of line with industry peers
- Unusual reduction in the number of days' purchases in accounts payable ratio
- Reducing accounts payable while competitors are stretching out payments to vendors

Improper Disclosures

Accounting principles require that financial statements include all the information necessary to prevent a reasonably discerning user of the financial statements from being misled. Clearly, this principle is subject to the professional judgment of the accountants and management preparing the financial statements. Events, transactions, and policy changes that are probable to have a *material impact* on the entity's financial position must be disclosed. The financial statement notes should include narrative disclosures, supporting schedules, and any other information required to avoid misleading potential investors, creditors, or any other users of the financial statements.

Management has an obligation to disclose all significant (material) information appropriately in the financial statements and in management's discussion and analysis (MD&A). In addition, the disclosed information must not be misleading. Improper disclosures resulting in financial statement fraud usually involve the following:

- Contingent liabilities
- Subsequent events

- Management fraud
- Related-party transactions
- Accounting changes

Contingent Liabilities

Typical omissions include the failure to disclose loan covenants or contingent liabilities. Loan covenants are agreements, in addition to or as part of a financing arrangement, that a borrower has promised to keep if the financing is in place. The agreements can contain various types of covenants, including certain financial ratio limits and restrictions on other major financing arrangements. Contingent liabilities are potential obligations that will materialize only if certain events occur in the future. A corporate guarantee of personal loans received by a company officer and potential losses from ongoing litigation are examples of contingent liabilities that must be disclosed. Current accounting standards require entities to disclose contingent liabilities in the notes to the financial statements if it is reasonably possible that an outflow of cash will be required to settle a present obligation in the future.

Subsequent Events

Events occurring or becoming known after the close of the period that could have a significant effect on the entity's financial position must be disclosed. Fraudsters typically avoid disclosing court judgments and regulatory decisions that undermine the reported values of assets, that indicate unrecorded liabilities, or that adversely reflect upon management's integrity. A review of subsequent financial statements, if available, might reveal whether management improperly failed to record a subsequent event that it had knowledge of in the previous financial statements. Public record searches can also help reveal this information.

Management Fraud

Management has an obligation to disclose to the shareholders significant frauds committed by officers, executives, and others in positions of trust. Withholding such information from auditors would constitute lying to auditors, which is an illegal act.

Related-Party Transactions

Related-party transactions are business deals or arrangements between two parties who hold a pre-existing connection prior to the transaction. These transactions generally occur when a company does business with another entity whose management or operating policies can be controlled or significantly influenced by the company or by some other party in common. There is nothing inherently wrong with related-party transactions if they are fully disclosed. If

the transactions are not fully disclosed, the company might injure its shareholders by engaging in economically harmful dealings without their knowledge.

The financial interest that a company official might have might not be readily apparent. For example, common directors of two companies that do business with each other, any corporate general partner and the partnerships with which it does business, and any controlling shareholder of the corporation with which they do business may be related parties. Family relationships can also be considered related parties, such as all direct descendants and ancestors, without regard to financial interests. Related-party transactions are sometimes referred to as self-dealing.

EXAMPLE

In September 2002, the U.S. SEC charged former top executives of Tyco International Ltd., including former CEO L. Dennis Kozlowski, with violating the U.S. securities laws by failing to disclose to shareholders hundreds of millions of dollars of low-interest and interest-free loans they took from the company, and in some cases, never repaid. The SEC complaint, which also charged former Tyco CFO Mark H. Swartz and Chief Legal Officer (CLO) Mark A. Belnick, alleges that the three former executives also sold shares of Tyco stock valued at millions of dollars while their self-dealing remained undisclosed. The complaint alleges numerous improper transactions, such as Kozlowski's use of $242 million of loans for unauthorized purposes that included funding an extravagant lifestyle. With these undisclosed loans, Kozlowski allegedly amassed millions of dollars in fine art, yachts, and estate jewelry, as well as a $31 million Park Avenue apartment and a lavish estate in Nantucket. Kozlowski and Swartz allegedly engaged in undisclosed non-arm's-length real estate transactions with Tyco or its subsidiaries and received undisclosed compensation and perquisites, including forgiveness of multimillion-dollar loans, rent-free use of large New York apartments, and use of corporate aircraft for personal purposes at little or no cost.

In July 2004, Belnick was acquitted of all the charges brought against him. In a separate trial, Kozlowski and Swartz were each found guilty of 22 charges, including grand larceny, falsifying business records, conspiracy, and securities fraud, and were sentenced to eight and one-third to 25 years in prison.

Accounting Changes

In general, three types of accounting changes must be disclosed to avoid misleading the user of financial statements: changes in accounting principles, estimates, and reporting entities.

Although the required treatment for these accounting changes varies for each type and across jurisdictions, they are all susceptible to manipulation. For example, fraudsters might fail to properly restate financial statements retroactively for a change in accounting principle if the change causes the company's financial statements to appear weaker. Likewise, they might fail to disclose significant changes in estimates such as the useful life and estimated salvage values of depreciable assets or the estimates underlying the determination of warranty or other liabilities. They might even secretly change the reporting entity by adding entities owned privately by management or by excluding certain company-owned units to improve reported results.

Backdating Stock Options

As a supplement to salary, companies frequently offer employees stock options, which grant the recipient the privilege to purchase a share of the company's stock at a future date for a specific price called the *strike price*. A strike price is the value of a share at a particular date. Generally, the strike price is set at the price of the underlying stock on the day the option is granted; therefore, the option becomes valuable only with future increases in the stock price.

In this way, companies grant stock options as an incentive for employees to enhance company performance and thus raise the stock price. The practice of backdating stock options, however, gives the employee a chance to profit by purchasing stock at past low prices, providing an immediate payoff. Backdating stock options occurs when a company alters the date of the grant to a time when the stock was trading at a lower price in the interest of making the option instantly valuable and further increasing the employee's gain if the stock price continues to rise.

EXAMPLE

On June 1, 20X1, Company XYZ grants its CEO a stock option that provides the executive the right to purchase one hundred shares of XYZ stock on January 1, 20X2 for the strike price. Per its usual policy, the strike price is set at the price of the company stock on the date of the option grant. On June 1, 2008 (the grant date), XYZ stock was trading at $40 per share. Therefore, if the stock price increases to $45 per share by January 1, 20X2, the CEO could exercise the option and purchase the shares for $40 per share, and then sell them immediately on the market for $45 per share, resulting in a gain of $5 per share. However, the company has recently experienced a dramatic increase in its share price. On May 24, 20X1, the stock was trading for $15 per share. To provide the CEO with an opportunity to exploit this increase in share price, the company chooses to backdate the stock options to make

it appear that they were granted on May 24, 20X1. Because the strike price is set at the price of the stock on the option grant date, the strike price is effectively changed to $15 per share. As a result, the CEO now has the option to buy one hundred shares of XYZ stock on January 1, 20X2 for $15 per share. Thus, the CEO has immediately gained $25 per share (the difference between the stock price on the actual grant date of June 1 and the stated grant date of May 24) based solely on the manipulation of the grant date used.

Backdating is not necessarily illegal but can be if not handled appropriately. To be legal, the practice typically must be explicitly reported to shareholders and the government; failure to do so could constitute securities fraud. To help address the possibility of this type of illegal activity, auditors should assess the information obtained from the audit to determine if there is a need for further audit procedures to test for stock option backdating.

What Red Flags Are Associated with Improper Disclosures?

The following red flags might indicate improper disclosures:

- Domination of management by a single person or small group (in a nonowner-managed business) without compensating controls
- Ineffective board of directors or audit committee oversight over the financial reporting process and internal control
- Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management or the communication of inappropriate values or ethical standards
- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Significant, unusual, or highly complex transactions, especially those close to a period's end that pose difficult questions about substance
- Significant related-party transactions not in the ordinary course of business or with related entities either not audited or audited by a different firm
- Significant bank accounts or subsidiary or branch operations in tax-haven jurisdictions for which there appears to be no clear business justification
- Overly complex organizational structure involving unusual legal entities or managerial lines of authority
- Known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or board members alleging fraud or violations of laws and regulations

- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality
- Formal or informal restrictions on the auditor that inappropriately limit access to people or information, or limit the auditor's ability to communicate effectively with those charged with governance

What Red Flags Are Associated with Financial Statement Fraud in General?

Red flags associated with particular financial statement fraud schemes have been discussed previously. There are many red flags associated with financial statement fraud generally. An extensive list of such red flags can be found in the appendix to both AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*, and International Standard on Auditing (ISA) 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements,* where they are called "fraud risk factors." Some red flags indicate increased vulnerability to financial statement fraud; others indicate a greater likelihood that financial statement fraud has occurred.

Some of the more significant red flags are:

- Domination of management by a single person or small group (in a nonowner-managed business) without compensating controls
- Profitability or trend level expectations of investment analysts, institutional investors, significant creditors, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages
- Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management, or the communication of inappropriate values or ethical standards
- Recurring negative cash flows from operations or an inability to generate positive cash flows from operations while reporting earnings and earnings growth
- Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
- Significant, unusual, or highly complex transactions, especially those close to a period's end that pose difficult questions about substance
- Significant related-party transactions not in the ordinary course of business or with related entities not audited or audited by another firm

- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality
- Formal or informal restrictions on the auditor that inappropriately limit access to people or information, or limit the ability of the auditor to communicate effectively with those charged with governance

Detection of Fraudulent Financial Statement Schemes

To better understand basic accounting concepts and to see how an analysis of accounting records and procedures can reveal a fraud, consider the following example:

EXAMPLE

Jackson Hardware Supply is a medium-sized plumbing and electrical wholesale distributor. On December 31, the balance sheet and income statement were as follows:

Jackson Hardware Supply
Balance Sheet
As of December 31

Assets		**Liabilities and Owners' Equities**	
Cash	$2,427,000	**Liabilities**	
Accounts Receivable	300,000	Accounts Payable	$ 300,000
Inventory	300,000	Salaries Payable	70,000
Supplies	11,000	Rent Payable	50,000
Prepaid Insurance	44,000	Deferred Taxes Payable	438,000
Equipment	440,000	Total Liabilities	858,000
		Owners' Equities	
		Common Stock	$2,000,000
		Retained Earnings	664,000
		Total Owners' Equity	2,664,000
Total Assets	$3,522,000	Total Liabilities and Owners' Equity	$3,522,000

Jackson Hardware Supply
Income Statement
For the Year Ending December 31

Revenues		
Sales Revenue	$3,470,000	
Cost of Goods Sold	(2,100,000)	
Gross Profit from Sales	1,370,000	
Rent Revenue	10,000	
Gross Profit		$1,380,000
General and Administrative Expenses		
Insurance Expense	$4,000	
Salary Expense	220,000	
Supplies Expense	14,000	
Rental Expense	40,000	
Total General and Administrative Expenses		(278,000)
Net Income Before Taxes		1,102,000
Income Taxes		(438,000)
Net Income		$664,000

An anonymous tip was received that the paymaster, a long-time trusted employee, is stealing cash from the company. Lately, he has been seen driving a new luxury car and has taken expensive vacations. The president of the company wants to follow up on the tip and asks the fraud examiner to determine if the paymaster has been stealing. Although there are several ways to proceed with the investigation, the fraud examiner with accounting knowledge decides to first compare this year's total salary expense with last year's balance. He theorizes that if the paymaster is dishonest, he might be concealing the theft in the salaries expense account. Past experience has taught the fraud examiner to look in the most obvious place first.

The fraud examiner notes that the balance of $220,000 in the salary expense account this year is significantly larger than the $180,000 balance last year. He asks the owner if there was an increase in the number of employees and how large across-the-board raises were this year. He discovers that the workforce did not increase and all employees, including the owner, received 10% raises. He recalculates this year's salaries by increasing last year's salaries 10% and determines that the balance in the salary expense account should be approximately $198,000 ($180,000 × 1.10 = $198,000). He now believes that excess salaries went to someone.

The next step is to follow the overstatement in salary expense backward from the income statement through the accounts and journal entries to the source documents—the payroll checks, in this case. He finds that there are 12 checks payable to John Doe, an employee who quit in January of last year. He compares the endorsements on John Doe's checks with those on the paymaster's checks and notices distinct similarities in the signatures. Armed with this evidence, he interviews the paymaster, who confesses that he has stolen $22,000 and concealed the theft by issuing payroll checks to a nonexistent employee, checks that he subsequently endorsed and cashed.

Obviously, this example is relatively simple; but most fraud schemes are simple, especially for a fraud examiner who understands concealment techniques and accounting concepts.

Other detection techniques are available for determining if the paymaster is stealing. These include running a report of all employees who do not elect insurance coverage and other payroll withholdings (withholdings on fictitious employees create additional concealment problems for perpetrators), having someone else distribute the checks, and examining identification numbers of all active employees. Any of these methods might have revealed the false paychecks to John Doe. The approach shows, however, how an understanding of accounting can be invaluable for detecting fraud.

Financial Statement Analysis

Comparative financial statements provide information for current and past accounting periods. Accounts expressed in whole dollar amounts yield a limited amount of information. The conversion of these numbers into ratios or percentages allows the reader of the statements to analyze them based on their relationship to each other; in addition, it allows the reader to compare current performance more readily with past performance. In fraud detection and investigation, the determination of the reasons for relationships and changes in amounts can be important. These determinations are the red flags that point a fraud examiner in the direction of possible fraud. If large enough, a fraudulent misstatement can affect the financial statements in such a way that relationships between the numbers become questionable. Many schemes are detected because the financial statements do not make sense when analyzed closely. Financial statement analysis includes the following:

- Vertical analysis
- Horizontal analysis
- Ratio analysis

Vertical Analysis

Traditionally, there are two methods of percentage analysis of financial statements: horizontal and vertical analysis. *Vertical analysis* is a technique for analyzing the relationships among the items on an income statement, balance sheet, or statement of cash flows during a specific accounting period by expressing components as percentages of a specified base value within the statement being analyzed. This method is often referred to as *common sizing* financial statements because it allows an analyst to compare entities of different sizes more easily. In the vertical analysis of an income statement, total sales are the base value and are assigned 100%. This means that every line item on the income statement is stated as a percentage of total sales. On the balance sheet, total assets are assigned 100% on the asset side and total liabilities and equity are expressed as 100%. In turn, each line item on the balance sheet is stated as a percentage of total assets (or total liabilities and equity). Vertical analysis of a cash flow statement shows each cash inflow or outflow as a percentage of the total cash inflows. Vertical analysis emphasizes the relationship of statement items within each accounting period. These relationships can be used with historical averages to determine statement anomalies.

Horizontal Analysis

Horizontal analysis is a technique for analyzing the percentage change in individual line items on a financial statement from one accounting period to the next. The first period in the analysis is considered the base period, and the changes in the subsequent period are computed as a percentage of the base period. If more than two periods are presented, each period's changes are computed as a percentage of the preceding period. The resulting percentages are then studied in detail. As is the case with vertical analysis, this technique does not work for small, immaterial frauds.

The following is an example of financial statements that are analyzed using both horizontal and vertical analysis:

BALANCE SHEET		*Vertical Analysis*			*Horizontal Analysis*	
	Year One		***Year Two***		***Change***	***%Change***
Assets						
Current Assets						
Cash	45,000	14%	15,000	4%	(30,000)	-67%
Accts Receivable	150,000	45%	200,000	47%	50,000	33%
Inventory	75,000	23%	150,000	35%	75,000	100%
Fixed Assets (net)	60,000	18%	60,000	14%	-	0%
Total	330,000	100%	425,000	100%	95,000	29%
Acc'ts Payable	95,000	29%	215,000	51%	120,000	126%
Long-term Debt	60,000	18%	60,000	14%	-	0%
Stockholder's Equity					-	
Common Stock	25,000	8%	25,000	6%	-	0%
Paid-in Capital	75,000	23%	75,000	18%	-	0%
Retained Earnings	75,000	23%	50,000	12%	(25,000)	-33%
Total	330,000	100%	425,000	100%	95,000	29%

INCOME STATEMENT		*Vertical Analysis*			*Horizontal Analysis*	
	Year One		***Year Two***		***Change***	***%Change***
Net Sales	250,000	100%	450,000	100%	200,000	80%
Cost of Goods Sold	125,000	50%	300,000	67%	175,000	140%
Gross Margin	125,000	50%	150,000	33%	25,000	20%
Operating Expenses						
Selling Expenses	50,000	20%	75,000	17%	25,000	50%
Administrative Expenses	60,000	24%	100,000	22%	40,000	67%
Net Income	15,000	6%	(25,000)	-6%	(40,000)	-267%
Additional Information						
Average Net Receivables	155,000		210,000			
Average Inventory	65,000		130,000			
Average Assets	330,000		425,000			

In the example, we can observe that accounts payable makes up 29% of total liabilities in Year One. Historically, we might find that this account averages slightly over 25% of total liabilities. In Year Two, accounts payable, as a percentage of total liabilities, increased to 51%. Although this increase might be explainable through a correlation with a rise in sales, such a significant increase could also be the starting point of a fraud examination. Source documents should be examined to determine the reason for the rise in this percentage. With this type of examination, fraudulent activity might be detected. The same type of change can be seen as selling expenses decline as a percentage of sales in Year Two from 20% to 17%. Again, this

change might be explainable, but close examination could cause a fraud examiner to uncover fictitious sales because there was not a corresponding increase in selling expenses.

It is important to consider the dollar amount of change as well as the percentage when conducting a horizontal analysis. A 5% change in an account with a very large dollar amount could be much more of a change than a 50% change in an account with much less activity.

In the example, it is obvious that the 80% increase in sales has a much greater corresponding increase in cost of goods sold, which rose 140%. These accounts are often used to hide fraudulent expenses, withdrawals, or other illegal transactions.

Ratio Analysis

Ratio analysis is a means of measuring the relationship between any two different financial statement amounts. The relationship and comparison are the keys to the analysis. Many professionals, including bankers, investors, and business owners, as well as major investment firms, use this method. Ratio analysis allows for internal evaluations using financial statement data. Traditionally, financial statement ratios are compared to an entity's industry averages. The ratios and comparisons can be very useful in detecting red flags for a fraud examination.

If the financial ratios present a significant change from one year to the next or over a period of years, it becomes obvious that there could be a problem. As in all other analyses, specific changes are often explained by changes in the business operations. If a change in specific ratios is detected, the appropriate source accounts should be researched and examined in detail to determine if fraud has occurred. For instance, a significant decrease in a company's current ratio might point to an increase in current liabilities or a reduction in assets, both of which could be used to cover fraud.

In financial statement analysis, each reader of a statement will determine which portions are most important. Like the financial statement analysis discussed previously, the analysis of ratios is limited by its inability to detect fraud on a smaller, immaterial scale. Some of the types of financial ratio comparisons are shown in the following section.

Many of the possible ratios are used in industry-specific situations, but the nine comparisons described here are ratios that might lead to the discovery of fraud. The following calculations are based on the financial statement example presented earlier:

Common Financial Ratios

CURRENT RATIO

$$\frac{Current\ assets}{Current\ liabilities}$$

The current ratio—current assets divided by current liabilities—is one of the most commonly used liquidity ratios in financial statement analysis. This comparison measures a company's ability to meet present obligations from its liquid assets; specifically, the current ratio measures the amount of times current assets would be able to pay back current liabilities.

In detecting fraud, this ratio can be a prime indicator that the accounts involved have been manipulated. Embezzlement will cause the ratio to decrease, and liability concealment will cause a more favorable ratio.

In the case example, the drastic change in the current ratio from Year One (2.84) to Year Two (1.70) should cause a fraud examiner to look at these accounts in more detail. For instance, a check-tampering scheme will usually result in a decrease in cash, a current asset, which will in turn decrease the ratio.

QUICK RATIO

$$\frac{Cash + securities + receivables}{Current\ liabilities}$$

The quick ratio, commonly referred to as the *acid test ratio*, compares quick assets (i.e., those that can be immediately liquidated) to current liabilities. This calculation divides the total of cash, securities, and receivables by current liabilities to yield a measure of a company's ability to meet sudden cash requirements. It is important to note that while the current ratio includes inventory in its current assets, the quick ratio does not. Thus, the quick ratio offers a more conservative view of a company's liquidity because it excludes inventory and other current assets that are more difficult to turn into cash rapidly.

A fraud examiner will analyze the quick ratio for fraud indicators. In Year One of the example, the company balance sheet reflects a quick ratio of 2.05. This ratio drops to 1.00 in Year Two. In this situation, a closer review of accounts receivable shows it is increasing at an unusual rate, which could indicate that fictitious accounts receivable have been added to

inflate sales. Of more concern, perhaps, is the increase in accounts payable, which at a minimum might require a closer review to determine why this increase took place.

ACCOUNTS RECEIVABLE TURNOVER

$$\frac{Net\ sales\ on\ account}{Average\ net\ receivables}$$

Accounts receivable turnover is defined as net sales on account—total sales on account less cost of returns, allowances, and discounts—divided by average net receivables. It measures the number of times accounts receivable is turned over during the accounting period. In other words, it measures a firm's effectiveness in extending credit and in collecting debts on that credit. This ratio is one that uses both income statement and balance sheet accounts in its analysis. If the fraud includes fictitious sales, this fraudulent income will never be collected. As a result, the turnover of receivables will decrease.

COLLECTION RATIO

$$\frac{365}{Receivable\ turnover}$$

Accounts receivable aging is measured by the collection ratio. It divides 365 days by the receivable turnover ratio to arrive at the average number of days it takes to collect receivables. In general, the lower the collection ratio, the faster receivables are collected. A fraud examiner might use this ratio as a first step in detecting fictitious receivables or larceny and skimming schemes. Normally, this ratio will stay consistent from year to year, but changes in billing policies or collection efforts could cause a fluctuation. The example shows a favorable reduction in the collection ratio from 226.3 in Year One to 170.33 in Year Two. This means that the company is collecting its receivables more quickly in Year Two than in Year One.

INVENTORY TURNOVER

$$\frac{Cost\ of\ goods\ sold}{Average\ inventory}$$

The relationship between a company's cost of goods sold and average inventory is shown through the inventory turnover ratio. This ratio measures the number of times inventory is sold during the period. This ratio is a good determinant of purchasing, production, and sales

efficiency. In general, a higher inventory turnover ratio is considered more favorable. For example, if cost of goods sold has increased due to theft of inventory (ending inventory has declined, but not through sales), then this ratio will be abnormally high. In the case example, inventory turnover increases in Year Two, signaling the possibility that an embezzlement is buried in the inventory account. A fraud examiner should investigate the changes in the ratio's components to determine where to look for possible fraud.

AVERAGE NUMBER OF DAYS INVENTORY IS IN STOCK

$$\frac{365}{Inventory\ turnover}$$

The average number of days inventory is in stock ratio is a restatement of the inventory turnover ratio expressed in days. This rate is important for several reasons. An increase in the number of days that inventory stays in stock causes additional expenses, including storage costs, risk of inventory obsolescence, and market price reductions, as well as interest and other expenses incurred due to tying up funds in inventory stock. Inconsistency or significant variance in this ratio is a red flag for fraud investigators. Fraud examiners might use this ratio to examine inventory accounts for possible larceny schemes. Purchasing and receiving inventory schemes can affect the ratio. Understating the cost of goods sold will result in an increase in the ratio as well. Significant changes in the inventory turnover ratio are good indicators of possible fraudulent inventory activity.

DEBT-TO-EQUITY RATIO

$$\frac{Total\ liabilities}{Total\ equity}$$

The debt-to-equity ratio is computed by dividing total liabilities by total equity. This financial leverage ratio is one that is heavily considered by lending institutions. It provides a better understanding of the relative risk assumed by the creditors and owners. The higher the ratio, the more difficult it will be for the owners to raise capital by increasing long-term debt. Debt-to-equity requirements are often included as borrowing covenants in corporate lending agreements. The example displays a very favorable Year One ratio of 0.89. Year Two, however, shows a ratio of 1.84, which indicates that debt is greatly increasing. In this case, the

increase in the ratio corresponds with the rise in accounts payable. Sudden changes in this ratio might signal a fraud examiner to look for fraud.

PROFIT MARGIN

$$\frac{Net\ income}{Net\ sales}$$

The profit margin ratio is defined as net income divided by net sales. This ratio is often referred to as the efficiency ratio in that it reveals profits earned per dollar of sales. This percentage of net income to sales relates not only the effects of gross margin changes, but also changes to sales and administrative expenses. As fraud is committed, net income will be artificially overstated, and the profit margin ratio will be abnormally high. False expenses and fraudulent disbursements will cause an increase in expenses and a decrease in the profit margin ratio. Over time, this ratio should be fairly consistent.

ASSET TURNOVER

$$\frac{Net\ sales}{Average\ total\ assets}$$

The asset turnover ratio is used to determine the efficiency with which assets are used during the period. The asset turnover ratio is typically calculated by dividing net sales by average total assets (net sales / average total assets). However, average operating assets can also be used as the denominator (net sales / average operating assets). The case example displays a greater use of assets in Year Two than in Year One.

By performing a financial statement analysis, the fraud examiner might be directed toward the direct evidence to resolve an allegation of fraud. After the analysis, the fraud examiner can select statistical samples in the target account and eventually examine the source documents. If an irregularity of overstatement is suspected, the fraud examiner should begin the examination with the financial statements. If, however, an irregularity of understatement is suspected, the fraud examiner should begin the examination with a review of the source documents. This method is especially effective with omission of liabilities, such as litigation, contingent liabilities, leases, and some product warranties.

The asset turnover ratio is one of the more reliable indicators of financial statement fraud. A sudden or continuing decrease in this ratio is often associated with improper capitalization of expenses, which increases the denominator without a corresponding increase in the numerator.

Inflating revenue is the most common form of financial statement fraud, but overstated sales are most often accompanied by inflated assets (e.g., phony accounts receivable). This adds equal amounts to both the numerator and denominator of the total asset turnover, which affects the ratio, but not as strongly as when just a numerator or denominator are affected. Accordingly, increases in the total asset turnover have less of a correlation with overstatement of sales than do decreases with false capitalization of costs.

Tax Return Review

Tax returns are good sources of additional and comparative information on the business's operations. A complete review and comparison to the financial statement could provide information unknown to the lender or disclose unexplained discrepancies. Again, the lack of properly prepared or timely filed tax returns could be a method of delaying by not providing the required information. Most perpetrators of fraud are reluctant to continue the deception and falsify a tax return. Year-after-year extensions and filing of the tax returns on the last possible date could be a ploy to cover up financial statement and tax return differences.

Interviews in Fraudulent Financial Statement Cases

For in-depth interviewing techniques, please refer to the "Interview Theory and Application" chapter in the Investigation section of the *Fraud Examiners Manual.*

Financial statement fraud does not occur in an isolated environment. People in organizations who have both motive and opportunity are the prime candidates to commit fraudulent misstatement. In most situations, two key managers participate actively in the fraud: the chief executive officer (CEO) and the chief financial officer (CFO). Others become involved largely out of necessity. Those who are not directly involved most often are not aware that anything is wrong.

Investigations of financial statement frauds are unique in that they almost always involve interviewing the executive management of the organization. To detect or deter financial statement fraud, it is necessary that top management be interviewed by a competent and

experienced fraud examiner who possesses the ability to solicit honest answers to tough—but vital—questions about whether anyone has tampered with the books.

Interviewing Techniques

Situations in which accountants are tempted to misstate financial statements most often involve pressure connected with financial performance. The following is a fictitious conversation between upper managers of a corporation. The example shows how the pressure to commit financial statement fraud can greatly influence accounting personnel.

> *CFO: (To CEO) "Boss, it looks like we will not have a good year financially. We told the shareholders (or bank) that our earnings would be $4 a share, and it looks like we will be very lucky to even make $3."*
>
> *CEO: "Well, what are we going to do about it? If we miss the earnings projections (or do not get the loan), it will not look good for the company; we will both lose our jobs. We must get those earnings up to where they should be."*
>
> *CFO: "What do you mean?"*
>
> *CEO: "What I mean is that it is your job to bring in the numbers. You are going to have to find a way to get them up. I am sure we can probably make up the difference next year, but for now, you get our earnings/assets/equity up however you have to. All financial statements are essentially estimates, anyhow. So you figure out how to 'estimate' the numbers more in our favor. I do not know how to do it, and I do not want you to tell me, but get it done."*

The CFO must choose to either falsify the records or lose their job. The CFO's actions are very hard to predict. If they decide to falsify the records, chances are that they will need to enlist the aid of accounting and clerical personnel to execute the plan, even if these employees do not know what they are doing. For example, the CFO might tell the chief accountant to book certain receivables and income, which would produce the needed effect—inflating the equity. Such a scheme might only be apparent to the real insiders.

To detect financial statement frauds through interviews, management and key support staff must be interviewed. Fraud examiners and auditors (collectively referred to as "examiners") must consider many important issues when conducting interviews. One important issue examiners should keep in mind is that there is generally no liability in asking questions in

which they have a legitimate interest, no matter how insulting the questions might be to the respondents. Examiners, therefore, have the legal right to be fearless in asking questions if the questions are asked privately and under reasonable circumstances. This legal right does not extend to accusations—only to questions. "Are you still manipulating the records?" is an accusation whereas, "Are you manipulating the records?" is a question. It is important to know the difference and to frame questions accordingly.

Examiners should also be sure to interview only one person at a time. Groups of people should not be interviewed together because members tend to influence each other. The interviews should always be conducted under private conditions, which permit the respondent to answer candidly.

It is important that examiners aim to be nonthreatening in their interview approaches. The less threatening the interviewer appears, the less reluctant the respondent will be to answer questions. An interviewer should not be judgmental or show surprise or disgust; such actions can inhibit the flow of information.

Examiners should warm up respondents thoroughly before asking sensitive questions. It is best to obtain all of the procedural information and information pertaining to internal controls prior to discussing fraud. Fraud should usually be the last thing covered in an interview.

To reduce the possibility of offending respondents, examiners can explain the nature of their interest before asking sensitive questions. For example, an examiner can say, "As you know, as an auditor, I am required to actively look for fraud. This means I must ask you some direct questions about the subject. Do you understand?" Then, after obtaining a positive response, the examiner can proceed to ask questions about fraud. It is best to ask the least difficult questions first.

Another approach examiners can take to make tough interview questions more palatable is to phrase them hypothetically, especially during the beginning of the interview. For example, rather than asking a CFO, "Have you committed fraud?" an examiner can say to the executive, "Suppose someone in the position of CFO decided to increase the financials. How would they do it?" The latter question is far more likely to elicit specific information than the former. Later in the interview, the executive should be asked specifically if they have committed the fraud. The examiner can say something such as, "My professional

responsibilities require me to ask you one particularly sensitive direct question: Have you committed fraud or other illegal acts against the company?" Most respondents will answer "no" to such a question without hesitation, whether they have or not; however, simply asking the question places the examiner in a much more favorable position if attacked professionally for not detecting a fraud.

The Interview

Fraud examiners and auditors should ask questions designed to elicit the most specific information possible in a professional manner.

THE CHIEF EXECUTIVE OFFICER

Generally, the CEO should be interviewed first in any proactive or reactive fraud situation. There are several good reasons for this approach. First, the auditor or fraud examiner must have a thorough understanding with members of management as to what their responsibilities in this area are. Second, it is unwise to conduct sensitive inquiries within any organization without first advising the CEO. If the CEO discovers that the auditor or fraud examiner is making discreet fraud-related inquiries from some other source, the CEO is more likely to misunderstand their objectives and take such inquiries as a personal affront. Third, if there is any significant manipulation of the financial records, the CEO is almost always involved. The fraud-related questions that a fraud examiner or auditor should ask in connection with a regular audit should include the following, at a minimum. Note how the questions are for set-up purposes.

1. *As you know, we are required to assess the risk that material fraud exists in every company, not just yours. This is sort of a sensitive area for everyone, but our professional responsibilities dictate that we address this area. Do you understand? (Wait for an affirmative response before proceeding.)*

2. *Do you have any reason to believe that material fraud is being committed at any level within the organization?*

3. *One trend in fraud is that small frauds are committed by employees with little authority, which means that the largest frauds are usually committed with upper management's knowledge. Do you understand that? (Wait for an affirmative response before proceeding.)*

4. *Because of that, we are required to at least look at the possibility that all CEOs, including you, might commit significant fraud against customers, investors, or shareholders. Do you understand our situation? (Wait for an affirmative response.)*

5. *During this audit (examination), we need to ask direct questions about this subject to you and your staff. As a matter of fact, we will at least discuss the possibility of fraud with every employee we talk with in connection with this audit (examination). Do you have any problem with that? (Wait for a negative response. If the CEO protests, satisfy the objections. If the CEO cannot be satisfied, assess the risk of whether the CEO is attempting to obstruct the audit or examination.)*

6. *First, let's look at your CFO. Can you think of a reason they might have to get back at you or the company by committing fraud?*

7. *Has the CFO ever asked you to approve any financial transaction you thought might be improper or illegal?*

8. *Do you know whether the CFO has any outside business interests that might conflict with their duties here?*

9. *Does the CFO employ any friends or relatives in the company? (Look for possible conflicts or sweetheart deals.)*

10. *What information do you have about the CFO's lifestyle? (Look for expensive homes, cars, items, and habits.)*

11. *What is your general impression of how the CFO gets along with their staff? (Look for abuses of authority or any other reasons that would motivate employees directly below the CFO to participate in fraud.)*

12. *How do you think fraud in your company compares with others in the same industry?*

13. *Of course, I must ask you many of the same questions about yourself. Is there any reason that anyone below you might claim you are committing fraud against the company?*

14. *I must also ask you some personal financial questions. Do you have any problem with this? (Wait for a negative response.)*

15. *Please give me a current estimate of your personal assets, liabilities, income, and expenses. (List.) What percentage of your net worth is tied directly to this company? (Look for highly leveraged individuals whose company holdings are a significant portion of their net worth.)*

16. *Are you currently experiencing any personal financial problems? (Look for lawsuits, liens, judgments, or other indicators.)*

17. *Do you have friends or relatives working for this company? (Look for conflicts of interest.)*

18. *Do you have friends or relatives working for major suppliers or vendors to this company? (Look for conflicts of interest.)*

19. *Do you own any portion of a company that does business with this organization? (Look for conflicts of interest.)*

20. *Hypothetically, if you wanted to increase your company's profits, what would be the easiest way to do it?*

21. *As I said, we will be required to ask many questions of your staff. Is there any reason why someone who works for you would say you are at risk to commit significant fraud against the company or its shareholders?*

22. *This is the last question, and it should be obvious why I have to ask it. Have you committed fraud or other illegal acts against the company? (Do not apologize for asking the question; it is your job to ask.)*

THE CEO'S TOP STAFF

CEOs of corporations, both large and small, are busy individuals. Because they tend to focus on the broad aspects of the business, they rely heavily on their staffs—principally their personal assistants—to take care of details. But personal assistants do not usually become closely tied to the boss without a demonstrated history of loyalty and discretion. In short, making the boss's assistant mad will result in any fraud-related questions being interpreted in the worst possible light, thus making the interview much more difficult.

The key to interviewing the CEO's top staff, therefore, is to approach the interviewing process correctly from the outset. This involves making conversation and asking general questions before moving to more sensitive questions. Start with procedural matters, or some

other non-sensitive topic, and ask the fraud-related questions toward the end of the conversation.

1. *Part of my job as an auditor (fraud examiner) is to assess the risk that the company's books are not materially correct as a result of fraud by employees or management. I have already talked about these issues with your boss. Your boss understands their importance and is aware that, as part of the audit, I will be talking to everyone about the subject to some extent. Do you have any problem with this? (Wait for a negative response.)*

2. *Do you think fraud is a problem for business in general? (Icebreaker.)*

3. *How do you think this company stacks up to others in terms of its employees' and managers' honesty?*

4. *Have you ever heard rumors in the company that someone is committing fraud, especially someone high up in the organization?*

5. *Is the company in any kind of financial trouble that would motivate management to misstate the company's profits?*

6. *Do you think your coworkers are essentially honest?*

7. *Has anyone you work with ever asked you to do something you felt was not legal or ethical?*

8. *How would you handle such a situation? (Solicit information on the company's fraud reporting program.)*

9. *If someone in a position of authority in the company wanted to commit fraud, what would be the easiest way to do it?*

10. *As your auditor, may I ask you to report any instances in the future of anyone asking you to do anything to the books and records that you feel is not right? (Solicit future cooperation.)*

THE CHIEF FINANCIAL OFFICER

In most cases, the CFO is an integral part of any financial statement fraud. As a result, the interview with the CFO should concentrate not only on possible motivations to commit fraud but also on the opportunity to do so. Because most CFOs are accountants, they should more readily understand the interviewer's mission to uncover fraud. This can be good or

bad—good if the CFO is honest and bad if they are not. Among all financial personnel, the CFO is in the best position to know how to manage the books and keep a fraud from being uncovered. As if that were not enough, many CFOs are hired directly from the firms that audit the company. Is there any other person more likely to be at the center of the fraud?

The following are recommended fraud-related questions for a company's CFO.

1. *You now know that audit standards require us to actively assess the risk that material fraud could be affecting the financial statements. We have talked with the CEO, who is fully aware that we will be asking most everyone we speak with about the possibility of fraud or irregularities. You understand this, don't you? (Wait for an affirmative response.)*

2. *Of the accounts on the company's books, which do you suspect might be the most vulnerable to manipulation, and why?*

3. *What kind of history does the company have with fraud in general, including defalcations and employee thefts? (Look for signs of a weak corporate culture.)*

4. *We know that fraud usually exists to some extent—even if it is small—in most companies. How do you think your company compares to others?*

5. *What is your impression of the company's ethics and corporate culture?*

6. *During our assessment of fraud risk in your company, are there any specific areas you would like to discuss with us?*

7. *Is there any reason that anyone in the company might say that management had a motive to misstate the financials?*

8. *Has anyone you work with ever asked you to do anything with the books that you thought was questionable, unethical, or illegal?*

9. *Are you involved in the personal finances of the CEO? If so, is there anything about them that might make you think the CEO is under personal financial pressure?*

10. *Do either the CEO's lifestyle or habits give you any reason to think they might be living beyond their means?*

11. *Has anyone in a position of authority ever asked that you withhold information from the auditors, alter documents, or make fictitious entries in the books and records?*

12. *Is there anything about your own background or finances that would cause someone to suspect that you had a motive for committing fraud?*

13. *Because of your importance as CFO, I must ask you one final question: Have you, yourself, committed fraud or illegal acts against this company? (Remember that you should not apologize.)*

THE ACCOUNTING STAFF

If a CFO orders the commission of financial statement fraud, this executive will likely either be the one to do the actual illegal work or will task staff members with the crime. In some cases, staff members will understand the plan, but in most situations, the employees are told only what they need to know. It is uncommon for a CFO to admit to cooking the books to a lower staff member.

As a result, the fraud examiner generally must complete the audit work before beginning the interviews of the accounting staff. This will allow specific transactions to be discussed with the people who entered them into the company's records. For example, all thorough audits will examine the major journal entries. Frequently, these journal entries will be ordered by the CFO but entered by a staff member. There would generally be no record of the CFO requesting the entry, so this fact must be established through interviews.

Interviews of the accounting staff will allow for sufficient examination of procedures and controls over assets. After these questions are answered, you can generally pursue the line of inquiry suggested previously for the CEO's assistant.

It should be noted that there are similarities and differences in the questions asked of the CEO, the CFO, and their staffs. In the case of the CEO and the CFO, both were specifically asked if they had committed fraud against the company, although in a nice way. The staffers were not asked that specific question.

The reasoning is this: significant financial statement fraud, as previously stated, generally originates with one or both executives. Staffers have less motivation to engage in financial statement fraud and are, therefore, at less risk to do so. They are also less likely to have the financial authority to enter transactions into the books without higher approval.

Thus, absent any specific information to the contrary, asking employees directly if they have committed fraud is less likely to produce information and more likely to offend them. But with the CFO and the CEO, asking the direct question will add measurably to the prevention of fraud. There are few defenses to not asking the question, other than the possibility of embarrassing the executives being audited. And that will, of course, sound rather weak in a court of law where the fraud examiner's professional credibility is in question.

Prevention of Financial Statement Fraud

Prevention and deterrence of financial statement fraud consists of those actions taken to discourage the perpetration of fraud and limit the exposure if fraud does occur. Because financial statements are the responsibility of management, preventing financial statement fraud requires minimizing the pressures, incentives, and opportunities unique to management for manipulating the company's financial position.

Management and the Board of Directors

Financial statements are management's presentation of the financial position of the entity. Setting the ethical tone of the organization is the responsibility of management and the board of directors. As with other types of occupational fraud and abuse, reducing the three factors that contribute to fraud (the Fraud Triangle) as they specifically relate to management and the board can mitigate the risk of financial statement fraud. Reducing existing pressures to commit fraud, removing potential opportunities to commit fraud, and relieving possible rationalizations for committing fraud will greatly aid in the prevention of financial statement fraud.

Reduce the Situational Pressures That Encourage Financial Statement Fraud

The following measures can help reduce situational pressures that might encourage financial statement fraud:

- Avoid setting unachievable financial goals.
- Eliminate external pressures that might tempt accounting personnel to prepare fraudulent financial statements.

- Remove operational obstacles that block effective financial performance, such as working capital restraints, excess production volume, or inventory restraints.
- Establish clear and uniform accounting procedures that do not contain exception clauses.

Reduce the Opportunity to Commit Fraud

Implementing the following measures can help reduce the opportunity to commit fraud:

- Maintain accurate and complete internal accounting records.
- Carefully monitor the business transactions and interpersonal relationships of suppliers, buyers, purchasing agents, sales representatives, and others who interface in the transactions between financial units.
- Establish a physical security system to secure company assets, including finished goods, cash, capital equipment, tools, and other valuable items.
- Segregate duties between employees, ensuring that no single individual has total control of one area.
- Maintain accurate personnel records, including background checks (where permitted by law) on new employees.
- Encourage strong supervisory and leadership relationships within groups to ensure enforcement of accounting procedures.

Reduce the Rationalization of Fraud—Strengthen Employee Personal Integrity

The following measures can help strengthen employee integrity and reduce the rationalization of fraud:

- Managers should set an example by promoting honesty in the accounting area. It is important that management practice what it preaches. Dishonest acts by management, even if they are directed at someone outside of the organization, create a dishonest environment that can spread to other business activities and other employees, both internal and external.
- Honest and dishonest behavior should be defined in company policies. Organizational accounting policies should clear up any ambiguity in accounting procedures.
- The consequences of violating the rules, including the punishment of violators, should be clear.

Internal Auditors

Internal auditors are responsible for helping to deter fraud by examining and evaluating the adequacy and effectiveness of controls, along with the extent of the potential exposure in the various segments of an entity's operations. The internal auditing standards state that the

principal mechanism for deterring fraud is internal control. Primary responsibility for establishing and maintaining internal control rests with management. The Treadway Commission addresses this issue by recommending that internal audit departments or staffs have not only the support of top management, but also the necessary resources available to carry out their mission. The internal auditors' responsibility is to aid management in the deterrence of fraud by evaluating the adequacy and effectiveness of the company's internal control system, as well as the company's potential exposure to fraud, with particular consideration given to the five elements of internal control laid out by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The five elements of internal control are discussed in more detail in the Fraud Prevention and Deterrence section of the *Fraud Examiners Manual.*

External Auditors

External auditors inspect clients' accounting records and independently express an opinion as to whether financial statements are presented fairly in accordance with the applicable accounting standards of the entity, such as generally accepted accounting principles (GAAP) or International Financial Reporting Standards (IFRS). They must assert whether financial statements are free of material misstatement, whether due to error or fraud.

Independence is the foundation of the auditing function. The only way external auditors can uncover and rectify instances of fraud is if they view the financial statements objectively. However, external auditors are not required to uncover all instances of fraud that might be occurring, as this would be a difficult and nearly impossible task.

The responsibilities of the external auditor as they relate to fraud detection are clearly outlined in both the American Institute of Certified Public Accountants (AICPA) Auditing Standard AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*, and the International Standard on Auditing (ISA) 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.* According to this guidance:

> *The auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this [standard] are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement.*

Audited financial statements are examined by a variety of external users, including investors, creditors, and government bodies. These users depend on the integrity of the statements for a variety of decision-making purposes. Therefore, external auditors have a professional obligation to evaluate the financial statements as thoroughly and objectively as possible. Furthermore, if management and the accountants know that external auditors conduct sensible audits, they might be deterred from committing financial statement fraud.

ASSET MISAPPROPRIATION: CASH RECEIPTS

Asset misappropriation is the most common form of occupational fraud. There are three major categories of asset misappropriation schemes. Cash receipts schemes are discussed in this section, fraudulent disbursements of cash are addressed in the next section, and the following section covers schemes involving the theft of inventory and other noncash assets.

Cash is the focal point of most accounting schemes. Cash, both on deposit in banks and on hand at the company's location, can be misappropriated through many different schemes. These schemes can be either on-book or off-book, depending on where they occur.

Cash receipts schemes fall into two categories: *skimming* and *larceny*. The difference in the two types of fraud depends completely on when the cash is stolen. Cash larceny is the theft of money that has *already appeared* on a victim organization's books while skimming is the theft of cash that has *not been recorded* in the accounting system. The way in which an employee extracts the cash might be exactly the same for a cash larceny or skimming scheme.

Skimming

Skimming is the removal of cash from a victim entity prior to its entry in an accounting system. Employees who skim from their companies steal sales or receivables before they are recorded in the company books. Skimming schemes are known as *off-book frauds*, meaning cash is stolen before it is recorded in the victim organization's accounts. This aspect of skimming schemes means they leave no direct audit trail. Because the stolen funds are never recorded, the victim organization might not be aware that the cash was ever received. Consequently, it can be difficult to detect that the cash has been stolen. This is the primary advantage of a skimming scheme to the fraudster.

Skimming can occur at any point where cash enters a business, so almost anyone who handles cash might be able to skim money. This includes salespeople, tellers, waitpersons, and others who receive cash directly from customers.

In addition, many skimming schemes are perpetrated by employees whose duties include receiving and recording payments made by customers through the mail. These employees slip customer payments out of the incoming mail instead of posting the payments to the proper

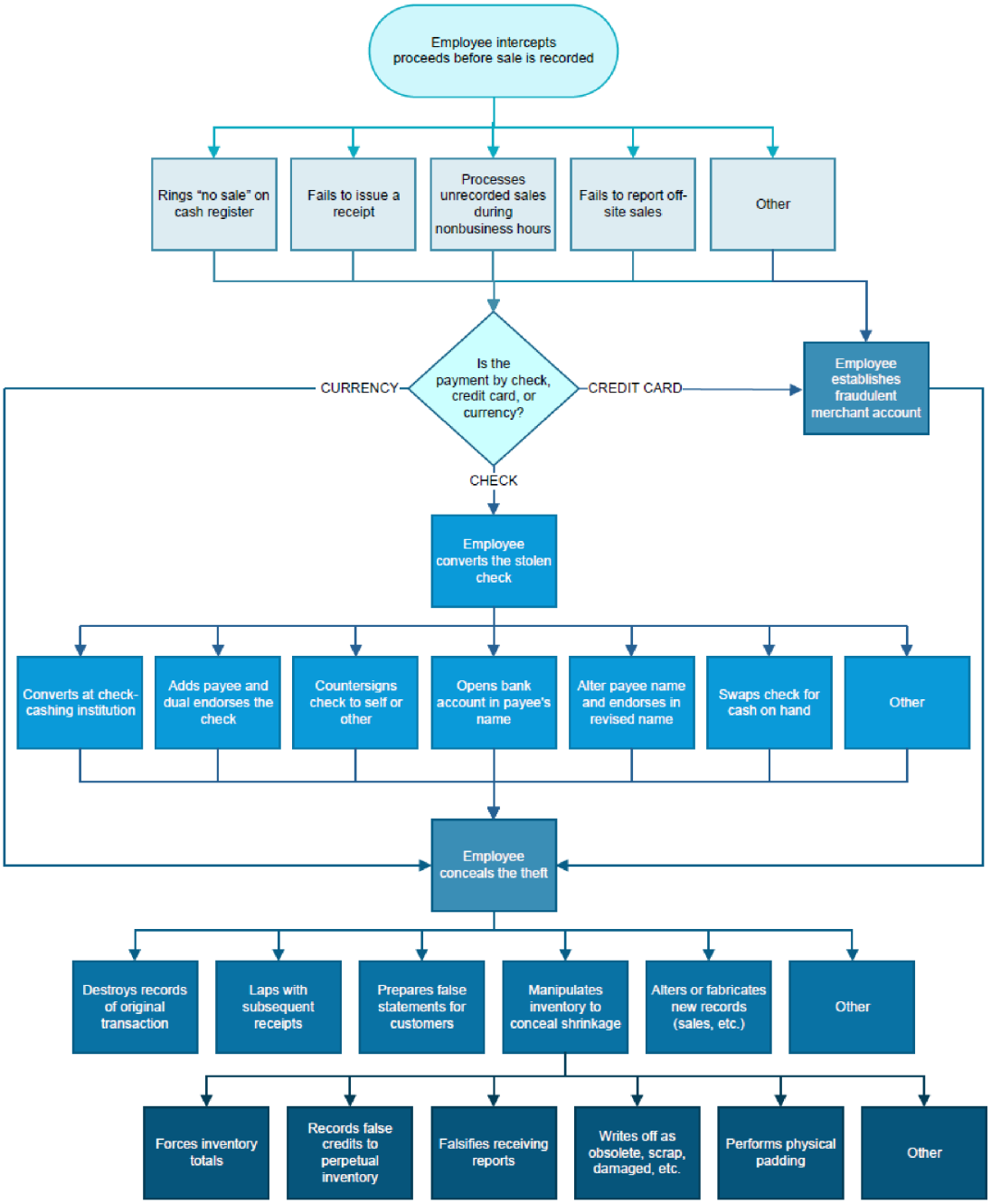
revenue or receivables accounts. Those who work directly with customers or who handle customer payments are the most likely candidates to skim funds.

Sales Skimming

The most basic skimming scheme is an *unrecorded sales scheme*, which 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 keeps the money received from the customer instead of turning it over to their employer. (See the "Unrecorded Sales" flowchart.)

Consider one of the simplest and most common sales transactions: a sale of goods at the cash register. In a normal transaction, a customer purchases an item and an employee enters the sale on the register. The register log reflects that the sale has been made and shows that a certain amount of cash (the purchase price of the item) should have been placed in the register. By comparing the register log to the amount of money on hand, it might be possible to detect thefts. For instance, if there were $500 worth of sales recorded on a particular register on a given day, but only $400 cash in the register, it would be obvious that someone had stolen $100 (assuming no beginning cash balance).

If the employee is skimming money, however, it will be impossible to detect theft by comparing the register log to the cash drawer. Returning to the example in the previous paragraph, assume that an employee wants to steal $100. Throughout the workday, there is $500 worth of sales at their register; one sale is for $100. When the $100 sale is made, the employee does not record the transaction on the register. The customer pays $100 and takes the merchandise home, but the employee keeps the money instead of placing it in the cash drawer. To create the appearance that the sale is being entered in the register, the employee might perform a No-Sale transaction or other noncash transaction. Since the employee did not record the sale, at the end of the day, the register log will only reflect $400 in sales. There will be $400 on hand in the register ($500 in total sales minus the $100 that the employee stole), so the register will balance. Thus, by not recording the sale, the employee is able to steal money without the missing funds appearing on the books. Of course, the theft will show up indirectly in the company's records as inventory shrinkage. But the books will provide no direct evidence of the theft.



Unrecorded Sales

The most difficult part in skimming at the register is that the employee must commit the overt act of taking money. If the employee takes the customer's money and shoves it into their pocket without entering the transaction on the register, the customer will probably suspect that something is wrong and might report the conduct to another employee or a manager. It is also possible that a manager, a fellow employee, or a surveillance camera will spot the illegal conduct. Therefore, it is often desirable for perpetrators to act as though they are properly recording a transaction while they skim sales.

Register Manipulation

Some employees might perform a No-Sale transaction or other noncash transaction to mask the theft of sales. The false transaction is entered on the register so that it appears that a sale is being made. The perpetrator opens the register drawer and pretends to place the cash they received in the drawer, but in reality, they put it in their pocket. To the casual observer, it looks as though the sale is being properly recorded.

Some employees might also manipulate their registers so that a sale can be entered on the register keys but will not appear on the register logs. The employee can then safely skim the sale. Anyone observing the employee will see the sale entered, the register drawer open, etc., yet the register log will not reflect the transaction.

EXAMPLE

A service station employee hid stolen gasoline sales by manipulating the printer on their register. They collected and kept the sales, which were not recorded on the register log. The fraudster would then again manipulate the printer to the point where the next transaction should appear. The next transaction would be printed without leaving any blank space on the tape, apparently leaving no trace of the fraud.

Some enterprising fraudsters might manipulate the register so that a blank space appears on the register log where the skimmed sale should have been printed. Unusual gaps between transactions on a register log might mean that someone is skimming sales.

Fraudsters will often manually roll back the register receipt tape when they replace the ink on their registers so that there is no gap between transactions. Most register transactions, however, are sequentially numbered. If a transaction has been omitted from the register log, the result is a break in the sequence. For instance, if an employee skimmed sale #155, then

the register log would only show transactions #153, #154, #156, #157, and so on. The missing transaction numbers would indicate fraud.

Skimming During Nonbusiness Hours

Another way to skim unrecorded sales is to conduct sales during nonbusiness hours. For instance, some employees will open stores on weekends or before/after hours without the owners' knowledge. They can keep the proceeds of all sales made during these times because the owners have no idea that their stores are even open for business.

EXAMPLE

A manager of a retail facility went to work two hours early every day, opening their store at 8:00 a.m. instead of 10:00 a.m., and kept all the sales made during those two hours. They recorded sales on the register as if it were business as usual but then removed the register log and all the cash they had accumulated. The manager then started from scratch at 10:00 as if the store was just opening. The tape was destroyed so there was no record of the before-hours revenue.

To this point, skimming has been discussed in the context of cash register transactions, but skimming does not have to occur at a register. Some of the costliest skimming schemes are perpetrated by employees who work at remote locations or without close supervision. This can include on-site salespersons who do not deal with registers, independent salespersons who operate off-site, and employees who work at branches or satellite offices. These employees have a high level of autonomy in their jobs, which often translates into poor supervision and, in turn, fraud.

Skimming of Off-Site Sales

Several industries rely on remote salespersons to generate revenue. The fact that these employees are largely unsupervised puts them in a good position to skim revenues. For example, consider the apartment rental industry, where apartment managers handle the day-to-day operations without much oversight. A common scheme is for an on-site employee to identify the tenants who pay in currency and remove them from the books. This causes a particular apartment to appear as vacant on the records when, in fact, it is occupied. The manager can skim the rental payments from the "vacant" unit, and the revenue will never be missed. As long as no one physically checks the apartment, the perpetrator can continue skimming indefinitely.

Another rental-skimming scheme occurs when apartments are rented without a lease being signed. On the books, the apartment will still appear to be vacant even though there are tenants on the premises. The perpetrator can skim the rental payments from these tenants without fear that they will show up as past due in the company records. Sometimes the employees in these schemes work in conjunction with the renters and give them a "special rate." In return, the renters' payments are made directly to the employee and any complaints or maintenance requests are directed only to that employee so the tenant's presence in the apartment remains hidden.

Instead of skimming rent, some property managers focus on less predictable forms of revenue like application fees and late fees. Ownership might know when rent is due and how many apartments are occupied, but often there is no control in place to track the number of people who fill out rental applications or how many tenants pay their rent a day or two late. Property managers can make thousands of dollars by skimming these small payments.

Off-site skimming is by no means limited to the apartment rental industry. The schemes described previously can easily translate into any position where those who generate or collect revenues operate in an independent fashion. A prime example is the insurance agent who sells policies to customers and then neglects to file the policies with the company. Most customers do not want to file claims on a policy, especially early in the term, for fear that their premiums will rise. Knowing this, the agent keeps all documentation on the policies instead of turning it over to the company. The agent is able to skim the customer's payments because the company does not know the policy exists. The customer continues to make payments, thinking that they are insured when in fact the policy is a ruse.

Poor Collection Procedures

Poor collection and recording procedures can make it easy for an employee to skim sales or receivables.

EXAMPLE

A government authority that dealt with public housing was victimized because it failed to itemize daily receipts. This agency received payments from several public housing tenants, but at the end of the day, monies received from tenants were listed as a whole. Receipt numbers were not used to itemize the payments made by tenants, so there was no way to pinpoint which tenant had paid how much. Consequently, the employee in charge of collecting money from tenants was able to skim a portion of their payments. The employee did not record the receipt

of over $10,000. This action caused certain accounts receivable to be overstated where tenant payments were not properly recorded.

Understated Sales

The previous discussion focused on purely off-book sales—those which are never recorded. Understated sales work differently because the transaction in question is posted to the books but for a lower amount than what the perpetrator collected. (See the "Understated Sales" flowchart that follows.) One way that employees commit understated sales schemes is by altering receipts or preparing false receipts that misstate sales amounts.

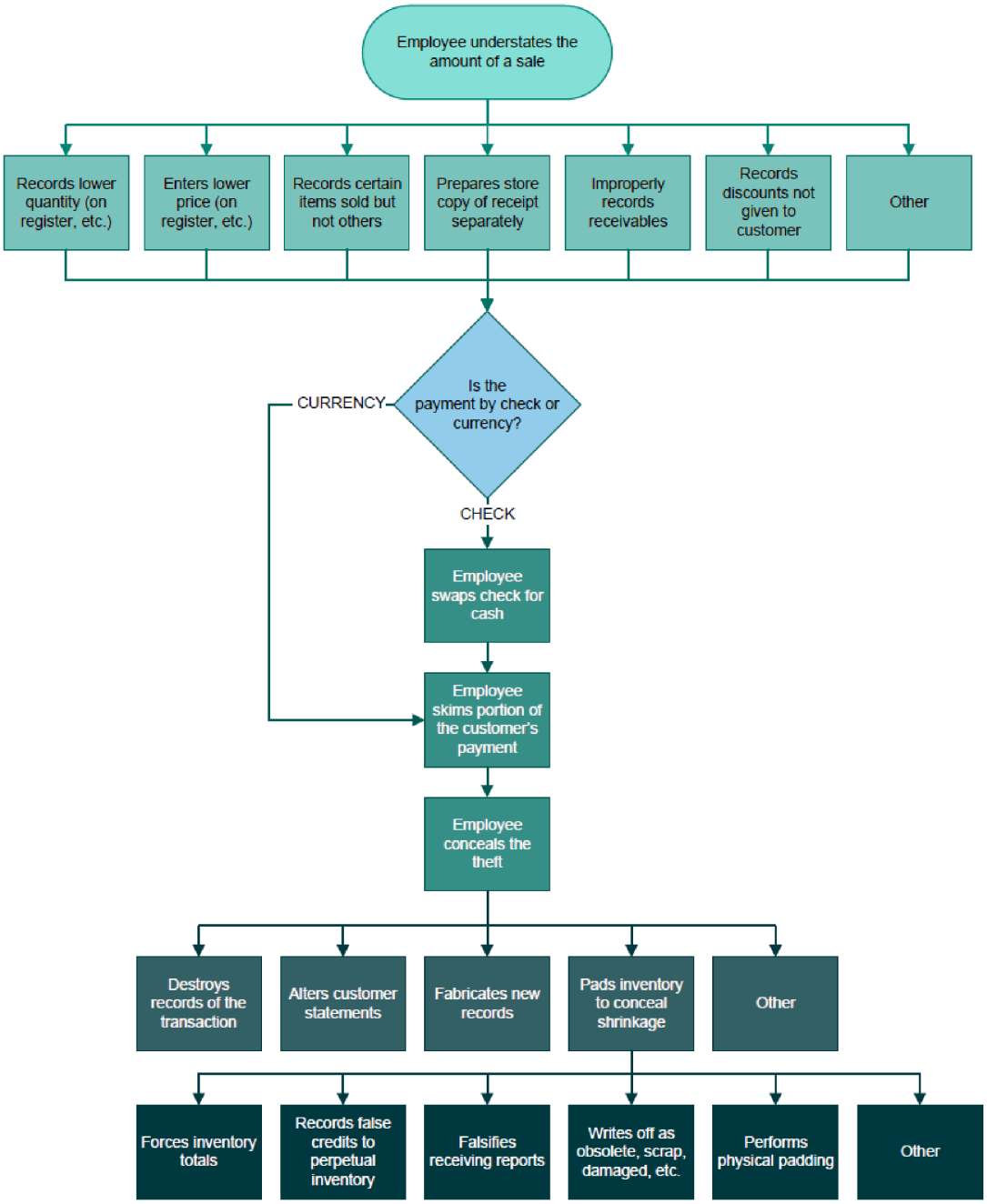
EXAMPLE

An employee wrote receipts to customers for their purchases but removed the carbon paper backing on the receipts so that they did not produce a company copy. The employee then used a pencil to prepare company copies that showed lower purchase prices. For example, if the customer had paid $100, the company copy might reflect a payment of $80. The employee skimmed the difference between the actual amount of revenue and the amount reflected on the fraudulent receipt.

Understated sales schemes are commonly undertaken by employees who work at the cash register. In a typical scheme, an employee enters a sales total that is lower than the amount paid by the customer. The employee skims the difference between the actual purchase price of the item and the sales figure recorded on the register. For instance, if an item is sold for $100, the employee could record the sale of an $80 item and skim the excess $20.

Rather than reduce the price of an item, an employee might record the sale of fewer items. If one hundred units are sold, for instance, an employee might only record the sale of fifty units and skim the excess amount paid for the additional fifty units.

A similar method is used when sales are made on account. The bill to the customer reflects the true amount of the sale, but the receivable is understated in the company books. For instance, a company might be owed $1,000, but the receivable is recorded as $800. (Sales are correspondingly understated by $200.) When the customer makes payment on the account, the employee can skim $200 and post the $800 to the account. The account will appear to have been paid in full.



Understated Sales

FALSE DISCOUNTS

Those employees with the authority to grant discounts might use this authority to skim sales and receivables. In a false discount skimming scheme, an employee accepts full payment for an item but records the transaction as if the customer had been given a discount. The employee skims the amount of the discount. For example, on a $100 purchase, if an employee granted a false discount of 20%, the employee could skim $20 and leave the company's books in balance.

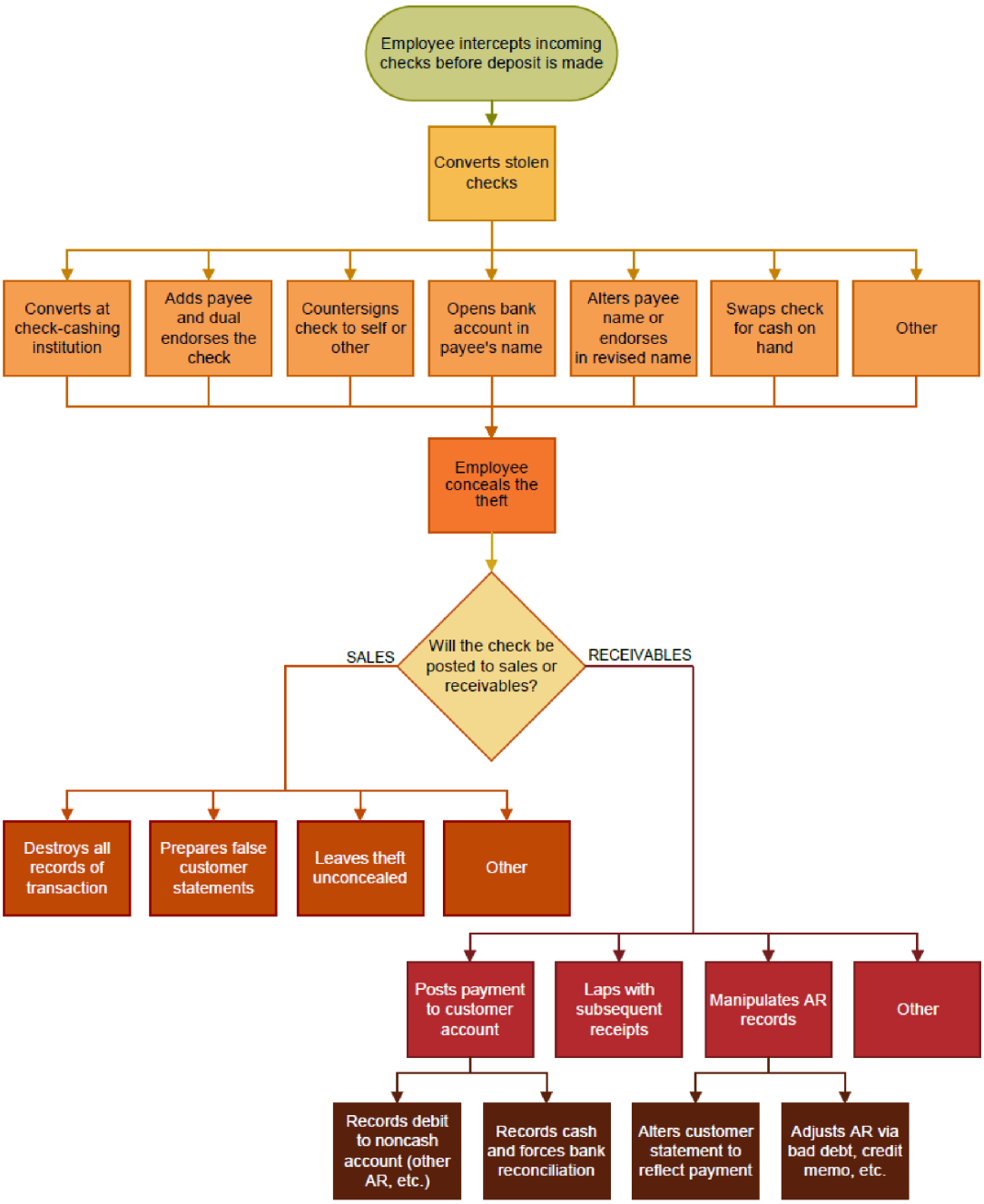
Theft of Checks Received Through the Mail

Checks received through the mail are a frequent target of employees seeking illicit gains. Theft of incoming checks usually occurs when a single employee is in charge of opening the mail and recording the receipt of payments. This employee steals one or more incoming checks instead of posting them to customer accounts. (See the "Theft of Incoming Checks" flowchart that follows.) When the task of receiving and recording incoming payments is left to a single person, it is all too easy for that employee to make off with an occasional check.

EXAMPLE

A mailroom employee stole more than $2 million in government checks that arrived through the mail. This employee identified and removed envelopes delivered from a government agency that was known to send checks to the company. Using a group of accomplices acting under the names of fictitious persons and companies, this individual was able to launder the checks and divide the proceeds with the accomplices.

The theft of checks is not usually complicated, but it is sometimes more difficult to conceal a check theft scheme than other forms of skimming. If the stolen checks were payments on the victim company's receivables, then these payments were *expected.* As receivables become past due, the victim company will send notices of nonpayment to its customers. Customers are likely to complain when they receive a second bill for a payment that they have already made. In addition, the cashed check will serve as evidence that a customer made the payment in question. The methods used to conceal check theft schemes will be discussed later in this section.



Theft of Incoming Checks

Check for Currency Substitutions

A criminal generally prefers to steal currency rather than checks if given the opportunity. The reasons why are obvious. First, currency is harder to trace than a check. A cashed check eventually returns to the person who wrote it and might provide evidence of who cashed it or where it was spent. Endorsements, bank stamps, and so forth might indicate the thief's identity. Currency, on the other hand, disappears into the economy once it is stolen.

The second reason that currency is preferable to a check is the difficulty in converting the check. When currency is stolen, it can be spent immediately. A check, however, must be endorsed and cashed or deposited before the thief can access the money it represents. To avoid this problem, employees who steal unrecorded checks will frequently substitute them for receipted currency. If, for example, an employee skims an incoming check worth $500, the employee can add the check to the day's receipts and remove $500 in currency. The total receipts will match the amount of cash on hand, but payments in currency are replaced by the check.

EXAMPLE

An employee responsible for receipting ticket and fine payments on behalf of a municipality abused their position and stole incoming revenues for nearly two years. When payments in currency were received by this individual, they issued receipts, but when checks were received, they did not issue receipts. The check payments were therefore unrecorded revenues—ripe for skimming. These unrecorded checks were placed in the days' receipts and an equal amount of cash was removed. The receipts matched the amount of money on hand except that payments in currency had been replaced with checks.

The check for currency substitution is very common. While these substitutions make it easier for a crook to convert stolen payments, the problem of concealing the theft remains. The fact that the stolen checks are not posted means that some customers' accounts are in danger of becoming past due. If this happens, the perpetrator's scheme is in danger because these customers will almost surely complain about the misapplication of their payments. However, the misapplied payments can be concealed on the books by forcing account totals, stealing customers' account statements, lapping, and making other fraudulent accounting entries. These concealment techniques will be discussed in more detail in the "Skimming Receivables" section.

Checks for currency substitutions are especially common when an employee has access to some unexpected source of funds, such as a manufacturer's refund that arrives outside the regular stream of sales and receivables payments. In these cases, the check can be swapped for cash and there is usually no additional step required to conceal the crime. The refund check, an unexpected source of funds, will not be missed by the victim organization, and the party who issued the check expects no goods or services in return.

Skimming Receivables

It is generally more difficult to conceal the skimming of receivables than the skimming of sales because receivables payments are *expected*. The victim organization knows the customer owes money and it is waiting for the payment to arrive. When unrecorded sales are skimmed, it is as though the sale never existed. But when receivables are skimmed, the absence of the payment appears on the books as a delinquent account. To conceal a skimmed receivable, a perpetrator must somehow account for the payment that was due to the company but never received. There are several common techniques that fraudsters use to conceal the skimming of receivables.

Forcing Account Balances or Destroying Transaction Records

Among the most dangerous receivables skimming schemes are those in which the perpetrator is in charge of collecting and posting payments. If fraudsters are involved in both ends of the receipting process, they can falsify records to conceal the theft of receivables payments. For example, a fraudster might post the customer's payments to the company's receivables accounts even though the payments will never be deposited. This keeps the receivable from aging, but it creates an imbalance in the cash account. The perpetrator hides the imbalance by forcing the total on the cash account, overstating it to match the total postings to accounts receivable.

EXAMPLE

The chief financial officer (CFO) of a small corporation stole approximately $100,000 from their company by diverting customer checks. This individual controlled all the books and records for the victim company. The CFO stole checks from customers and deposited them in their personal bank account. The customers' payments were still posted to keep the receivables from aging.

The perpetrator stole checks in an amount equal to the victim company's tax liability. To keep the books in balance, they would prepare checks payable to the national tax authority

but would not mail them. The checks were recorded in the victim's records and the false disbursements offset the amount of false postings to accounts receivable. The scheme was uncovered when the government notified the victim company that its taxes were delinquent.

Some fraudsters destroy all records that might prove that they have been stealing. Destroying records does not prevent the victim organization from realizing that it is being robbed, but it might help conceal the thief's identity.

Lapping

Lapping customer payments is one of the most common methods used to conceal receivables skimming. *Lapping* is the crediting of one account through the abstraction of money from another account.

Suppose a company has three customers, A, B, and C. When A's payment is received, the fraudster steals it instead of posting it to A's account. Customer A expects that their account will be credited with the payment they have made. If the payment has not been posted by the time A's next statement is mailed, A will see that the payment was not applied to their account and will almost certainly complain. To avoid this, the thief must take some action to make it appear that the payment was posted.

When B's payment arrives, the thief posts this money to A's account. Payments now appear to be up to date on A's account, but B's account remains unpaid. When C's payment is received, the perpetrator 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.

EXAMPLE

A clerk working for a government agency committed a lapping scheme that involved the theft of more than 150 customer payments, causing a total misappropriation of more than $30,000 in government funds. This individual stole taxes, fees, and other incoming payments from customers to cover personal expenses. When a customer's payment was stolen, the documentation on that payment would be hidden until a later payment was received. The later payment would be applied to the earlier customer's records.

As the rotating schedule of applying and misapplying payments became more and more complicated, the perpetrator insisted on exerting more and more control over the receipting

process. The fraudster insisted on handling all incoming mail, preparing the deposit, and delivering the deposit to the bank so that they could continue to delay the posting of payments. The fraud was detected in large part because several consumers complained that they had not received confirmation of their payments even though their checks had cleared months earlier.

Because lapping schemes can become very intricate, fraudsters sometimes keep a second set of books that detail the true nature of the payments received. In many skimming cases, a search of the fraudster's work area will reveal a set of records tracking the actual payments and how they have been misapplied to conceal the theft. It might seem odd that people would keep records of their illegal activity, but many lapping schemes become extremely complicated as more and more payments are misapplied. The second set of records helps the perpetrator keep track of the funds that were stolen and which accounts need to be credited to conceal the fraud. Uncovering these records, if they exist, will greatly facilitate the investigation of a lapping scheme.

While lapping is more commonly used to conceal receivables skimming, it can also be used to disguise the skimming of sales. Employees sometimes steal all or part of one day's receipts and replace them with the receipts from the following day. This type of concealment requires the employee to delay making the company deposit until enough money can be collected to recoup the stolen funds. If an organization rigidly adheres to a deposit schedule, it is unlikely that lapping will be effective in concealing this type of fraud.

Stolen Statements

When employees skim receivables, they might let the targeted accounts age instead of attempting to force the balances. In other words, they steal an incoming check intended as payment on a receivable, and they act as if the check never arrived. This method keeps the victim organization's cash account in balance because the stolen payment is never posted.

Of course, if the customer's payment is not posted, the receivable will eventually become past due. The customer will have proof in the form of a canceled check that a payment was made on the account. The question will arise: Where did the payment go? The answer, of course, is that a fraudster stole the payment. So the fraudster's goal must be to keep the customer from realizing that their account was not credited with the payment. If this can be accomplished, the customer will not complain about the missing payment, and the victim organization will not realize that skimming has occurred.

One way that fraudsters attempt to conceal the fact that they have skimmed a payment from a customer is to intercept the customer's account statement and/or late notices. In some cases, the perpetrator intercepts the account statement by changing the customer's address in the billing system so that statements are sent directly to the perpetrator's home or to another address where the perpetrator can retrieve them. In other instances, the perpetrator physically intercepts the statements before they are mailed.

Once the real statement indicating that the payment was not received has been intercepted, the fraudster usually alters the statement or produces a counterfeit. The false statements indicate that the customer's payment was properly posted. This leads the customer to believe that their account is up to date and keeps the customer from complaining about stolen payments.

False Accounting Entries

Intercepting the customer's statements will keep them unaware of their account's status, but as long as the customer's payments are being skimmed, their account is slipping further and further past due. The perpetrator must bring the account back up to date to conceal their crime. Lapping is one way to keep accounts current as the employee skims from them. Another way is to make false entries in the victim organization's accounting system.

DEBITS TO EXPENSE ACCOUNTS

An employee might conceal the skimming of funds by making unsupported entries in the victim company's books. If a payment is made on a receivable, for instance, the proper entry is a debit to cash and a credit to the receivable. Instead of debiting cash, the employee might choose to debit an expense account. This transaction still keeps the company's books in balance, but the incoming cash is never recorded. In addition, the customer's receivable account is credited, so it will not become delinquent.

DEBITS TO AGING OR FICTITIOUS RECEIVABLES

The same method discussed previously is used when employees debit existing or fictitious accounts receivable to conceal skimmed cash. For example, an employee who has skimmed one customer's payments might add the stolen amounts to aging accounts that will soon be written off as uncollectible or to very large accounts where a small debit might go unnoticed.

Some perpetrators also set up completely fictitious accounts and debit them for the cost of skimmed receivables. The employees then wait for the fictitious receivables to age and be

written off as uncollectable. In the meantime, the fictitious receivables carry the cost of a skimming scheme where it will not be detected.

WRITING OFF ACCOUNT BALANCES

Some employees cover their skimming by posting entries to contra revenue accounts such as discounts and allowances. If, for instance, an employee intercepts a $1,000 payment, the employee would create a $1,000 "discount" on the account to compensate for the missing money. Another account that might be used in this type of concealment is the bad debts expense account.

EXAMPLE

A billing manager was authorized to write off certain patient balances as hardship allowances. This employee accepted payments from patients and then instructed billing personnel to write off the balance in question. The payments were never posted; they were intercepted by the billing manager. The billing manager stole approximately $30,000 by using their authority to write off patients' balances.

Inventory Padding

A problem for fraudsters in some skimming schemes is the victim organization's inventory. Off-book sales of goods (skimming schemes) will always leave an inventory shortage and a corresponding rise in the cost of goods sold.

When a sale of goods is made, the physical inventory is reduced by the amount of merchandise sold. For instance, when a retailer sells a pair of shoes, there is one less pair of shoes in the stockroom. However, if a fraudster hands over the pair of shoes to a paying customer and keeps their cash without recording the sale, then the inventory balance on the company's books will be higher than the physical inventory on hand. Thus, there is one less pair of shoes available than in the perpetual inventory. A reduction in the physical inventory without a corresponding reduction in the perpetual inventory is known as *shrinkage*.

There is no shrinkage when an employee skims sales of services (because there is no inventory for services), but when sales of goods are skimmed, shrinkage always occurs. Some shrinkage is expected due to customer theft, faulty products, and spoilage, but high levels of shrinkage can be a warning that a company could be a victim of occupational fraud. The general methods used to conceal inventory shrinkage are discussed in detail in the

"Asset Misappropriation: Inventory and Other Assets" chapter in this section of the *Fraud Examiners Manual.*

Short-Term Skimming

Short-term skimming is not a distinct method for stealing sales and receivables but rather a distinct way of using skimmed money. The peculiar aspect to short-term skimming is that the fraudster keeps the stolen money only for a short while before eventually passing the payment on to their employer. The employee merely delays the posting. In a short-term skimming scheme, an employee steals an incoming payment and then places the skimmed funds in an interest-bearing account or in a short-term security. The employee earns interest on the skimmed payments while they remain under their control. Eventually, they withdraw the principal and apply it to the customer's account but retain the interest for themselves.

Detection of Skimming Schemes

The following are some detection methods that might be effective in detecting skimming schemes.

Receipt- or Sales-Level Detection

Key analytical procedures, such as vertical and horizontal analysis of sales accounts, can be used for skimming detection on a grand scale. These procedures analyze changes in the accounts and can possibly point to skimming problems, including understated sales.

Ratio analysis can also provide keys to the detection of skimming schemes. These procedures are discussed in detail in the "Financial Statement Fraud" chapter.

Detailed inventory control procedures can also be used to detect inventory shrinkage due to unrecorded sales. Inventory detection methods include statistical sampling, trend analysis, reviews of receiving reports and inventory records, and verification of material requisition and shipping documentation, as well as actual physical inventory counts. These procedures are reviewed in the "Asset Misappropriation: Inventory and Other Assets" chapter.

Journal Entry Review

Skimming can sometimes be detected by reviewing and analyzing all journal entries made to the cash and inventory accounts. Journal entries involving the following topics should be examined:

- False credits to inventory to conceal unrecorded or understated sales
- Write-offs of lost, stolen, or obsolete inventory
- Write-offs of accounts receivable accounts
- Irregular entries to cash accounts

Detecting Lapping of Sales or Receivables

A skimming scheme that involves lapping can be detected by comparing the dates of customers' payments with the dates that those payments are posted to the books. This requires an examination of the source documents, such as canceled check copies, bank statements, and deposit slips. Any significant discrepancies between these two dates might indicate that a customer's payment was skimmed, and the fraudster had to wait until another customer paid to post payment to the victim's account. Any significant discrepancies between deposit date and posting date should be investigated.

Confirmation of customers' accounts is another method that might detect skimming schemes that involve lapping.

In a *receivables skimming scheme*, the fraudster skims a customer's payment instead of posting it to the customer's account. The next payment that arrives gets posted to the skimming victim's account, and so on. Therefore, in a skimming scheme, at least one customer account will appear delinquent on the books, even though that customer has paid.

Confirmation of large accounts is especially effective in instances where the time value of money is an issue. However, customers who pay on invoice rather than on balance might not know the exact balance of their account. If this is the case, it might be more effective to confirm by invoice and reconstruct the account balance using the source documents in the files and the results of the confirmation. If fraud is suspected, ask the customer or the bank to return a copy of both the front and the back of the check(s) used to pay specific invoices. Match the data on the check copies with the posting dates in the customer's account.

Prevention of Skimming Schemes

Receipt- or Sales-Level Control

As with most fraud schemes, internal control procedures are a key to the prevention of skimming schemes. An essential part of developing control procedures is management's communication to employees. Controlling whether an employee will not record a sale, understate a sale, or steal incoming payments is extremely difficult.

General Controls

Sales entries and general ledger access controls should include documented policies and procedures, which are communicated directly from management. The control procedures will generally cover the following subjects:

- Appropriate separation of duties and access control procedures over the recording of ledger transactions
- Proper recording of all transactions (i.e., amount, date of occurrence, and correct account)
- Effective measures to safeguard access to the accounting systems and company assets
- Monitoring of all areas where employees handle cash with visible video cameras
- Independent reconciliations, as well as internal verification, of accounts

It is important to note that since skimming is an off-book fraud, routine account reconciliation is not likely to prevent or detect a skimming scheme. If such a scheme is taking place, reconciling the register records to the cash in the drawer will not indicate there is anything amiss. Reconciling the physical inventory count with the perpetual inventory records, however, might reveal that there is shrinkage, and therefore a skimming scheme.

Skimming Controls

The discovery of theft of incoming payments involves proper controls on the receipt process. Deficiencies in the answers to these typical audit-program questions might be red flags.

- Is mail opened by someone independent of the cashier, accounts receivable bookkeeper, or other accounting employees who may initiate or post journal entries?
- Is the delivery of unopened business mail prohibited to employees having access to the accounting records?
- Does the employee who opens the mail:
  - Place restrictive endorsements ("For Deposit Only") on all checks received?
  - Prepare a list of the money, checks, and other receipts?

  - Forward all remittances to the person responsible for preparing and making the daily bank deposit?
  - Forward the total of all remittances to the person responsible for comparing it to the authenticated deposit ticket and amount recorded?
- Is a lockbox used?
- Do cash sales occur? If yes:
  - Are cash receipts prenumbered?
  - Is an independent check of prenumbered receipts done daily and reconciled to cash collections?
- Do cash refunds require approval?
- Are cash receipts deposited intact daily?
- Are employees who handle receipts bonded?
- Is the accounts receivable bookkeeper restricted from:
  - Preparing the bank deposit?
  - Obtaining access to the cash receipts journal?
  - Having access to collections from customers?
  - Are banks instructed not to cash checks drawn to the order of the company?
- Is the cashier restricted from gaining access to the accounts receivable records and bank and customer statements?
- Are areas where physical handling of cash takes place reasonably safeguarded?
- Is the person who makes postings to the general ledger independent of the cash receipts and accounts receivable functions?
- Does a person independent of the cashier or accounts receivable functions handle customer complaints?

Cash Larceny

The second type of cash receipts scheme is cash larceny. In the occupational fraud setting, *cash larceny* is the intentional taking of an employer's cash (the term *cash* includes both currency and checks) without the consent and against the will of the employer. However, recall that skimming also involves the intentional taking of an employer's cash. The difference between skimming and cash larceny is that skimming is the theft of cash *before* it appears on the books. Cash larceny schemes involve the theft of money that has *already appeared* on a victim company's books. Accordingly, cash larceny schemes are easier to detect than skimming schemes because they leave an audit trail.

A cash larceny scheme can take place in any circumstance in which an employee has access to cash. Note, however, that cash larceny schemes do not include theft of cash on hand (i.e., cash located in a bank vault or other secure area). Every company must deal with the receipt, deposit, and distribution of cash, so every company is potentially vulnerable to a cash larceny scheme. While the circumstances in which an employee might steal cash are nearly limitless, most larceny schemes involve the theft of incoming cash, currency available (in a cash register, cash box, etc.), or theft of cash from the victim organization's bank deposits.

Incoming Cash

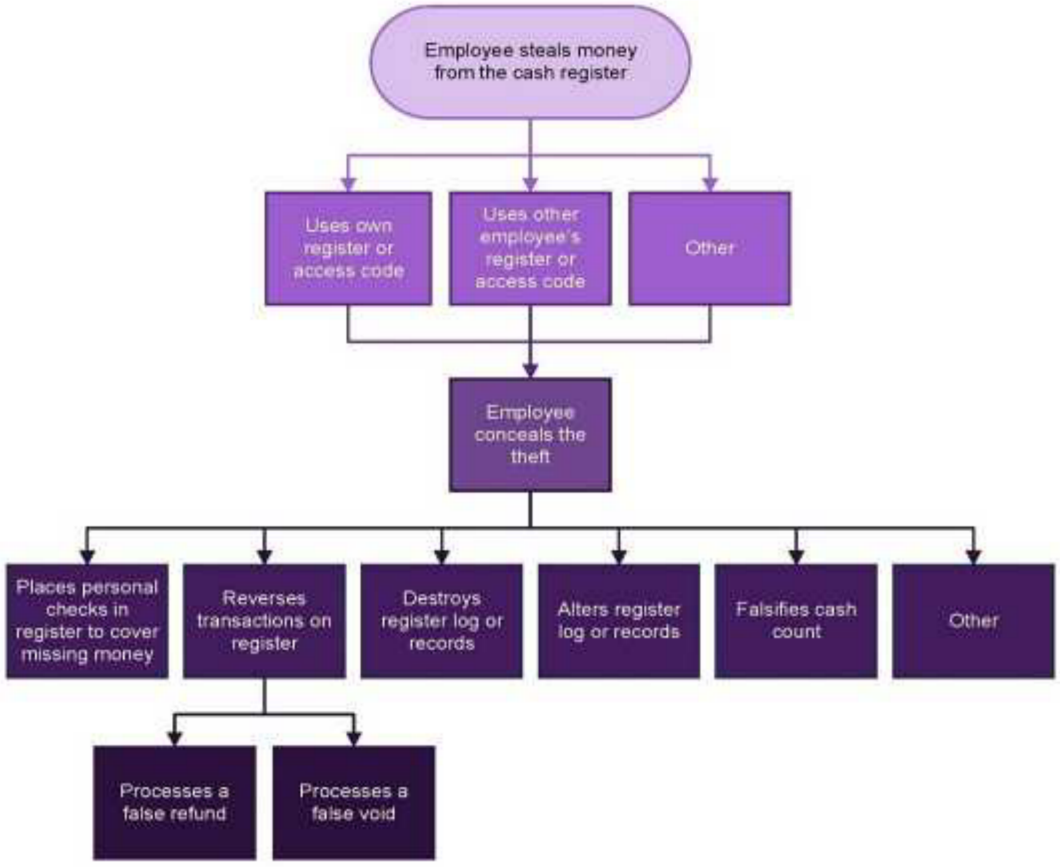
Theft of Cash from the Register

A large percentage of cash larceny schemes occur at the cash register, and for good reason—the register is usually where the cash is. The register (or similar cash collection points like cash drawers or cash boxes) is usually the most common point of access to cash for employees, so it is understandable that this is where larceny schemes frequently occur. Furthermore, there is often a great deal of activity at the register—numerous transactions that require employees to handle cash. This can serve to prevent cash theft from being discovered. In a flurry of activity, with money being passed back and forth between customer and employee, an employee can often sneak cash out of the register and into their pocket undetected.

The most straightforward cash larceny scheme is to open the register and remove currency or checks. (See the "Cash Larceny from the Register" flowchart that follows.) The theft is often committed while a sale is being conducted so that it appears to be part of the transaction. In other circumstances, perpetrators wait for a moment when no one is around to notice them reaching into the cash drawer.

Recall that the difficulty in detecting skimming schemes comes from the fact that the stolen funds are never entered on the victim organization's accounts. In a larceny scheme, however, the funds that the perpetrator steals have already been reflected on the register log. As a result, an imbalance will result between the register log and the cash drawer.

A register is balanced by comparing the transactions on the register log to the amount of cash on hand. Sales, returns, and other register transactions that are recorded on the register log are added to or subtracted from a known balance to determine the total for the period in question. The actual cash is then counted, and the two totals are compared. If the register log shows that there should be more cash in the register than what is present, the discrepancy might be due to larceny.



Cash Larceny from the Register

The actual method for taking money at the register—opening the register and removing currency—rarely varies. It is the methods that perpetrators use to avoid getting caught that distinguish larceny schemes. Oddly, in many instances the perpetrators have no plan for avoiding detection. A large part of fraud is rationalization; employees convince themselves that they are somehow entitled to what they are taking or that what they are doing is not actually a crime. Register larceny schemes frequently begin when perpetrators convince themselves that they are only borrowing the funds to cover a temporary monetary need. These people might carry the missing currency in their registers for several days, deluding themselves in the belief that they will one day repay the funds they have stolen.

Employees who do nothing to camouflage their crimes are easily caught. More dangerous is the person taking active steps to hide their crimes. One basic way for employees to disguise the fact that they are stealing currency is to take money from someone else's register.

In some retail organizations, employees are assigned to certain registers. Alternatively, one register is used, and each employee has a different access code. When cash is missing from a certain cashier's register, that cashier is obviously the most likely suspect of the theft. Therefore, by stealing from a coworker's register, or by using someone else's access code to enter the register, the perpetrator makes sure that another employee will be the prime suspect in the theft.

EXAMPLE

A teller for a retail sales company logged onto a register, performed a No-Sale transaction, and took currency from the drawer. Over a period of time, the teller took approximately $6,000 through this simple method. To get away with the theft, the teller waited until a coworker was on break and then logged onto that person's register, performed a No-Sale transaction, and took the cash. The resulting cash shortage therefore appeared in an honest employee's register, deflecting attention from the true thief.

A very unsophisticated way to avoid detection is to steal currency in very small amounts over an extended period of time. Because the missing amounts are small, the shortages might be dismissed as accounting errors rather than theft. Typically, the employee becomes dependent on the extra money and begins stealing more frequently or taking larger amounts, which causes the scheme to be uncovered. Most retail organizations track overages or shortages by employee, making this method largely ineffective.

REVERSING TRANSACTIONS

Some employees conceal cash larceny by processing reversing transactions, which cause the register log to reconcile to the amount of cash on hand after the theft. By processing false voids or refunds, an employee can reduce the cash balance reflected on the register log.

EXAMPLE

A cashier received payments from a customer and recorded the transactions on their system. The cashier stole the payments from the customers and then destroyed the company's receipts that reflected the transactions. To complete the cover-up, the cashier went back and voided the transactions that they had entered at the time the payments were received. The reversing entries brought the receipt totals into balance with the cash on hand.

REGISTER MANIPULATION

Instead of using reversing entries, an employee might manually alter the register log. Again, the purpose of this activity is to force a balance between the cash on hand and the actual cash received. An employee might use correction fluid to cover up a sale where the proceeds were stolen or might cross out or alter the numbers on the tape so that the register total and the cash drawer balance. This type of concealment is not common because the alterations will generally be noticeable.

ALTERING CASH COUNTS

Another method for concealing cash larceny is to alter the cash counts on registers. When cash from a register is totaled and prepared for deposit, an employee records the wrong amount so that the cash on hand appears to balance with the total on the register log. Employees who deal with the receipt of cash should not be charged with verifying the amount of cash on hand in their own register, but this control is often overlooked.

DESTROYING REGISTER LOGS

If the fraudster cannot make the cash and the tape balance, the next best thing is to prevent others from computing the totals and discovering the imbalance. Employees who are stealing from the register sometimes destroy detail tapes that would implicate them in a crime. When detail tapes are missing or defaced, it might be because someone is trying to conceal a fraud.

Other Larceny of Sales and Receivables

Not all receipts arrive via the cash register. Employees can just as easily steal money received at other points. One of the more common methods is to take checks received through the mail and post the payments to the accounting system but steal the checks. (See the "Other Cash Larceny" flowchart that follows.) Obviously, this type of scheme leaves the cash account out of balance. From a perpetrator's perspective, it would make much more sense to take checks that have not yet been posted to customer accounts. Often, this type of cash larceny scheme is committed by an employee who claims to only be "borrowing" the funds for a short while—one of the classic rationalizations in occupational fraud schemes.

Those employees who have total control of a company's accounting system can overcome the problem of out-of-balance accounts. It is common, especially in small businesses, for a single person to control all of a company's deposits and ledgers. These employees can steal incoming cash that has already been posted and then conceal the crime by making

unsupported entries in the victim organization's books. Poor separation of duties is often the weakness that allows cash larceny schemes to go undetected.

EXAMPLE

An employee posted customer payments to the accounts receivable journal but stole the cash received. This resulted in an imbalance in the victim company's cash account. But the perpetrator had control over the company's deposits and all its ledgers. This allowed the employee to conceal the crime by making unsupported entries in the company's books that produced a fictitious balance between receipts and ledgers.

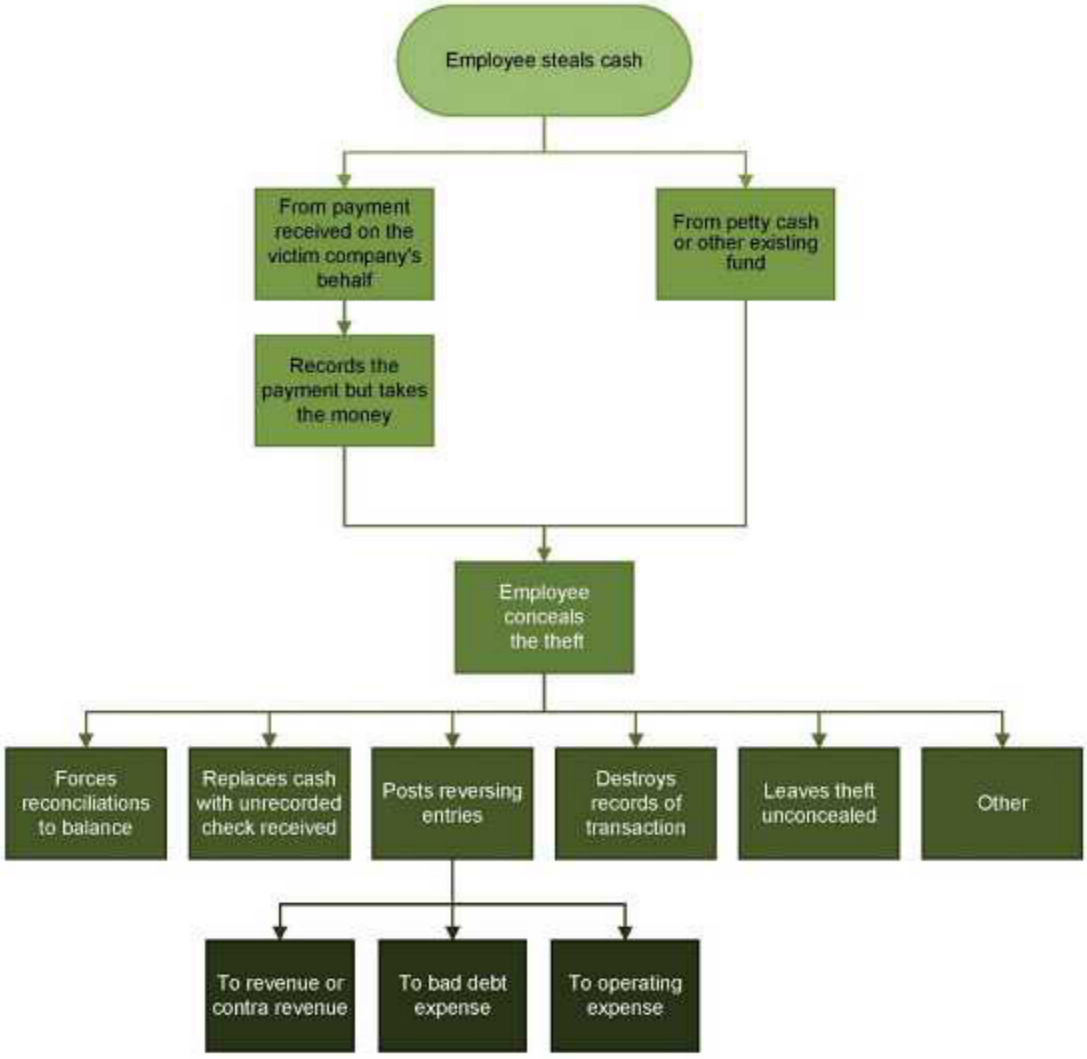
In circumstances in which payments are stolen but nonetheless posted to the cash receipts journal, reversing entries are sometimes used to balance the victim company's accounts. The incoming payment is initially credited to the customer's account, but the entry is later reversed with an unauthorized adjustment such as a "courtesy discount."

A less elegant way to hide a crime is to destroy all records that might prove that the perpetrator has been stealing. This "slash-and-burn" concealment technique does not prevent the victim company from realizing that it has been robbed, but it might help conceal the thief's identity.

Cash Larceny from the Deposit

At some point in every revenue-generating business, someone must physically take the company's currency and checks to the bank. Any individual(s) left alone in possession of the currency and checks will have an opportunity to take a portion of the money prior to depositing it into the company's accounts.

Typically, when a company receives cash, someone is assigned to tabulate the receipts, list the form of payment (currency or check), and prepare a deposit slip for the bank. Then another employee takes the cash and deposits it in the bank. The person who made out the deposit generally retains one copy of the slip. This copy is matched to a receipted copy of the slip, which the bank stamps when the deposit is made.



Other Cash Larceny

This procedure is designed to prevent the theft of funds from the deposit, but thefts still occur, often because companies do not adhere to the process. (See the "Cash Larceny from the Deposit" flowchart that follows.) For example, when one person is in charge of preparing the deposit slips, making the deposit, and reconciling the bank statement, that person can pilfer money from the day's receipts and conceal it by falsifying the deposit slips. If the day's receipts are $1,000, the perpetrator might fill out a deposit slip for $500 and steal the other $500. The employee then makes correspondingly false entries in the books, understating the day's receipts. This process creates a false balance in the victim organization's records.

A failure to reconcile the bank copy of the deposit slip with the office copy can result in fraud. When the person making the deposit knows their company does not reconcile the two copies, they can steal cash from the deposit on the way to the bank and alter the deposit slip so that it reflects a lesser amount. In some cases, sales records are also altered to match the diminished deposit.

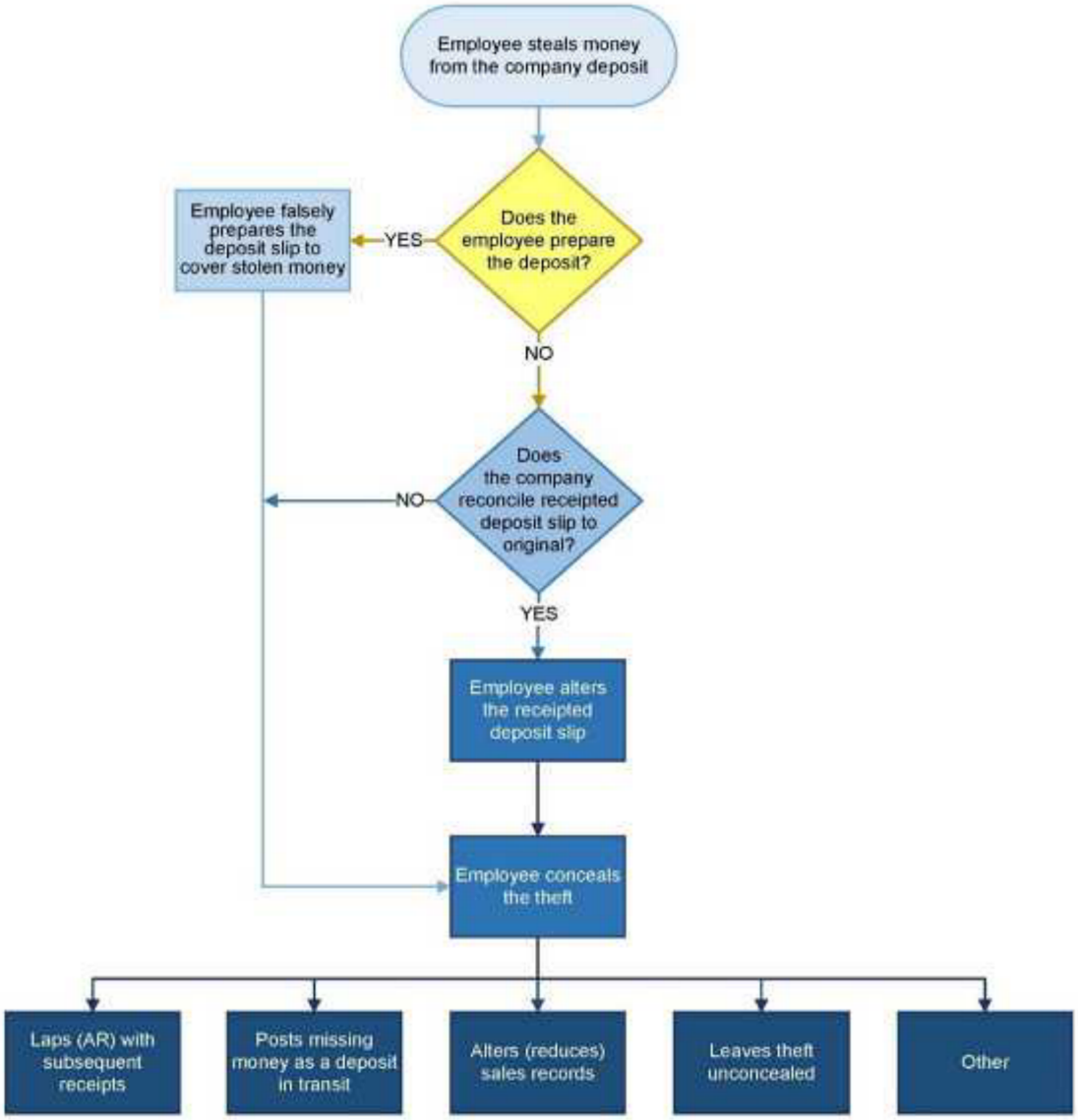
When cash is stolen from the deposit, the receipted deposit slip will of course be out of balance with the company's copy of the deposit slip (unless the perpetrator also prepared the deposit). To correct this problem, some perpetrators alter the bank copy of the deposit slip after it has been validated. This brings the two copies back into balance.

EXAMPLE

An employee altered 24 deposit slips and validated bank receipts in the course of a year to conceal the theft of more than $15,000. These documents were altered with correction ink to match the company's cash reports.

One common-sense issue that organizations sometimes overlook is the handling of the deposit on the way to the bank. Once prepared, the deposit should immediately be put in a safe place until it is taken to the bank. Unfortunately, some organizations leave their deposits carelessly unattended. For example, some companies prepare the daily deposit and then leave it in the office overnight to be taken to the bank the next morning. Employees familiar with this routine have little trouble pilfering checks and currency from the deposit after hours.

As with all cash larceny schemes, stealing from the company deposit can be rather difficult to conceal. In most cases, these schemes are only successful in the long term when the person who counts the cash also makes the deposit. In any other circumstance, the scheme's success depends primarily on the inattentiveness of those charged with preparing and reconciling the deposit.



Cash Larceny from the Deposit

Deposit Lapping

One method that fraudsters sometimes use to conceal cash larceny from the deposit is *lapping*. Lapping occurs when an employee steals the deposit from day one and then replaces it with day two's deposit. Day two's deposit is then replaced with money received on day three, and so on. The perpetrator is always one day behind, but as long as no one demands an immediate reconciliation of the deposits to the bank statement—and if daily receipts do not drop precipitously—they might be able to avoid detection for a period of time. Lapping is discussed in more detail in the "Skimming" section.

Deposits in Transit

A final concealment strategy used for stolen deposits is to carry the missing money as *deposits in transit* on the bank reconciliation, which is money that has been recorded in the company's cash account in its general ledger but has not cleared the bank. This is one of the ways to account for discrepancies between the company's records and the bank statement. Although usually reasonable, deposits in transit can be used to conceal a cash larceny from the deposit. The deposit in transit amount should be traced to subsequent bank statements to ensure its legitimacy.

EXAMPLE

An employee was responsible for receiving collections, issuing receipts, posting transactions, reconciling accounts, and making deposits. This employee took over $20,000 in collections from their employer over a five-month period. To hide the theft, the perpetrator carried the missing money as deposits in transit, meaning that the missing money would appear on the next month's bank statement. Of course, it never did. The balance was carried for several months as deposits in transit (d.i.t.) until an auditor recognized the discrepancy and put a halt to the fraud.

Detection of Cash Larceny

As mentioned previously, cash larceny involves the theft of cash that appears on a company's books or records, whether it is theft of cash in a cash register or theft of cash from a deposit. Cash larceny schemes are easier to detect than skimming schemes because they leave an audit trail.

Receipt Recording

In-depth analysis of the cash receipts and recording process is the key to detecting a cash larceny scheme. Areas of analysis might include:

- Mail and register receipt points
- Journalizing and recording of the receipts
- Security of the cash from receipt to deposit

Control Objectives

In analyzing the cash receipt process, it is important to meet the following control objectives:

- Cash receipts must be complete. Each day's receipts must be promptly collected and deposited in full.

- Each receivable transaction recorded must be legitimate and have supporting documentation.
- All information included in the transaction must be correctly verified as to amount, date, account coding, and descriptions.
- The cash must be safeguarded while in the company's physical possession.
- There must be appropriate personnel responsible for overseeing cash control processes.
- Cash register log totals should be reconciled to the amount of cash in the drawer.
- An independent listing of cash receipts should be prepared before the receipts are submitted to the cashier or accounts receivable bookkeeper.
- An independent person should verify the listing against the deposit slips.
- Authenticated deposit slips should be retained and reconciled to the corresponding amounts in the cash receipts records.
- The bank deposit should be made by someone other than the cashier or the accounts receivable clerk. A person independent of the cash receipts and accounts receivable functions should compare entries to the cash receipts journal with:
  - Authenticated bank deposit slips
  - The deposit per the bank statements
- Areas where physical handling of cash takes place should be reasonably safeguarded.

Analytical Review

Analyzing the relationship among sales, cost of sales, and the returns and allowances can detect inappropriate refunds and discounts.

- If a large cash fraud is suspected, a thorough review of these accounts might enlighten the fraud examiner as to the magnitude of the suspected fraud.
- An analysis of refunds and returns and allowances with the actual flow of inventory might reveal some fraud schemes. The refund should cause an entry to inventory even if it is damaged inventory. Likewise, a return will cause a corresponding entry to an inventory account.
- There should be a linear relationship between sales and returns and allowances over a relevant range. Any change in this relationship might point to a fraud scheme unless there is another valid explanation, such as a change in the manufacturing process, change in product line, or change in price.

Detection at the Register

As cash is received, whether at a register or through the mail, it is important to ensure that the employees responsible for completing these important tasks are informed of their responsibility and properly supervised.

- Access to the register must be closely monitored and access codes must be kept secure.
- All employees should have unique access codes to the cash registers. The time periods that each access code is used should be checked against employee work schedules to ensure an employee's access code was not used in their absence.
- An employee other than the register worker should be responsible for preparing register count sheets and reconciling them with register totals.
- Popular concealment methods must be watched for. These methods, discussed earlier, include checks for cash, reversing transactions, register log destruction or alteration, and sales cash counts.
- Complete register documentation and cash must be delivered to the appropriate personnel in a timely manner.
- Cash thefts are sometimes revealed by customers who have either paid money on an account and have not received credit or, in some cases, have noticed that the credit they have been given does not agree with the payment they have made. Complaints and inquiries are also received frequently from banks.

Cash Account Analysis

Cash larceny can be detected by reviewing and analyzing all journal entries made to the cash accounts. This review and analysis should be performed regularly. If an employee is unable to conceal the fraud by altering the source documents, such as the cash register log, then the employee might resort to making a journal entry directly to cash. Except in financial institutions, there are generally very few instances in everyday business activity where an independent journal entry is necessary for cash. One of these exceptions is the recording of the bank service charge. However, this is an easy journal entry to trace to its source documentation, namely the bank statement. Therefore, all other entries directly to cash are suspect and should be traced to their source documentation or explanation. Suspect entries will generally credit the cash account and correspondingly debit various other accounts such as a sales contra account or bad debt expenses.

Prevention of Cash Larceny

Cash larceny can be prevented through the implementation of certain controls by management. These controls include the following:

- Separation of duties
- Assignment rotation and mandatory vacations
- Surprise cash counts and procedure supervision
- Physical security of cash

Separation of Duties

The primary means of preventing cash larceny is separation of duties. Whenever one individual has control over the entire accounting transaction (e.g., authorization, recording, and custody), the opportunity is present for cash fraud. Ideally, each of the following duties and responsibilities should be separated:

- Cash receipts
- Cash counts
- Bank deposits
- Deposit receipt reconciliations
- Bank reconciliations
- Posting of deposits
- Cash disbursements

If any one person has the authority to collect the cash, deposit the receipts, record that collection, and disburse company funds, the risk of fraud is high.

Assignment Rotation and Mandatory Vacations

Many internal fraud schemes are continuous in nature and require ongoing efforts by the employee to conceal the fraud. Mandatory vacations are an excellent method of detecting cash fraud. If mandatory vacations are within the company's policies, then it is important that another individual continues to perform the normal workload of an absent employee. The purpose of mandatory vacations is lost if the work is allowed to remain undone during the employee's time off.

Surprise Cash Counts and Procedure Supervision

Surprise cash counts and supervisory observations can be useful fraud prevention methods. It is important that employees know that cash will be counted on a periodic and unscheduled basis. These surprise counts must be made at all steps of the process, from receiving

the check, to reconciling the register log to the cash in the drawer, to depositing the funds in the bank.

Physical Security of Cash

Physically securing cash is a measure used to help prevent theft of cash. The following are examples of ways cash can be properly and adequately secured:

- Ensure proper separation of duties of key personnel.
- Review the check and cash composition of the daily bank deposit during unannounced cash counts and during substantive audit tests of cash receipts.
- Review the entity's records of the numerical series of printed prenumbered receipts, and verify that these receipts are used sequentially (including voided documents).
- Review the timeliness of deposits from locations to the central treasurer function.
- Observe locations' cash receipting operations.
- Prepare and review a schedule of all cash receipting functions from a review of revenue reports, from cash receipt forms at the central treasurer function, and from discussion with knowledgeable employees.
- Prepare and analyze an inventory of all imprest and change funds by purpose, amount, custodian, date, and location.
- Audit all revenue sources on a cycle.
- Periodically use comparative analytical reviews to determine which functions have unfavorable trends.
- Determine reason(s) why revenue has changed from previous reporting periods.
- Confirm responses obtained from managers by using alternative records or through substantive audit tests.
- Adhere to a communicated policy of unannounced cash counts.

Theft of Cash on Hand

Another way cash can be misappropriated involves the theft of cash on hand. This type of fraud scheme differs from cash larceny and skimming in that it relates to cash that is kept in a secure place, such as a vault or safe. Employees who have access to this stored cash might have the ability to misappropriate or steal these funds.

ASSET MISAPPROPRIATION: FRAUDULENT DISBURSEMENTS

In fraudulent disbursement schemes, an employee makes a distribution of company funds for a dishonest purpose. Some examples of fraudulent disbursements include submitting false invoices for payment, altering time cards, and making personal purchases with company funds. Outwardly, the fraudulent disbursements do not appear any different from valid disbursements of cash. In many cases, the fraudster tricks the victim company into remitting payment. For instance, when an employee submits a fake invoice into the accounts payable system, the victim organization pays for the bad invoice right along with all the legitimate payments it makes. The perpetrator has taken money from their employer in such a way that it appears to be a normal disbursement of cash. Someone might notice the fraud based on the amount, recipient, or destination of the payment, but the *method* of payment is legitimate.

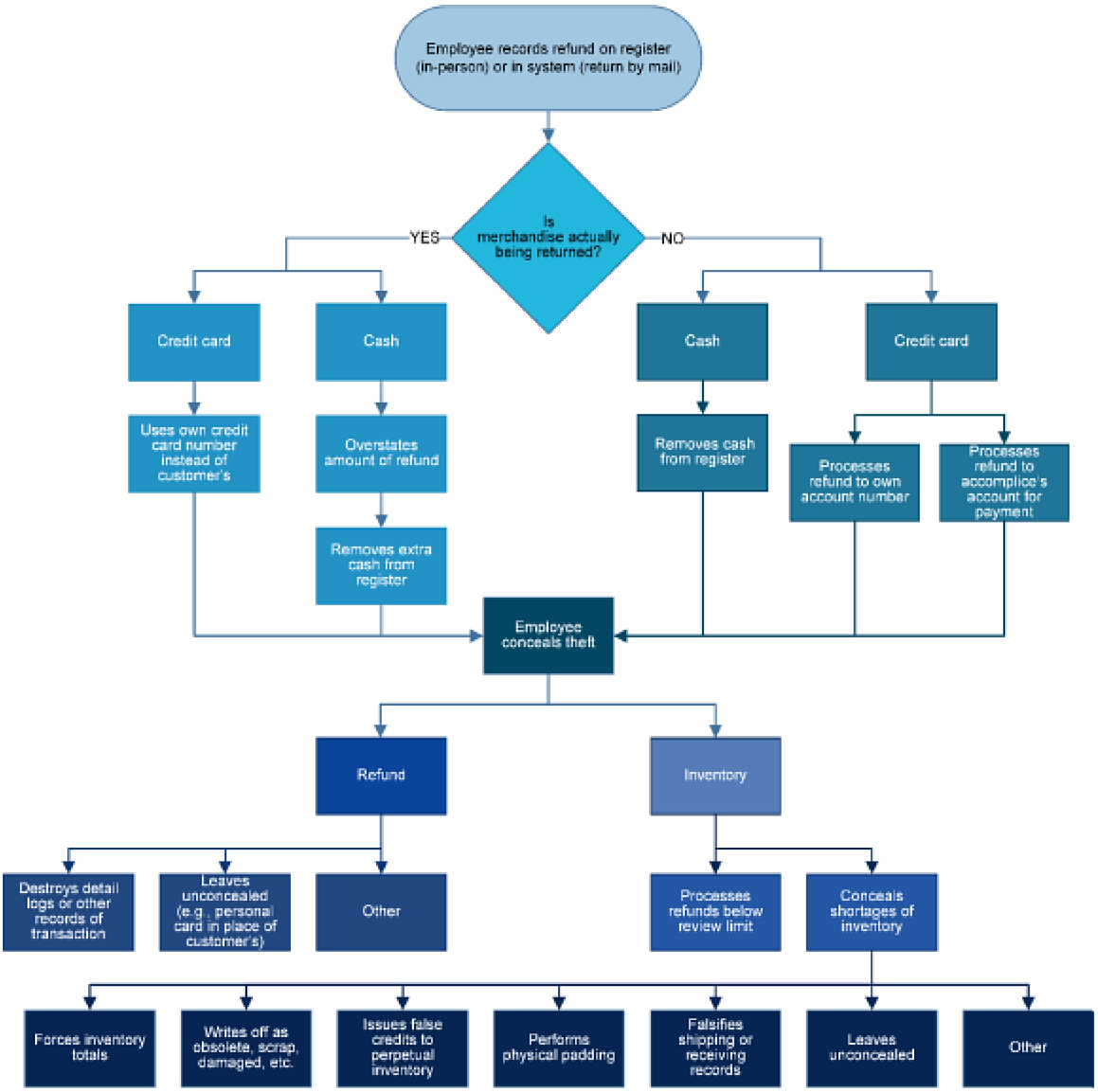
Register Disbursement Schemes

Fraudulent disbursements at the cash register are different from the other schemes that often take place at the register, such as skimming and cash larceny. When cash is stolen as part of a register disbursement scheme, the removal of the cash is recorded.

There are two basic register disbursement schemes: *false refunds* and *false voids*. While the schemes are largely similar, there are a few differences between the two that merit discussing them separately.

False Refunds

A refund is processed at the register when a customer returns an item of merchandise that was purchased from the store. The transaction that is entered on the register indicates that the merchandise is being replaced in the store's inventory and the purchase price is being returned to the customer. In other words, a refund shows cash being disbursed from the register to the customer. (See the "False Refunds" flowchart that follows.)



False Refunds

Fictitious Refunds

In a fictitious refund scheme, an employee processes a transaction as if a customer were returning merchandise, even though there is no actual return. Then the employee takes cash from the register in the amount of the false return. The customer might or might not be aware of the scheme taking place.

For instance, if an employee processes a fictitious return for a $100 pair of shoes, they remove $100 from the register. There are two results of this fraudulent transaction. First, the register log indicates that the shoes were returned, so the disbursement appears to be legitimate. The register log balances with the amount of cash in the register, because the money that was taken by the fraudster is supposed to have been removed and given to a customer as a refund.

The second repercussion is that a debit is made to the inventory system showing that the merchandise has been returned to the inventory. Since the transaction is fictitious, no merchandise is returned. The result is that the company's inventory balance on the books is overstated by the amount of the excess refund.

EXAMPLE

A manager created $5,500 worth of false returns, resulting in a large shortage in the company's inventory. The manager was able to carry on the scheme for several months because (1) inventory was not counted regularly and (2) the perpetrator (i.e., the manager) was one of the people who performed inventory counts.

Overstated Refunds

Rather than create an entirely fictitious refund, some employees merely overstate the amount of a legitimate refund and steal the excess money. For example, if a customer returns $100 worth of merchandise, the employee might record a $200 return. The employee gives the customer $100 in return for the merchandise and then keeps the remaining $100. This will result in shrinkage of $100 worth of inventory.

Payment Card Refunds

When purchases are made with a payment card (e.g., credit card or debit card) rather than cash, refunds appear as credits to the customer's card account rather than as cash disbursements. Some dishonest employees process false refunds on payment card sales in lieu of processing a normal cash transaction. One benefit of the payment card method is that the

perpetrator does not have to physically take cash from the register and carry it out of the store. By processing the refunds to a payment card account, a perpetrator reaps a financial gain and avoids the potential embarrassment of being caught taking cash.

In a typical payment card refund scheme, the perpetrator records a refund on a payment card sale even though the merchandise is not being returned. The employee credits their own payment card number rather than the customer's. The result is that the item's cost is credited to the perpetrator's payment card account.

A more creative and wide-ranging application of the payment card refund scheme occurs when employees process refunds to other people's accounts and receive a portion of the refund as a kickback in return. Suppose a person is $100 short on the rent. That person goes to the retail store where their friend is a teller and has the teller process a credit of $150 to their account. The "customer" then goes to an automated teller machine (ATM) and withdraws $150 in cash. They pay $50 to the teller and keep $100.

Refund schemes are more difficult to perpetrate in many high-tech retail stores where the cash registers have anti-fraud controls that require the refund to be made to the original payment card used for the purchase or that only allow for refunds in the form of a store credit for the current value of the item purchased.

False Voids

Fictitious voids are similar to refund schemes in that they make fraudulent disbursements from the register appear to be legitimate. When a sale is voided on a register, a copy of the customer's receipt is usually attached to a void slip, along with the signature or initials of a manager indicating that the transaction has been approved. (See the "False Voids" flowchart that follows.) To process a false void, the perpetrator first needs the customer's copy of the sales receipt. Typically, when an employee sets about processing a fictitious void, the employee withholds the customer's receipt at the time of the sale. In many cases, customers do not notice that they are not given a receipt.

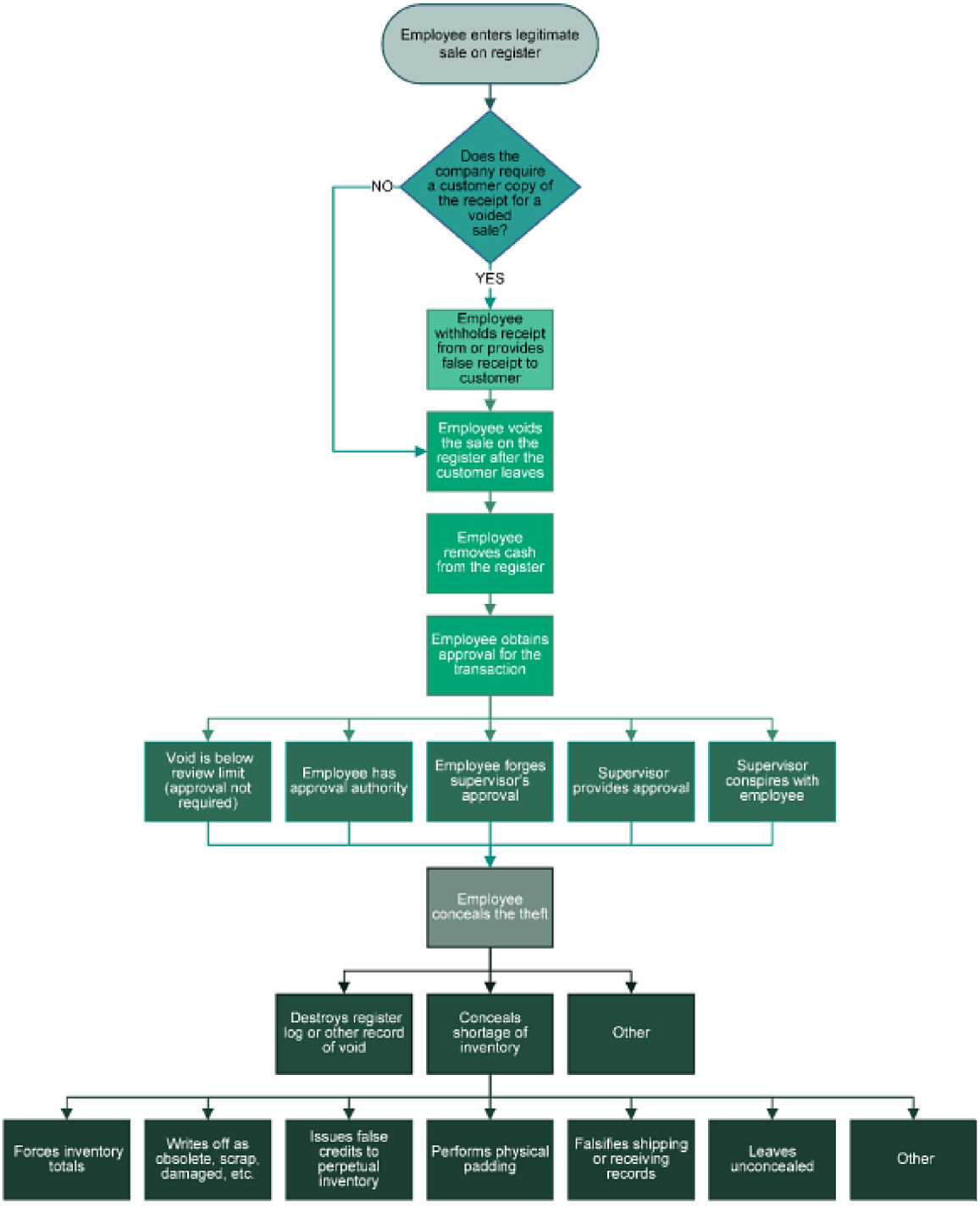
With the customer's copy of the receipt in hand, the culprit rings a voided sale. Whatever money the customer paid for the item is removed from the register as though it is being returned to a customer. The copy of the customer's receipt is attached to the void slip to verify the transaction's authenticity.

Before the voided sale will be perceived as valid, a manager generally must approve the transaction. In many instances, the manager in question neglects to verify the voided sale's authenticity. Some managers will sign almost anything presented to them and thus leave themselves vulnerable to voided sales schemes. It is not a coincidence that the perpetrators of these crimes present their void slips to managers who are lackadaisical about authorizing them. These kinds of managers are generally targeted by the fraudsters and are essential to the schemes' success.

EXAMPLE

An employee processed fraudulent voids, kept customer receipts, and presented them to supervisors for review at the end of the workday, long after the alleged transactions had taken place. The supervisors approved the voided sales, and the accounts receivable department failed to notice the excessive voided sales processed by this employee.

Obviously, not all managers give unquestioned approval to voided sales. Some employees must therefore take other routes to get their voided sales approved. In most of these cases, the perpetrator forges their supervisor's authorization on the fraudulent void slips. It is also possible that managers will conspire with cashiers and approve false voids in return for a share of the proceeds from the scheme.



False Voids

Concealing Register Disbursement Schemes

As previously discussed, there are two occurrences when a false refund or void is entered into the register. The first is that the employee committing the fraud removes cash from the register, and the second is that the item allegedly being returned is debited back into the

perpetual inventory. Of course, there is no merchandise being returned. This leads to inventory shrinkage, a situation in which there is less inventory on hand than the perpetual inventory records show. A certain amount of shrinkage is expected in any retail industry, but too much of it raises concerns of fraud. It is therefore in the perpetrator's best interest to conceal the appearance of shrinkage on the books.

Inventory is accounted for by a two-step process. The first part of the process is the perpetual inventory, which is a continuous tabulation of how much inventory *should be on hand*. When a sale of merchandise is made, the perpetual inventory is credited to remove this merchandise from the records. The amount of merchandise that should be on hand is reduced. (Conversely, when merchandise is returned, the perpetual inventory is debited.) Periodically, someone from the company takes a physical count of the inventory, going through the stockroom or warehouse and counting the amount of inventory that *is on hand*. The two figures are then compared to see if there is a discrepancy between the perpetual inventory (what should be on hand) and the physical inventory (what is on hand).

In register disbursement schemes, shrinkage is often concealed by overstating inventory during the physical count, especially if taking inventory is one of the perpetrator's duties. The perpetrator overstates the amount of inventory on hand so it matches the perpetual inventory. For a more detailed analysis of methods used to conceal inventory shrinkage, please see the "Asset Misappropriation: Inventory and Other Assets" chapter.

Small Disbursements

Another way for employees to avoid detection in a refund scheme is to keep the sizes of the disbursements low. Many companies set limits below which management review of a refund is not required. Where this is the case, employees process numerous refunds that are small enough that they do not have to be reviewed.

EXAMPLE

An employee created over one thousand false refunds, all under the review limit of $15. The employee was eventually caught because they began processing refunds before store hours and another employee noticed that refunds were appearing on the system before the store opened. Nevertheless, the employee made off with over $11,000 of their employer's money before their scheme was detected.

Destroying Records

One final means of concealing a register scheme is to destroy all records of the transaction. Most concealment methods are concerned with keeping management from realizing that fraud has occurred. When employees resort to destroying records, however, they typically have conceded that management will discover their theft. The purpose of destroying records is usually to prevent management from determining *who* the thief is.

Detection of Register Disbursement Schemes

Fictitious Refunds or Voided Sales

Fictitious refunds or voided sales can often be detected when closely examining the documentation submitted with the cash receipts.

- One detection method is to evaluate the refunds or discounts given by each cashier or salesperson. This analysis might indicate that a single employee or group of employees has a higher incidence of refunds or discounts than others. Further examination is then necessary to determine if the refunds are appropriate and properly documented.
- Signs in the register area asking customers to ask for and examine their receipts employ the customer as part of the internal control system. This helps ensure that the cashier or salesperson is properly accounting for the sale and prevents employees from using customer receipts as support for false void or refunds.
- Random service calls to customers who have returned merchandise or voided sales can be used to verify the legitimacy of transactions.

Review and Analysis of Decreases in Gross Sales or Increases in Returns and Allowances

Analyzing the relationship between sales, cost of sales, and the returns and allowances can detect inappropriate refunds and discounts. If a large cash fraud is suspected, a thorough review of these accounts might enlighten the examiner as to the suspected fraud's magnitude. An analysis of refunds and returns and allowances with the actual flow of inventory might reveal some fraud schemes. The refund should cause an entry to inventory, even if it is damaged inventory. Likewise, a return will cause a corresponding entry to an inventory account. There should be a linear relationship between sales and returns and allowances over a relevant range. Any change in this relationship might point to a fraud scheme unless there is another valid explanation, such as a change in the manufacturing process, change in product line, or change in price.

Register Disbursement Scheme Red Flags

Red flags of register disbursement schemes include the following:

- There is inappropriate separation of duties for employees. For example, register counting and reconciling should not be done by the cashier.
- Cashiers, rather than supervisors, have access to the controls necessary for refunds and voids.
- Cashiers are authorized to void their own transactions.
- Register refunds are not carefully reviewed.
- Multiple cashiers operate from a single cash drawer without separate access codes.
- Personal checks from cashiers are found in the cash register.
- Voided transactions are not properly documented or approved by a supervisor.
- Voided cash receipt forms (manual systems) or supporting documents for voided transactions (cash register systems) are not retained on file.
- There are missing or obviously altered register logs.
- There are gaps in the transaction numbers on the register log.
- There are excessive refunds, voids, or no-sales on the register records.
- Inventory totals appear forced.
- There are multiple refunds or voids for amounts just under the review limit.

Prevention of Register Disbursement Schemes

The following are preventive controls that can reduce the risk of register disbursement schemes:

- Review the separation of duties of employees who staff the register, as well as the duties of their supervisors.
- As cash is received, ensure that the employees responsible for completing these important tasks are informed of their responsibilities and properly supervised.
- Ensure that an employee other than the register worker is responsible for preparing register count sheets and reconciling them with register totals.
- Make sure that complete register documentation and cash are delivered to the appropriate personnel in a timely manner.
- Be aware that cash thefts are sometimes revealed by customers who have paid money on an account and have not received credit or have been credited for an amount that does not agree with the payment they have made. Complaints and inquiries are also received frequently from banks.
- Closely monitor access to the register and keep access codes secure.
- Analyze the quantity of refunds to detect multiple small refunds.

- Communicate and adhere to the company policy of performing unannounced cash counts.
- Maintain the presence of a manager or supervisor near the area of the cash register as a deterrent to theft.
- Review supporting documents for voided and refunded transactions for propriety (i.e., legitimacy and approvals).
- Review the numerical sequence and completeness of cash register logs.

Payment Tampering Schemes

Payment tampering schemes are those schemes in which an employee steals their employer's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts. Because many business payments are still made by check, the bulk of this section will focus on how traditional check-based payments can be manipulated by dishonest employees. However, businesses are increasingly using electronic forms of payment—such as wire transfers, automated clearing house (ACH) debits, and online bill-pay services—to pay vendors and other third parties. Consequently, the specific implications and considerations of these types of payments are discussed separately in the section on "Electronic Payment Tampering."

Check Tampering Schemes

Check tampering is unique among the fraudulent disbursement schemes because it is the one group in which the perpetrator physically prepares the fraudulent check. In most fraudulent disbursement schemes, the culprit generates a payment to themselves by submitting some false document to the victim organization, such as an invoice or a time card. The false document represents a claim for payment and causes the victim organization to issue a check that the perpetrator can convert.

Check tampering schemes are fundamentally different. In these schemes, the perpetrator takes physical control of a check and makes it payable to themselves through one of several methods. Check tampering frauds depend upon factors such as access to the company checkbook, access to bank statements, and the ability to forge signatures or alter other information on the face of the check. Most check tampering crimes fall into one of four categories: forged maker schemes, forged endorsement schemes, altered payee schemes, and authorized maker schemes.

Forged Maker Schemes

Forgery can include not only the *signing of another person's name* to a document (such as a check) with a fraudulent intent, but also the fraudulent *alteration* of a genuine instrument. This definition is so broad that it would encompass all check tampering schemes. For the purposes of this text, the definition of forgery has been narrowed to fit the fraud examiner's needs. To properly distinguish the various methods used by individuals to tamper with checks, the concept of *forgeries* will be limited to those cases in which an individual signs another person's name on a check.

The person who signs a check is known as the *maker* of the check. A forged maker scheme can thus be defined as a check tampering scheme in which an employee misappropriates a check and fraudulently affixes the signature of an authorized maker thereon. (See the "Forged Maker Schemes" flowchart that follows.) Frauds that involve other types of check tampering, such as the alteration of the payee or the changing of the amount, are classified separately.

To forge a check, an employee must have access to a blank check, be able to produce a convincing forgery of an authorized signature, and be able to conceal their crime. Concealment is a universal problem in check tampering schemes; the methods used are basically the same whether one is dealing with a forged maker scheme, an intercepted check scheme, or an authorized maker scheme. Therefore, concealment issues will be discussed as a group later in this section.

OBTAINING THE CHECK

EMPLOYEES WITH ACCESS TO COMPANY CHECKS

One cannot forge a company check unless one first possesses a company check. Most forgery schemes are committed by accounts payable clerks, office managers, bookkeepers, or other employees whose duties typically include the preparation of company checks. These are people who have regular access to the company checkbook and can steal blank checks.

EMPLOYEES LACKING ACCESS TO COMPANY CHECKS

If perpetrators do not have access to the company checkbook through their work duties, they will have to find other means of misappropriating a check. The method by which a person steals a check depends largely on how the checkbook is handled within a particular company. In some circumstances, the checkbook is poorly guarded and left in unattended areas where anyone can get to it. In other companies, the check stock might be kept in a restricted area, but the perpetrator might have obtained a key or combination to this area or might know

where an employee with access to the checks keeps their own copy of the key or combination. An accomplice might provide blank checks for the fraudster in return for a portion of the stolen funds. Perhaps an administrative assistant sees a blank check left on a manager's desk or a custodian comes across the check stock in an unlocked desk drawer.

In some companies, checks are computer-generated. When this is the case, an employee who knows the password for preparing and issuing checks can usually obtain as many unsigned checks as they desire. There is an unlimited number of ways to steal a check, each dependent on the way in which a particular company guards its blank checks. In some instances, employees go as far as to produce counterfeit checks.

EXAMPLE

An employee had an accomplice who worked for a check-printing company. The accomplice was able to print blank checks with the account number of the perpetrator's company. The perpetrator then wrote over $100,000 worth of forgeries on these counterfeit checks.

TO WHOM IS THE CHECK MADE PAYABLE?

TO THE PERPETRATOR

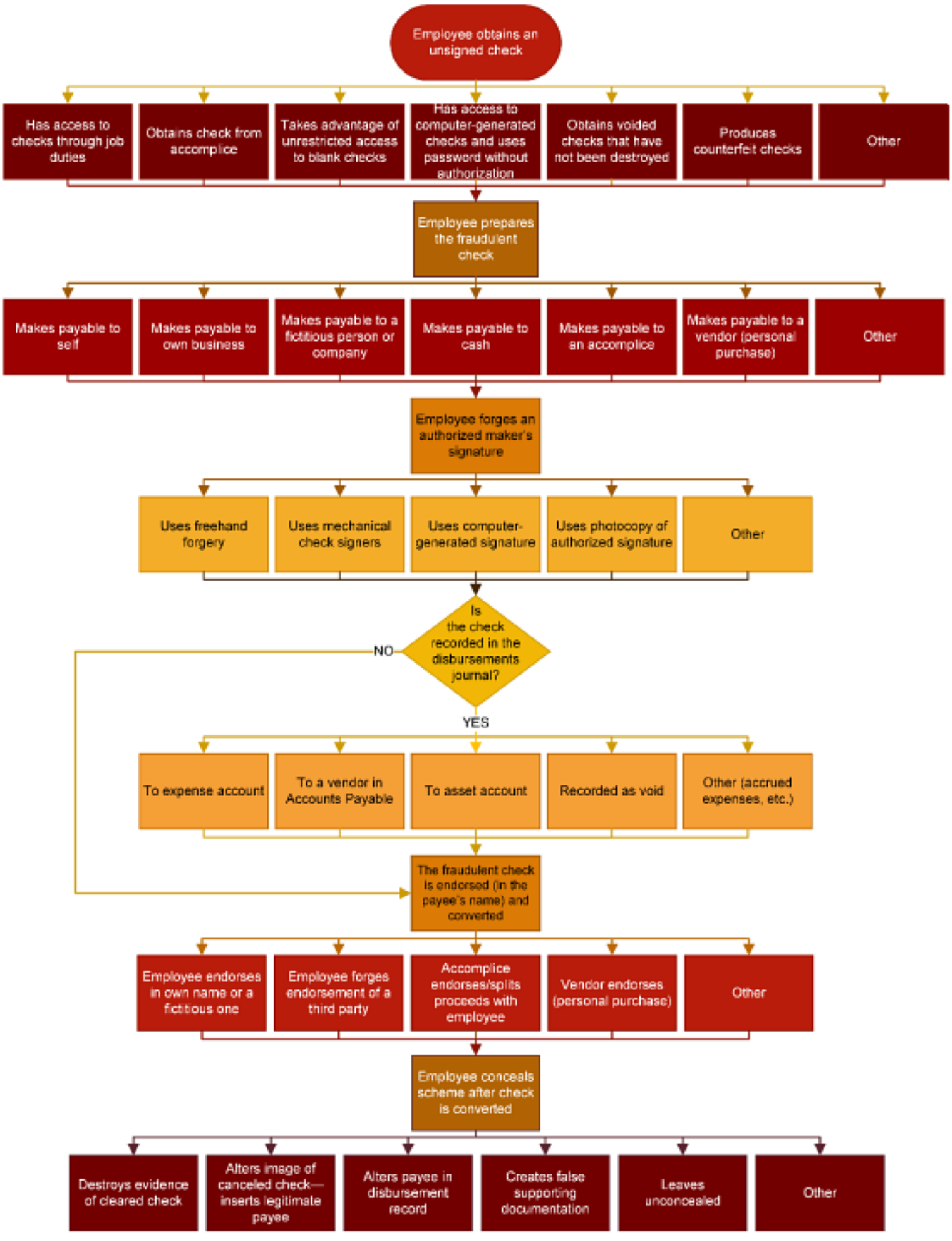
Once a blank check has been obtained, the perpetrator must decide to whom it should be made payable. In most instances, forged checks are made payable to the perpetrator so that they can be easily converted. Canceled checks that are payable to an employee should be closely scrutinized for the possibility of fraud.

If the perpetrator owns their business or has established a shell company, they will usually write fraudulent checks to these entities rather than themselves. These checks are not as obviously fraudulent on their faces as checks made payable to an employee. At the same time, these checks are easy to convert because the perpetrator owns the entity to which the checks are payable.

TO AN ACCOMPLICE

If a fraudster is working with an accomplice, the fraudster can make the forged check payable to that person. The accomplice then cashes the check and splits the money with the employee-fraudster. Because the check is payable to the accomplice in their true identity, it is easily converted. An additional benefit to using an accomplice is that a canceled check payable to a third-party accomplice is not as likely to raise suspicion as a canceled check to an

employee. The obvious disadvantage to using an accomplice in a scheme is that the employee-fraudster usually must share the proceeds.



Forged Maker Schemes

TO "CASH"

The perpetrator might also write checks payable to "cash" to avoid listing themselves as the payee. Checks made payable to cash, however, must still be endorsed. The perpetrator will have to sign their own name or forge the name of another to convert the check. Checks payable to cash are usually viewed more skeptically than checks payable to persons or businesses. Some institutions might refuse to cash checks made payable to cash.

TO VENDORS

Not all fraudsters forge company checks to obtain cash. Some employees use forged maker schemes to purchase goods or services for their own benefit. These fraudulent checks are made payable to third-party vendors who are uninvolved in the fraud. For instance, an employee might forge a company check to buy a home computer. The computer vendor is not involved in the fraud at all. Furthermore, if the victim organization regularly does business with this vendor, the person who reconciles the company's accounts might assume that the check was used for a legitimate business expense.

FORGING THE SIGNATURE

After the employee has obtained and prepared a blank check, they must forge an authorized signature to convert the check. The most obvious method, and the one that comes to mind when one thinks of the word *forgery*, is to sign the name of an authorized maker.

FREE-HAND FORGERY

The difficulty a fraudster encounters when physically signing the authorized maker's name is in creating a reasonable approximation of the true signature. If the forgery appears authentic, the perpetrator will probably have no problem cashing the check. In truth, the forged signature might not have to be particularly accurate. Many fraudsters cash forged checks at liquor stores, grocery stores, or other institutions that are known to be less than diligent in verifying signatures and identification. Nevertheless, a poorly forged signature is an obvious red flag of fraud. The maker's signature on canceled checks should be reviewed for forgeries during the reconciliation process.

PHOTOCOPIED FORGERIES

To guarantee an accurate forgery, some employees make photocopies of legitimate signatures. The signature of an authorized signer is copied from some document (such as a business letter) onto a transparency, and then the transparency is laid over a blank check so that the

signature copies onto the maker line of the check. The result is a check with a perfect signature of an authorized maker.

AUTOMATIC CHECK-SIGNING MECHANISMS

Companies that issue many checks sometimes use automatic check-signing mechanisms in lieu of signing each check by hand. Automated signatures are produced with manual instruments, such as signature stamps, or they are printed by computer. Obviously, a fraudster who gains access to an automatic check-signing mechanism will have no trouble forging the signatures of authorized makers. Even the most rudimentary control procedures should severely limit access to these mechanisms.

EXAMPLE

A fiscal officer maintained a set of manual checks that were unknown to other persons in the company. The company used an automated check signer and the custodian of the signer let the officer have uncontrolled access to it. Using the manual checks and the company's check signer, the fiscal officer was able to write over $90,000 worth of fraudulent checks in their own name over a period of approximately four years.

The same principle applies to computerized signatures. Access to the password or program that prints signed checks should be restricted, specifically excluding those who prepare checks and those who reconcile the bank statement.

CONVERTING THE CHECK

To convert the forged check, the perpetrator must endorse it. The endorsement is typically made in the name of the payee on the check. Since identification is typically required when one seeks to convert a check, the perpetrator usually needs fake identification if they forge checks to real or fictitious third persons. As discussed earlier, checks payable to "cash" require the endorsement of the person converting them. Without a fake ID, the perpetrator will likely have to endorse these checks in their own name. An employee's endorsement on a canceled check is obviously a red flag.

Forged Endorsement Schemes

Forged endorsements are those check tampering schemes in which an employee intercepts a company check intended to pay a third party and converts the check by endorsing it in the third party's name. In some cases, the employee also signs their own name as a second endorser. (See the "Forged Endorsement Schemes" flowchart that follows.)

A fraudster's main dilemma in a forged endorsement scheme (and in all intercepted check schemes, for that matter) is gaining access to a check after it has been signed. The fraudster must either steal the check between the point where it is signed and the point where it is delivered, or they must re-route the check, causing it to be delivered to a location where they can retrieve it. The manner used to steal a check depends largely upon the way the company handles outgoing disbursements. Anyone who is allowed to handle signed checks might be able to intercept them.

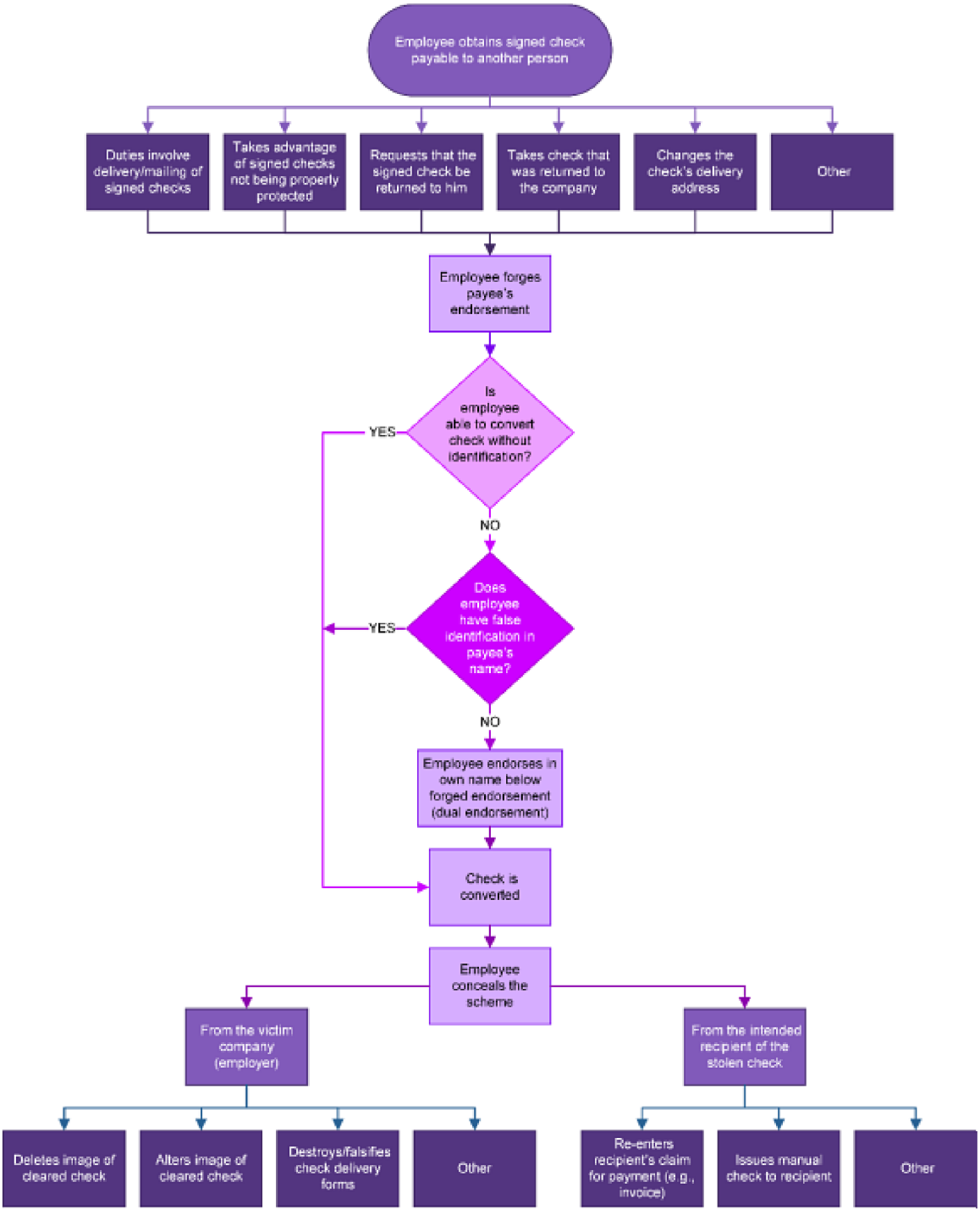
INTERCEPTING CHECKS BEFORE DELIVERY

EMPLOYEES INVOLVED IN DELIVERY OF CHECKS

Obviously, the employees who can intercept signed checks are those whose duties include the handling and delivery of signed checks. The most obvious example is a mailroom employee who opens outgoing mail containing signed checks and steals the checks. Other personnel who have access to outgoing checks might include accounts payable employees, payroll clerks, and administrative assistants.

POOR CONTROL OF SIGNED CHECKS

Unfortunately, employees are often able to intercept signed checks because of poor internal controls. For instance, many employees find signed checks left unattended in the work areas of the individuals who signed them or the people charged with their delivery. In these cases, it is easy for the perpetrator to steal the check. Another common breakdown occurs when the person who prepares a check is also involved in the delivery of that check once it has been signed.



Forged Endorsement Schemes

EXAMPLE

A high-level manager with authority to disburse employee benefits instructed accounts payable personnel to return signed benefits checks to them instead of immediately delivering the checks to the intended recipients. These instructions were not questioned due to the manager's level of authority within the company. The perpetrator took the returned checks and deposited them into their personal bank account, forging the endorsements of the intended payees.

In addition to the preceding example, administrative assistants or clerks who prepare checks for their bosses to sign are often responsible for mailing those checks. It is very simple for those employees to write a fraudulent check and obtain a signature, knowing that the boss will give the signed check right back to them. This scheme is indicative of the main problem with occupational fraud: trust. For an office to be efficient, high-level employees must be able to rely on their subordinates. Yet this reliance is precisely why subordinates can defraud their employer.

THEFT OF RETURNED CHECKS

Checks that have been mailed and are later returned to the victim for some reason, such as an incorrect address, are often targeted for theft by fraudsters. Employees with access to incoming mail can intercept these returned checks and convert them by forging the intended payee's endorsement.

EXAMPLE

A manager took and converted approximately $130,000 worth of checks that were returned due to noncurrent addresses (also stealing outgoing checks, cashing them, and then declaring them lost). The fraudster was well known at their bank and was able to convert the checks by claiming that they were doing it as a favor for the real payees, who were "too busy to come to the bank." The fraudster was able to continue with the scheme because the nature of their company's business was such that the recipients of the misdelivered checks were often not aware that the victim company owed them money. Therefore, they did not complain when their checks failed to arrive. In addition, the perpetrator had complete control over the bank reconciliation, so they could issue new checks to those payees who did complain and then force the reconciliation, making it appear that the bank balance and book balance matched when they did not.

RE-ROUTING THE DELIVERY OF CHECKS

Employees might also misappropriate signed checks by altering the addresses to which those checks are mailed. These perpetrators usually replace the payee's legitimate address with an address where the employee can retrieve the check, such as the employee's home or a post office box the employee controls. In other instances, the perpetrator might purposely misaddress a check so that it will be returned as undeliverable. The employee steals the check after it is returned to the victim organization.

Obviously, proper separation of duties should preclude anyone who prepares disbursements from being involved in their delivery. Nevertheless, the person who prepares a check is often allowed to address and mail it as well. In some instances where proper controls are in place, employees are still able to cause the misdelivery of checks.

EXAMPLE

A clerk in the customer service department of a mortgage company oversaw changing the mailing addresses of property owners. They were assigned a password that gave them access to make these changes. The clerk was transferred to a new department where one of their duties was the issuance of checks to property owners. Unfortunately, their supervisor forgot to cancel the clerk's old password. When the clerk realized this oversight, they would request a check for a certain property owner and then sign onto the system with the old password to change the address of that property owner so that the check would be sent to their own address. The next day, the employee would use their old password to re-enter the system and replace the proper address so that there would be no record of where the check had been sent. This fraudster's scheme resulted in a loss of over $250,000 to the victim company.

CONVERTING THE STOLEN CHECK

Once a check has been intercepted, the perpetrator can cash it by forging the payee's signature, hence the term *forged endorsement scheme*. Depending on where they try to cash the check, the perpetrator might or might not need fake identification at this stage. If a perpetrator is required to produce identification to cash their stolen check, and if they do not have a fake ID in the payee's name, they might use a dual endorsement to cash or deposit the check. In other words, the perpetrator forges the payee's signature as though the payee had transferred the check to them, and then the perpetrator endorses the check in their own name and converts it. When the bank statement is reconciled, dual endorsements on checks should always raise suspicions, particularly when the second signer is a company employee.

Altered Payee Schemes

The second type of intercepted check scheme is the altered payee scheme. This is a form of check tampering in which an employee intercepts a company check intended for a third party and alters the payee designation so that the employee or an accomplice can convert the check. (See the "Altered Payee Schemes" flowchart that follows.) The employee inserts their own name, the accomplice's name, or a fictitious entity's name on the check's payee line. The alteration makes the check payable to the employee (or an accomplice), so there is no need to forge an endorsement and no need to obtain false identification.

ALTERING CHECKS PREPARED BY OTHERS: INSERTING A NEW PAYEE

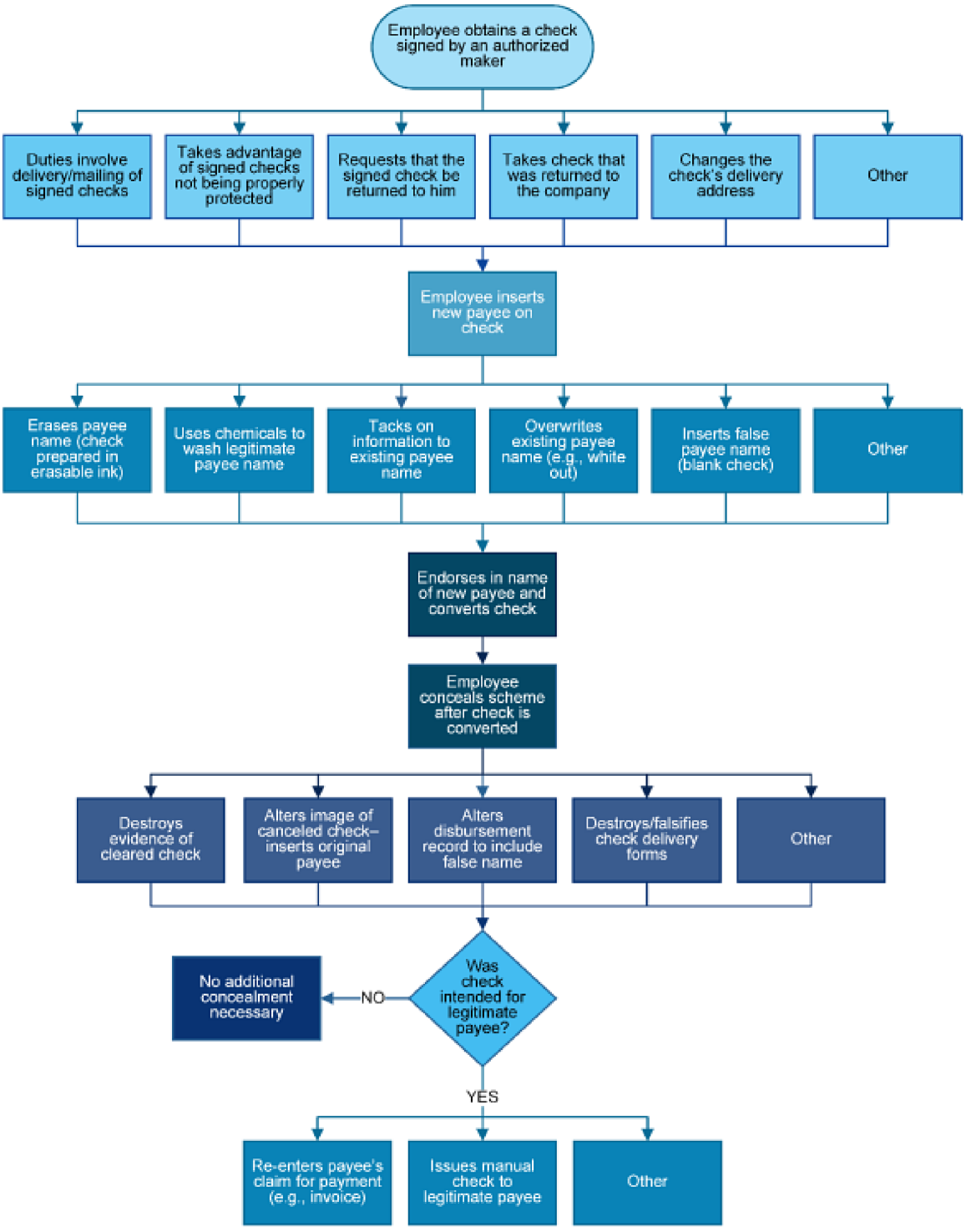
The method used to alter the payee designation on a check depends largely on how that check is prepared and intercepted. (Incidentally, the *amount* of the check might also be altered at the same time and by the same method as the payee designation.) Checks prepared by others can be intercepted by any of the methods discussed in the forged endorsements section. When the perpetrator intercepts a check that has been prepared by someone else, there are basically two methods that can be employed to change the payee. The first is to insert the false payee's name in place of the true payee's name. The true name might be scratched out with a pen or covered up with correction fluid. Another name is then entered on the payee designation line. These kinds of alterations are usually simple to detect.

A more sophisticated method occurs when the fraud perpetrator enters the accounts payable system and changes the payees' names before checks are generated. Anyone with a password that permits access to the accounts payable address file can accomplish this.

EXAMPLE

An accounts payable employee was so trusted that they were allowed to use the manager's computer password when the manager was out of the office. The password permitted access to the accounts payable address file. This employee waited until the manager was absent to select a legitimate vendor with whom the company did a lot of business. The employee stalled the vendor's invoices for the day and used the manager's log-in code to change the vendor name and address to that of a fictitious company after work. The new name and address were submitted into the accounts payable cycle with an old invoice number, causing a fraudulent check to be issued. The victim company had an automated duplicate invoice test, but the perpetrator circumvented it, substituting "1" for "I" and "0" (zero) for capital "O." The next day, the employee would replace the true vendor's name and address and manipulate the

check register so that the check payable to the fictitious vendor was concealed. Approximately $300,000 in false checks was issued using this method.



Altered Payee Schemes

ALTERING CHECKS PREPARED BY OTHERS: TACKING ON

The other method that can be used by perpetrators to alter checks prepared by others is tacking on additional letters or words to the end of the real payee designation. For instance, checks payable to "ABC" company might be altered to read "A.B. Collins." The employee then cashes the checks in the name of A.B. Collins. In these cases, the simple inclusion of a filler line after the payee designation would prevent the loss.

In addition to altering the payee designation, the amount of the check can be altered by tacking on extra numbers if the person preparing the check is careless and leaves space for extra numbers in the amount section of the check.

ALTERING CHECKS PREPARED BY THE FRAUDSTER: ERASABLE INK

When the perpetrator prepares the check that is to be altered, the schemes tend to be a bit more sophisticated. The reason for this is obvious: If the perpetrator can prepare the check themselves, the perpetrator can prepare it with the thought of how the payee designation will be changed. One of the most common ways to prepare a check for alteration is to write or type the payee's name (and possibly the amount) in erasable ink. After an authorized maker signs the check, the perpetrator retrieves the check, erases the payee's name, and inserts their own name.

EXAMPLE

A bookkeeper printed small checks to a local supplier and had the company's owner sign them. The bookkeeper then put the checks back in the printer so that they could alter the payee and check amount. For instance, the owner might sign a $10 check that later became a $10,000 check. These checks were entered in the disbursements journal as payments for aggregate inventory to the company's largest supplier, who received several large checks each month. The bookkeeper stole over $300,000 from their employer in this scheme.

Where a proper separation of duties is in place, a person who prepares a check should not be permitted to handle the check after it has been signed. Nevertheless, this is exactly what happens in most altered payee schemes. The person who prepares the check knows that the maker of the check will return it to them after it has been signed.

ALTERING CHECKS PREPARED BY THE FRAUDSTER: BLANK CHECKS

The most egregious example of poor controls in the handling of signed checks is one in which the perpetrator prepares a check, *leaves the payee designation blank*, and submits it to an

authorized maker who signs the check and returns it to the employee. Obviously, this makes it quite easy for the perpetrator to designate themselves or an accomplice as the payee. Common sense should prevent anyone from giving a signed, blank check to another person. Nevertheless, this is a common occurrence, especially when the perpetrator is a trusted long-time employee.

CONVERTING ALTERED CHECKS

As with all other types of fraudulent checks, conversion is accomplished by endorsing the checks in the payee's name. Conversion of fraudulent checks has been discussed in previous sections and will not be re-examined here.

Authorized Maker Schemes

The final check tampering scheme, the authorized maker scheme, might be the most difficult to defend against. An authorized maker scheme occurs when an employee with signature authority on a company account writes fraudulent checks for their own benefit and signs their own name as the maker. (See the "Authorized Maker Schemes" flowchart that follows.) Perpetrators in these schemes can write and sign fraudulent checks themselves. They do not have to alter a pre-prepared document or forge the maker's signature.

OVERRIDING CONTROLS THROUGH INTIMIDATION

When a person is authorized to sign company checks, preparing the checks is easy. The employee writes and signs the documents the same way they would with any legitimate check. In most situations, check signers are owners, officers, or otherwise high-ranking employees and thus have or can obtain access to all the blank checks they need. Even if company policy prohibits check signers from handling blank checks, the perpetrator can normally use their influence to overcome this impediment. What employee is going to tell the chief executive officer (CEO) that they cannot have a blank check?

The most basic way an employee accomplishes an authorized maker scheme is to override controls designed to prevent fraud. Most authorized signatories have high levels of influence within their companies. The perpetrators use this influence to deflect questions about fraudulent transactions.

A common authorized maker scheme is one in which a majority owner or sole shareholder uses their company to pay personal expenses directly out of company accounts. Instead of paying personal expenses, the perpetrator might write checks directly to themselves, their

friends, or their family. Using fear of job security as a weapon, the owner can maintain a work environment in which employees are afraid to question these transactions.

High-level managers or officers might also use their authority to override controls in companies with absent or inattentive owners. Intimidation can play a large part in the commission and concealment of occupational fraud schemes involving powerful individuals.

EXAMPLE

The manager of a sales office stole approximately $150,000 from their employer over a two-year period. This manager had primary check-signing authority and abused this power by writing company checks to pay their personal expenses. The manager's fraudulent activities were well known by certain members of the staff, but these employees' careers were controlled by the perpetrator. Fear of losing their jobs combined with lack of a proper whistleblowing structure prevented the manager's employees from reporting the fraud.

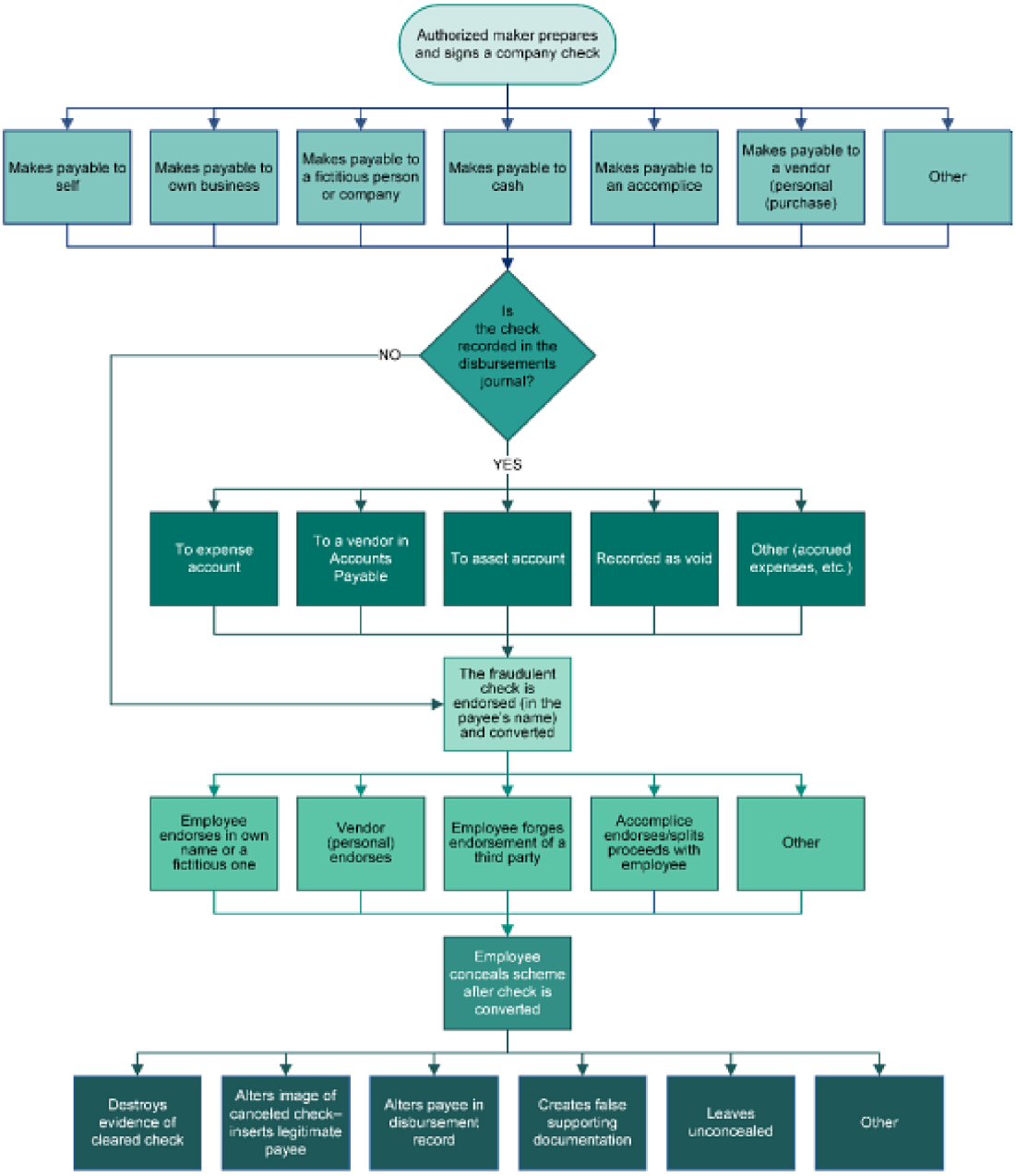
POOR CONTROLS

Although overriding controls is the most obvious way to execute an authorized maker scheme, it is not the most common. Far more of these schemes occur because no one is paying attention to the accounts and few controls are present to prevent fraud. Some employees who write checks to themselves or to purchase items for themselves code the checks to expense accounts that they know are not likely to be reviewed.

The failure to closely monitor accounts is supplemented by lack of internal controls, specifically the absence of separation of duties in the cash disbursement process. Employees who commit authorized maker fraud are often those reconciling the business's bank accounts. This is especially common in small businesses. Therefore, employees with total control over the disbursement process can easily write fraudulent checks for their own benefit.

EXAMPLE

The bookkeeper of a medium-sized company was charged with paying all bills and preparing the company payroll. They had access to an automatic check signer and total control over company bank accounts. The bookkeeper wrote extra checks in their own name, coded the expenditures to payroll, and destroyed the canceled checks when they were returned with the bank statement.



Authorized Maker Schemes

Concealing Check Tampering Schemes

Most check tampering schemes do not consist of a single occurrence; they continue over time. Therefore, concealing the fraud is arguably the most important aspect of the scheme. If an employee intended to steal a large sum of money and escape to another country, hiding the fraud might not be so important. But most occupational fraudsters remain employees of their companies as they continue to steal from them, which makes concealment critical to the crime.

Concealment of the fraud means not only hiding the criminal's identity, but also hiding the fact that a fraud has even occurred. The most successful frauds are those in which the victim organization is unaware that it is being robbed. Obviously, once a business learns that it is being victimized, it will take steps to find the source and put a stop to the scheme.

Check tampering schemes can present especially complex concealment problems for dishonest employees. In other types of fraudulent disbursements, such as invoice or payroll schemes, someone other than the perpetrator enters the fraudulent payment in the books as a legitimate transaction. The payments in those schemes are generated by the production of false documents that cause accounts payable personnel to think that money is owed to a particular person or vendor. When accounts payable issues a disbursement for a fake invoice, it does so because it believes the invoice to be genuine. The payment is then entered in the books as a legitimate payment. In other words, the perpetrator generally does not have to worry about concealing the payment in the books because someone else unintentionally does it for them. But in forgery and authorized maker schemes, the perpetrator is the one writing the check, and they are usually the one coding the check in the disbursements journal. They must "explain" the check on the books.

Forged endorsement schemes and altered payee schemes are different because they involve the alteration of checks that were already prepared and coded by someone else. Nevertheless, they create a problem for the perpetrator because the intercepted check was intended for a legitimate recipient. Someone is out there waiting for the check that the perpetrator has taken. The culprit in these schemes must worry not only about hiding the fraud from their employer but also about appeasing the intended payee.

THE FRAUDSTER RECONCILING THE BANK STATEMENT

A large percentage of those who perpetrate check tampering frauds are involved in reconciling the company's bank statement. The bank statement that a company receives normally includes the canceled checks that have been cashed in the preceding period. A person who reconciles the accounts is therefore able to hide the existence of any fraudulent checks they have written to themselves. They can remove the fraudulent checks, alter the bank statement, or both.

In forged maker and authorized maker schemes, the perpetrator usually must code the check in the disbursements journal. The most basic way to hide the check is to code it as void or to include no listing at all in the journal. Then, when the bank statement arrives, perpetrators

remove the fraudulent check from the returned checks and destroy it or alter the bank statement. Now there is no record of the payment in the journal and no physical evidence of the check. Of course, the bank will have a copy of the check, but unless someone questions the missing check, it is unlikely that the company will discover the problem. And since the perpetrator is the one who reconciles the account, it is unlikely that anyone will even notice that the check is missing.

The problem with omitting the fraudulent check from the disbursements journal is that the bank balance will not reconcile to the book balance. For instance, if the perpetrator wrote a $25,000 check to themselves and did not record it, then the book balance will be $25,000 higher than the bank balance ($25,000 was taken out of the bank account by the perpetrator, but it was not credited out of the company's cash account). Perpetrators usually omit their illegal checks from the disbursements journal only in situations in which they personally reconcile the bank statement and no one reviews their work, thus allowing fraudsters to force the reconciliation. In other words, fraudsters report that the bank balance and book balance match when in fact they do not.

Some victim organizations do not regularly reconcile their accounts. This makes it easy for employees to write checks without recording them. In a system in which controls are so lax, almost any concealment method will be effective to disguise fraud. In fact, it might not be necessary to make any effort at all to conceal the crime.

Some fraudsters physically alter the bank statement to cause it to match the company's book balance. For instance, a person engaging in a forged maker scheme might decide to steal blank checks from the bottom of the check stock. These checks are out of sequence and therefore will be listed last on the bank statement. This employee can delete the clump of fraudulent checks at the end of the statement and alter the balance to match the victim company's books.

RE-ALTERATION OF CHECKS

In altered payee schemes, remember that it is common for the perpetrator to take a check intended for a legitimate recipient and then alter the check so that the perpetrator becomes the designated payee. But a canceled check payable to an employee will obviously raise suspicions of fraud. Therefore, some employees re-alter their fraudulent checks when the bank statement arrives. It has been previously discussed how employees can alter checks by writing the payee's name in erasable ink when the check is prepared. These employees obtain

a signature for the check and then erase the true payee's name and insert their own. When the fraudulent checks return with the bank statement, the employee erases their own name and re-enters the proper payee's name. Thus, there will be no appearance of mischief.

MISCODING FRAUDULENT CHECKS

Rather than omit a fraudulent check from the disbursements journal or list it as void, perpetrators might write a check payable to themselves but list a different person as the payee on the books. Usually, the fake payee is a regular vendor—a person or business that receives numerous checks from the victim company. Employees tend to pick known vendors for these schemes because one extra disbursement to a regular payee is less likely to be noticed than a check to an unknown person.

The fraudster can also conceal a fraudulent check by overstating the amounts of *legitimate* disbursements in the journal to absorb a fraudulent check's cost. For instance, assume that a company owes $10,000 to a particular vendor. The fraudster would write a check to the vendor for $10,000 but would enter the check in the disbursements journal as a $15,000 payment. The company's disbursements are now overstated by $5,000. The fraudster can write a $5,000 check to themselves and list that check as void in the disbursements journal. The bank balance and the book balance will still match because the cost of the fraudulent check was absorbed when the amount of the legitimate check was overstated. Of course, the fact that the canceled checks do not match the entries in the journal should indicate potential fraud. This type of concealment is only effective when the bank accounts are not closely monitored or where the employee oversees reconciling the accounts.

If possible, fraudsters will try to code their fraudulent checks to existing accounts that are rarely reviewed or to accounts that are very active. Most of these checks are coded to expense accounts or liability accounts. This method can be very effective in concealing fraud, particularly when the victim company is not diligent in reconciling its bank accounts. For instance, some organizations reconcile their accounts by cross-referencing check numbers with the amounts of the checks, but they do not verify that the payee on the actual check matches the payee listed in the disbursements journal. These organizations will be unable to detect checks that have been coded to the wrong payee in the disbursements journal.

RE-ISSUING INTERCEPTED CHECKS

In intercepted check schemes, the fraudster faces detection not only through their employer's normal control procedures but also by the intended recipients of the stolen checks. When the

real payees do not receive their checks, they are likely to complain. These complaints, in turn, could trigger a fraud investigation. One way for a fraudster to avoid this problem is to issue new checks to the intended payees.

EXAMPLE

An accounts payable troubleshooter oversaw auditing payments to all suppliers, reviewing supporting documents, and mailing checks. Occasionally, they would purposely fail to mail a check to a vendor. The vendor, of course, called accounts payable about the late payment and was told that the invoice had been paid on a certain date. Since accounts payable did not have a copy of the canceled check (because the fraudster was still in possession of it), it would call the troubleshooter to research the problem. Unfortunately for the company, the troubleshooter was the one who had stolen the check and told accounts payable to issue another check to the vendor while they stopped payment on the first check. Thus, the vendor received their payment, and instead of stopping payment on the first check, the troubleshooter deposited it into their own account.

FRAUDULENT SUPPORTING DOCUMENTS

Whereas some perpetrators attempt to wipe out all traces of their fraudulent disbursements by destroying the checks or forcing the bank reconciliation, others opt to justify their checks by manufacturing fake support for them. These individuals prepare false payment vouchers, including false invoices, purchase orders, or receiving reports, to create an appearance of authenticity. This concealment strategy is only practical when the employee writes checks payable to someone else (such as an accomplice or a shell company). A check made payable to an employee might raise suspicions regardless of any supporting documents that they manufacture.

Detection of Check Tampering Schemes

ACCOUNT ANALYSIS THROUGH CUT-OFF STATEMENTS

Bank cut-off statements should be requested for 10 to 15 days after the balance sheet's closing date. These statements may be used to detect cash fraud during periods between monthly bank statements. Auditors often use cut-off statements to ensure that income and expenses are reported in the proper period. If employees know that a cut-off statement might be ordered at any time during the month and reviewed independently, cash fraud will be less likely.

A cut-off statement is generally ordered from the bank, delivered unopened to the auditor (or outsider), and reconciled. It can be ordered at any time during the accounting cycle. If cut-off bank statements are not ordered or received, obtain the following period bank statement and perform account analysis and investigation.

BANK RECONCILIATIONS

Copies of the bank reconciliations and account analysis should be obtained along with the complete set of bank statements on all checking and savings accounts, as well as certificates of deposit (CDs) and other interest-bearing and non-interest-bearing accounts. From the reconciliations, perform the following tests:

- Confirm the mathematical accuracy of the reconciliation.
- Examine the bank statement for possible alterations.
- Trace the balance on the statement back to the bank cut-off and bank confirmation statements.
- Compare the sum of the balance to the company's ledger.
- Trace the deposits in transit to the bank cut-off statement to ensure recording in the proper period.
- Examine canceled checks and compare them to the list of outstanding checks.
- Sample supporting documentation of checks written for a material amount.
- Verify supporting documentation on outstanding checks written for a material amount.
- Verify accuracy of nonoperational-cash or cash-equivalent accounts (CDs and other investment accounts). Analysis should include the verification of the institution holding the funds, interest rate, maturity date, beginning and ending balances, and current period activity. Book and bank balances should be compared and any accruals of interest analyzed.

BANK CONFIRMATION

Another method related to the cut-off statement is the bank confirmation request. Unlike the cut-off statement, this detection method is merely a report of the balance in the account as of the date requested. This balance should be requested to confirm the statement balance, as well as any other necessary balance date. If fraud is occurring at the bank reconciliation stage, this independent confirmation might prove to be very helpful.

CHECK TAMPERING RED FLAGS

The following irregularities might indicate fraud:

- Voided checks might indicate that employees have embezzled cash and charged the embezzlement to expense accounts. When the expense is paid (from accounts payable), fraudulent checks are marked and entered as void and removed from distribution points. An account-balancing journal entry is then made. The list of voided checks should be verified against physical copies of the checks. Bank statements should be reviewed to ensure that voided checks have not been processed.
- Missing checks might indicate lax control over the physical safekeeping of checks. Stop payments should be issued for all missing checks.
- Checks payable to employees, with the exception of regular payroll checks, should be closely scrutinized. Such an examination might indicate other schemes, such as conflicts of interest, fictitious vendors, or duplicate expense reimbursements.
- Altered endorsements or dual endorsements of returned checks might indicate possible tampering.
- Returned checks with obviously forged or questionable signature endorsements should be verified with the original payee.
- Altered payees on returned checks should be verified with the intended payee.
- Duplicate or counterfeit checks more than likely indicate fraud. These checks might be traceable to the depositor through bank check coding.
- An examination of all cash advances might reveal that not all advances were properly documented and, therefore, inappropriate payments have been made to employees.
- A questionable payee or payee address on a check should trigger review of the corresponding check and support documentation.

Prevention of Check Tampering Schemes

CHECK DISBURSEMENT CONTROLS

The following list of activities will help tighten controls and possibly deter employees from giving in to the temptation to commit check fraud.

- Check "cutting" and preparation is not done by a signatory on the account.
- Checks are mailed immediately after signing.
- Theft control procedures are adhered to.
- Accounts payable records and addresses are secure from possible tampering. Changes in vendor information should be verified.
- Bank statements should be reviewed diligently to ensure that amounts and signatures have not been altered.
- Bank reconciliations should be completed immediately after monthly statements are received.

- Bank reconciliations are not performed by signatories on the account.
- Bank statements should be reconciled and reviewed by more than one person.
- Appropriate separation of duties should be documented and adhered to.
- Detailed comparisons are routinely made between check payees and the payees listed in the cash disbursements journal.
- Personnel responsible for handling and coding checks are periodically rotated, keeping total personnel involved to a minimum.

BANK-ASSISTED CONTROLS

Companies should work in a cooperative effort with banks to prevent check fraud. Consider the following control measures that might be taken regarding a firm's checking accounts.

- Establish maximum amounts above which the company's bank will not accept checks drawn against the account.
- Use positive pay banking controls. Positive pay allows a company and its bank to work together to detect fraudulent items presented for payment. The company provides the bank with a list of checks and amounts that are written each day. The bank verifies items presented for payment against the company's list and rejects items that are not on the list. Investigations are conducted as to the origin of the unlisted items.

PHYSICAL TAMPERING PREVENTION

The following list details check tampering prevention techniques that are being used today by some institutions to secure businesses' check integrity. These methods can be used individually or in combination.

- Signature line void safety band—The word *VOID* appears on the check when photocopied.
- Rainbow foil bar—A horizontal colored bar placed on the check fades and is shaded from one bar to the next. Photocopied foil bars appear solid.
- Holographic safety border—Holographic images are created in a way that reflects light to reveal a three-dimensional graphic.
- Embossed pearlescent numbering—Checks are numbered using a technique that is revealed by a colored highlighter pen or by a bright light held behind the check.
- Other chemical voids—Checks reveal an image or the word *VOID* when treated with an eradicator chemical.
- Micro line printing—Extremely small print is too small to read with the naked eye and becomes distorted when photocopied.

- High-resolution microprinting—Images are produced on the check in high resolution. This technique is very difficult to reproduce.
- Security inks—Checks contain inks that react with eradication chemicals, reducing a forger's ability to modify the check.
- Watermark backers—Hidden images can only be seen when the check is held at an angle. This image is very difficult to reproduce.

CHECK THEFT CONTROL PROCEDURES

It is very important to provide internal controls that will minimize the possibility of check tampering and theft. The following is a list of items that should be incorporated into companies' policies and procedures to help deter check tampering.

- New checks should be purchased from reputable, well-established check producers.
- Unused checks should be stored in a secure area, such as a safe, vault, or other locked area. Security to this area should be restricted to authorized personnel only. Routinely change keys and access codes to storage areas.
- Review all hiring procedures. One of the most important means of fighting fraud is to not hire people with questionable backgrounds. Develop a distinct separation of duties in the accounts payable department, including written policies and procedures for all personnel who have the opportunity to handle checks, from mailroom clerks to the CEO.
- Use electronic payment services to handle large vendor and financing payments, eliminating the use of paper checks.
- Report lost or stolen checks immediately.
- Properly and securely store canceled checks.
- Destroy unused checks for accounts that have been closed.
- Printed and signed checks should be mailed immediately after signing.

Electronic Payment Tampering

As businesses move to using electronic payments—such as ACH payments, online bill payments, and wire transfers—in addition to or instead of traditional checks, fraudsters are adapting their methods to manipulate these payments as well. Some of these fraudsters abuse their legitimate access to their employer's electronic payment system; these schemes are similar to traditional check tampering frauds carried out by authorized makers. Others gain access through social engineering, password theft, or by exploiting weaknesses in their employer's internal control or electronic payment system. Regardless of how they log in to the system, the dishonest employees use this access to fraudulently initiate or divert electronic payments to themselves or their accomplices.