The ACFE would like to thank Cotton—A Sikich Company for contributing this list of fraud risk exposures and descriptions.

Cotton
A SIKICH. COMPANY

FRAUD RISK EXPOSURES

The following table illustrates the types of fraud schemes and fraud exposures an organization might encounter. The exposures list can be used either as a starting point for a fraud risk assessment (does our organization need to be concerned about this exposure?) or as a final check once a fraud scheme list has been compiled by the risk assessment team. Click on the title to access a summary of the fraud scheme, fraud exposures, and source.

This list is intended to be expanded to cover new and emerging frauds. Suggestions for additions to this list will be welcomed. Email suggestions to FRMG@acfe.com.

Fraud Risk Exposure
Intentional Manipulation of Financial Statements:
Inappropriately Reported Revenues
Fictitious Revenues
Fraudulent Audit Confirmations
Re-Dating or Refreshing Receivables to Conceal Uncollectables
Manipulation of Promotional Allowances
Improper Adjustments to Estimates
Premature Revenue Recognition
Side Agreements
Bill and Hold
Channel Stuffing
Round-Trip Transactions
Altered or False Shipping Documents
Sell-Through Agreements
Up-Front Fees
Holding Accounting Periods Open
Failure to Record Sales Provisions or Allowances
Manipulating Percentage of Completion
Manipulating Estimated Costs to Complete
Inappropriately Reported Expenses
Improper Period Recognition of Expenses
Improper Use of Special Purpose Variable Interest Entities

Fraud Risk Exposure
Inappropriately Reflected Balance Sheet Amounts, Including Reserves
Improper Asset Valuation
"Refreshed" Receivables
Misstated Inventory Quantities or Values
Misstated Accounts Receivable
Misstated Merger and Acquisition Values
Improper Capitalization of Intangible Items
Changing or Manipulating Depreciation Methods
Failure to Recognize Impaired Assets
Unrealistic or Unsupported Estimates
Unrealistic or Unsupported Adjustments to Estimates
Misclassification of Assets
Manipulating the Value of Investments
Inappropriate Depreciation Methods
Recording Fictitious Assets
Concealed Liabilities and Expenses
Omission
Sales Returns and Allowances and Warranties
Unrecorded and Undisclosed Warranty Costs and Product-Return Liabilities
Capitalization of Operating Expenses
Tax Liability Manipulation
Off-Balance-Sheet Entities and Liabilities
Improper or Unjustified Consolidation Entries
Intercompany Manipulations
Sham Related-Party Transactions
Disclosure Frauds
Top-Side Entries/Adjustments
Inappropriately Approved and/or Masked Disclosures
Liabilities Omissions
Subsequent Events
Related-Party Transactions
Accounting Changes
Management Frauds Uncovered
Backdating Transactions
Cookie Jar Accounting/ Cookie Jar Reserves
Management Override

Fraud Risk Exposure
Concealing Misappropriation of Assets
Concealing Unauthorized Acquisition, Disposition, and Use of Assets
Misappropriation of Tangible Assets
Cash Theft
Sales Register Manipulation
Skimming
Understated Sales
Theft of Checks Received
Lapping
Collection Procedures
Check for Currency Substitution
False Entries to Sales Accounts
Inventory Padding
Theft of Cash from Register
Deposit Lapping
Deposits in Transit
Fraudulent disbursements
False Refunds
False Voids
Small Disbursements
Check Tampering
Billing Schemes
Personal Purchases with Company Funds
Returning Merchandise for Cash
Creation of False or Fictitious Vendors, Suppliers, or Subcontractors
False Shipments of Inventory and Other Assets
Payments for Services Not Received
Payroll Fraud
Ghost Employees
Failure to Remove Terminated Employees from Payroll
Falsified Hours and Salary or Pay Rate
Failure to Report Leave Taken
Commission Sales
Expense Reimbursement Fraud
Mischaracterized Expenses
Overstated Expenses

Fraud Risk Exposure
Fictitious Expenses
Multiple Reimbursements
Loan Fraud
Loans to Nonexistent Borrowers
Double Pledged Collateral
False Application Information
Construction Loans
Real Estate Fraud
False Appraisal Value
Fraudulent Appraisal
Wire Transfer Fraud
System Password Compromise
Forged Authorizations
False or Unauthorized Transfers from Internal Accounts
ATM Fraud
Check and Credit Card Fraud
Counterfeiting Checks
Check Theft
Stop Payment Orders
Unauthorized Use of a Lost or Stolen Card
Counterfeit Credit Cards
Mail Theft
Insurance Fraud
Cash, Loan, and Dividend Payments
Settlement Checks
Premium Diversion
Fictitious Payee
Fictitious Death Claim
Underwriting Misrepresentation
Vehicle Insurance — Staged Accidents
Vehicle Insurance — Inflated Damages
Rental Car Fraud
Pension Fraud
Inflated Final Income Used in Benefit Calculation
Under-Reported Income in Years Not Used for Benefit Calculation
False Service Reported for Service Purchase

Fraud Risk Exposure
Enrolling Ineligible Persons
Not Enrolling All Eligible Persons
Inventory Fraud
Off-Site or Fictitious Inventory
Purchasing and Receiving Falsification
Misuse of Inventory
Theft of Inventory
False Shipments
Concealing Inventory Shrinkage
Theft of Intellectual Property
Espionage
Spying
Informants
Infiltration
Loss of Information
Trash and Waste Disposal Searches
Surveillance
Destruction of Customer Goodwill
Compromising Vendor Relationships
Proprietary Business Opportunities
Corruption
Bribery and Illegal Gratuities
Commercial Bribery
Official Bribery/Bribery of Public Officials
Receipt of Bribes, Kickbacks, and Gratuities
Kickbacks
Overbilling Schemes
Illegal Payments: Gifts, Travel, Entertainment
Loans
Credit Card Payments for Personal Items
Transfers for Other than Fair Value
Favorable Treatment
Conflicts of interest
Purchases
Sales
Business Diversion

Fraud Risk Exposure
Resourcing
Financial Disclosure of Interest in Vendors/Suppliers
Bid Rigging
Embezzlement
False Accounting Entries
Unauthorized Withdrawals
Unauthorized Disbursements
Paying Personal Expenses from Bank Funds
Unrecorded Cash Payments
Theft of Physical Property
Moving Money from Dormant Accounts
Contract, Grant, and Procurement Fraud
Comingling of Contracts
Product Substitution
False or Inflated Invoices or Claims
Change Order Abuse
Cost Mischarging
Multiple Claims
Failure to Credit/Refund
Fraudulent Indirect Cost
Defective Manufacturing
Anti-Competitive or Anti-Trust Schemes
Bid-Rotation
Complementary Bidding
Market Sharing
Bid Suppression
Proposal Schemes
Altering/Changing Submission
Accepting Late Proposal
Unnecessary Rebidding
Limiting Days to Submit
Unnecessary Pre-Qualification Criteria
Unbalanced Proposal
Scoring Proposal
Contract Specifications/Requirements Schemes (Excluding/Including Bidders)
Narrowing Requirements

Fraud Risk Exposure
Narrowing Specifications
Broadening Requirements
Broadening Specifications
Advertisement Schemes (Limiting Competition)
Inadequate or Vague Publication Synopsis
Using Obscure Publications
Advertisement During Holiday
Limiting Days to Advertise
False Representation Schemes
False Statement/Certification
Defective Pricing
Progressive Payment
Purchasing Schemes
Purchases for Personal Use or Resale
Purchase in Excess
Split Purchases
Unnecessary Purchases
Pass-through Purchases
Phantom Vendor
Leaking of Acquisition
Unjustified Sole Source
Manipulation of Delivery
Influence through Authority
Foreign Corrupt Practices Act (FCPA) Violations
Anti-Bribery Provisions
Books and Records Violations
Internal Control Weaknesses
Money Laundering
False Statements
Aiding and Abetting Fraud by Other Parties (Customers, Vendors)
Insider Trading
Health Care Fraud
Home Health Agency Billing Schemes
Durable Medical Equipment (DME) Billing Schemes
Speech Therapy Billing Schemes
Addiction Treatment Billing Schemes

Fraud Risk Exposure
Time & Effort Reporting Schemes
Kickback Cover-up Schemes
“Rent-a-Patient” Schemes
Recruited Patient Schemes
Patient Brokering Schemes—Opiod Addiction Treatment
Kickback Schemes Concealed/Disguised Through Office Rentals
Kickback Schemes Concealed/Disguised Through In-Office Pharmacy Dispensing, Rental Agreements, Consulting Fees, and So Forth
Pharmacy Fraud
Pharmacy Fraud: Kickback Law
Pharmacy Fraud: Best Price Rule Fraud
Pharmacy Fraud: Inflated Pricing Fraud
Pharmacy Fraud: Good Manufacturing Practices
Pharmacy Fraud: Pharmacy Benefit Manager Fraud
Home Healthcare Fraud
Durable Medical Equipment Fraud
Medical Device Fraud
Medical Coding Fraud
Lab Services Fraud
Medically Unnecessary Services Fraud
Medicare Part D Plan Fraud
Anti-Kickback Act Fraud
Stark Act Fraud
Off Label Marketing Fraud
Tainting the Doctor/Patient Relationship Through Illicit Financial Agreements
Upcoding/Unbundling CPT Codes
Billing for services not rendered
Falsification of Medical Records

The following table illustrates the types of fraud schemes and fraud exposures an organization might encounter. This listing is not meant to be all-inclusive, but rather, to support an initial assessment for an organization to identify areas vulnerable to fraud. This list can serve as a starting point for the risk assessment process; or as a final check following the risk assessment process. By reviewing this list and asking, "could this happen in our organization," the assessment team will gain an overview understanding of potential fraud risks. More focus will be needed to identify the organization's specific industry, location, and cultural factors that can influence other fraudulent behavior.

Fraud Risk Exposure and Description
Intentional Manipulation of Financial Statements "Fraud in financial statements typically takes the form of: • Overstated assets or revenue • Understated liabilities and expenses Overstating assets or revenue falsely reflects a financially stronger company by inclusion of fictitious asset costs or artificial revenues. Understated liabilities and expenses are shown through exclusion of costs or financial obligations. Both methods result in increased equity and net worth for the company. This manipulation results in increased earnings per share or partnership profit interests, or a more stable picture of the company's true situation. However, in some cases, financial statement fraud takes the opposite form: • Assets and revenues are understated • Liabilities and expenses are overstated To demonstrate the over- and understatements typically used to fraudulently enhance the financial statements, the schemes have been divided into five classes. Because the maintenance of financial records involves a double-entry system, fraudulent accounting entries always affect at least two accounts and, therefore, at least two categories on the financial statements. While the following areas reflect their financial statement classifications, keep in mind that the other side of the fraudulent transaction exists elsewhere. The five classifications of financial statement schemes are: • Fictitious revenues • Timing differences (including improper revenue recognition) • Improper asset valuations • Concealed liabilities and expenses • Improper disclosures" (p. 1.210).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Inappropriately Reported Revenues
Fictitious Revenues "Fictitious or fabricated revenues involve the recording of sales of goods or services that did not occur. Fictitious sales most often involve fake customers, but can also involve legitimate customers. For example, a fictitious invoice can be prepared (but not mailed) for a legitimate customer even though the goods are not delivered or the services are not rendered. At the end of the accounting period, the sale will be reversed, which will help conceal the fraud. However, the artificially high revenues of the period might lead to a revenue shortfall in the new period, creating the need for more fictitious sales. Another method is to use legitimate customers and artificially inflate or alter invoices to reflect higher amounts or quantities than are actually sold. The challenge with both of these methods is balancing the other side of the entry. A credit to revenue increases the revenue account, but the corresponding debit in a legitimate sales transaction typically either goes to cash or accounts receivable. Since no cash is received in a fictitious revenue scheme, increasing accounts receivable is the easiest way to get away with recording the entry. However, accounts receivable stay on the books as an asset until they are collected. If the outstanding accounts never get collected, they will eventually need to be written off as bad debt expense. Mysterious accounts receivable on the books that are long overdue are a common sign of a fictitious revenue scheme." (p. 1.213). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Fraudulent Audit Confirmations "Fraudulent audit confirmations can impact all types of accounts or transactions that are confirmed with third parties (sales, cash, accounts receivables, debt, liabilities, etc.). Schemes may involve collusion with third parties who receive the audit confirmations or may involve the company providing the auditors with false contact information (false mailing addresses, fax numbers, phone numbers, etc.) so that confirmations are diverted to co-conspirators involved in the scheme." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table

Fraud Risk Exposure and Description
Re-Dating or Refreshing Receivables to Conceal Uncollectables "In order to mask rising account receivable balances (including known or suspected uncollectible balances) while avoiding increasing the bad debt provision, a company may "refresh" the aging of receivables and improperly represent A/R balances as being current in nature instead of showing the true age of the receivables. This may occur with exchange transactions with customers, where customers can receive "credits" to their accounts and allowed to repurchase goods where little, if any, physical transfer of merchandise occurs. Some schemes may simply modify or edit dates of invoices in the A/R system that results in a "restart" of the aging process for the modified receivables. Schemes may involve the falsification or improper modification of accounting documentation (invoices, purchase orders, change orders, shipping reports, etc.) to cover up the fraud scheme." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Manipulation of Promotional Allowances "Promotional allowances may be provided as rebates, incentives, or other credits to buyers/customers as an incentive to purchase products. Allowances may take the form of volume discounts, reimbursements for special handling, co-advertising reimbursements, slotting fees, etc. Often promotional allowances are based on future events (such as purchase volumes over a specified period of time, future advertising costs, etc.) and often require considerable estimates that may be manipulated or biased. Some schemes involve the early recognition of revenue on up-front fees collected or the failure to accrue for rebates or credits that are likely to be earned by the buyer. Other fraud schemes involve fraudulent financial reporting and the misclassification of credits on the income statement. " [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Improper Adjustments to Estimates "Estimates are common throughout the accounting process and can be manipulated to impact revenues, expenses, asset valuations, and/or liabilities. Management is often in a position where it can influence or bias estimates. Common fraud schemes involve the reduction of accruals or reserves in order to increase earnings in the current period, and may involve the earlier creation of excess reserves or "cookie-jar reserves" when the company was in a financial position to create a "cushion" against future losses." [**Source:** Deloitte, Sample Listing of Fraud Schemes]

Fraud Risk Exposure and Description
Return to Table
Premature Revenue Recognition "Financial statement fraud might also involve timing differences—that is, the recording of revenues or expenses in improper periods. This can be done to shift revenues or expenses between one period and the next, increasing or decreasing earnings as desired. This practice is also referred to as income smoothing." (p. 1.216). "Under current U.S. GAAP revenue recognition standards, revenue is recognized when it is (1) realized or realizable and (2) earned. The Securities and Exchange Commission (SEC) issued Staff Accounting Bulletin (SAB) Topic 13, Revenue Recognition (now codified in FASB ASC 605-10-S99), to provide additional guidance on revenue recognition criteria and to rein in some of the inappropriate practices that had been observed. This guidance states that revenue is typically considered realized or realizable and earned when all of the following criteria are met: • Persuasive evidence of an arrangement exists. • Delivery occurs or services are rendered. • The seller's price to the buyer is fixed or determinable. • Collectability is reasonably assured. In general, revenue should be recognized in the accounting records when a sale is complete—that is, when title is passed from the seller to the buyer. This transfer of ownership completes the sale and is usually not final until all obligations surrounding the sale are complete and the four criteria set out in FASB ASC 605 have been satisfied." (p. 1.217). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Premature Revenue Recognition: Side Agreements "Sales terms and conditions may be modified, revoked, or otherwise amended outside of the recognized sales process or reporting channels and may impact revenue recognition. Common modifications may include granting of rights of return, extended payment terms, refund, or exchange. Sellers may provide these terms and conditions in concealed side letters, e-mails, or in verbal agreements in order to recognize revenue before the sale is complete. In the ordinary course of business, sales agreements can and often are legitimately amended, and there is nothing wrong with

Fraud Risk Exposure and Description
giving purchasers a right of return or exchange, as long as revenue is recognized in the proper accounting period with appropriate reserves established." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Bill and Hold "A bill and hold transaction takes place when products have been booked as a sale but delivery and transfer of ownership has not occurred as of the date the sale is recorded. The transaction may involve a legitimate sales or purchase order; however, the customer is not ready, willing, or able to accept delivery of the product at the time the sale is recorded. Sellers may hold the goods in its facilities or may ship them to different locations, including third-party warehouses." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Channel Stuffing "A challenging area of revenue recognition is channel stuffing. This term refers to the sale of an unusually large quantity of a product to distributors who are encouraged to overbuy through the use of deep discounts or extended payment terms. This practice is especially attractive to industries with high gross margins—such as tobacco, pharmaceuticals, perfume, soda concentrate, and branded consumer goods—because it can increase short-term earnings. On the downside, however, stealing from future periods' sales makes it harder to achieve sales goals in those future periods. The pressure to meet sales goals can, in turn, lead to increasingly disruptive levels of channel-stuffing and, ultimately, to a restatement. Although orders are received, the terms of the order might raise questions about the collectability of the accounts receivable, and any existing side agreements that grant a right of return might, effectively, turn the sales into consignment sales. Also, there might be a greater risk of returns for certain products if they cannot be sold before their shelf life ends." (p. 1.221). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Premature Revenue Recognition: Round-Trip Transactions "Recording transactions that occur between two or more companies for which there is no business purpose or economic benefit to the companies involved. These transactions are often entered into for the purpose of inflating revenues or creating the appearance of strong sales growth. Transactions may

Fraud Risk Exposure and Description
include sales between companies for the same amount within a short time period, or they may involve a loan to or investment in a customer so that the customer has the ability to purchase the goods. Cash may change hands, but payment alone does not legitimize the transaction or justify the recognition of revenue if there is no underlying business purpose or economic benefit for the transactions." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Altered or False Shipping Documents "By creating phony shipping documentation, a company may falsely record sales transactions and improperly recognize revenue. By altering shipping documentation (commonly changing shipment dates and/or terms), a company can increase revenue in a specific accounting period regardless of the facts and circumstances that the transaction and the resulting revenue should have been recorded in the subsequent accounting period." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Sell-Through Agreements "These sales agreements include contingent terms that are based on the future performance of the buyer of the goods (commonly distributors or resellers) and impact revenue recognition for the seller. These contingent terms may or may not be included in the sales agreements and may be provided in side agreements. "Sell through" agreements are similar to consignment sales and can involve shipment of goods to a party who agrees to sell them to third parties. A sale is not considered to have taken place (and therefore revenue should not be recorded) until the goods are sold to a third party (a customer or end-user) with no additional contingent sales terms." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Up-Front Fees "Some sales transactions require customers to pay up-front fees for services that will be provided over an extended period of time. Companies may attempt to recognize the full amount of the contract or the amount of the fees received before the services are performed (and before revenue is earned). In some instances, the scheme may involve the falsification or modification of accounting records (e.g., purchase orders, invoices and sales contracts)."

Fraud Risk Exposure and Description
[**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Holding Accounting Periods Open "Improperly holding accounting records open beyond the end of an accounting period can enable companies to record additional transactions that occur after the end of a reporting period in the current accounting period. This scheme commonly involves recording sales and/or cash receipts that occur after the end of the reporting period in the current period. Schemes sometimes include falsification or modification of accounting documentation (dates on shipping documents, purchase orders, bank statements, cash reconciliations, cash receipt journals, etc.) in an attempt to cover the trail of the fraud." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Failure to Record Sales Provisions or Allowances “Some sales transactions require companies to record provisions or reductions to gross sales amounts (e.g., to account for future sales returns). By failing to record sales provisions or reductions, companies can improperly overstate revenues. The scheme may involve the falsification or modification of accounting records in an attempt to hide the terms or conditions that may require the sales reduction (e.g., purchase orders, invoices and sales contracts).” [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Premature Revenue Recognition: Manipulating Percentage of Completion The completed-contract method or the percentage-of-completion method, depending partly on the circumstances. The completed-contract method does not record revenue until the project is 100 percent complete. Construction costs are held in an inventory account until completion of the project. The percentage-of-completion method recognizes revenues and expenses as measurable progress on a project is made, but this method is particularly vulnerable to manipulation. Managers can often easily manipulate the percentage-of-completion and the estimated costs to complete a construction project to recognize revenues prematurely and conceal contract overruns.” (p. 1.220).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Premature Revenue Recognition: Manipulating Estimated Costs to Complete "Long-term contracts can cause special problems for revenue recognition. In many countries, for example, revenues and expenses from long-term construction contracts can be recorded using either the completed-contract method or the percentage-of-completion method, depending partly on the circumstances. The completed-contract method does not record revenue until the project is 100 percent complete. Construction costs are held in an inventory account until completion of the project. The percentage-of-completion method recognizes revenues and expenses as measurable progress on a project is made, but this method is particularly vulnerable to manipulation. Managers can often easily manipulate the percentage-of-completion and the estimated costs to complete a construction project to recognize revenues prematurely and conceal contract overruns." (p. 1.221). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Inappropriately Reported Expenses
Improper Period Recognition of Expenses "The timely recording of expenses is often compromised due to pressures to meet budget projections and goals, or due to lack of proper accounting controls. As the expensing of certain costs is pushed into periods other than the ones in which they actually occur, they are not properly matched against the income that they help produce. For example, revenue might be recognized on the sale of certain items, but the cost of goods and services that went into the items sold might intentionally not be recorded in the accounting system until the following period. This might make the sales revenue from the transaction almost pure profit, inflating earnings. In the next period, earnings would have fallen by a similar amount" (p.1.222). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Improper Use of Special Purpose Variable Interest Entities

Fraud Risk Exposure and Description
"Special purpose entities (SPEs) are separate legal entities that are corporate in structure and are established (or chartered by) the national, state, or a sub-unit form of government. Because multiple parties often interact with SPEs, it can be difficult to determine, for accounting purposes, which party should consolidate the SPE's assets and liabilities on its statement of financial position. Although SPEs are used for legitimate purposes, SPEs and complex corporate structures were used to perpetrate some major financial frauds. In certain instances, some sponsoring entities provided an incomplete picture of their financial position by not disclosing the transfer of their assets and liabilities to their unconsolidated SPEs. … several IOSCO [International Organization of Securities Commissions] members have implemented regulatory and legislative changes that are expected to address the concerns raised by the recent financial frauds. Specifically, some IOSCO members have adopted additional nonfinancial statement disclosure requirements to solicit information about unconsolidated SPEs, while others have looked to changes in the relevant accounting standards that were intended to make it more likely that SPEs would be consolidated. The results of the survey and limited review of filings indicate that IOSCO members have only recently taken different approaches in this area and have not yet had an opportunity to evaluate the effectiveness of their initiatives. As a result, the technical committee has concluded that it would be premature at this time to determine a global approach for addressing the reporting of information to investors regarding unconsolidated SPEs. However, IOSCO will continue to monitor developments with respect to off-statement of financial position financings, including unconsolidated SPEs, and may consider at a later date whether guidance from IOSCO on unconsolidated SPEs would be useful." (p. 2.536). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Inappropriately Reflected Balance Sheet Amounts, Including Reserves "Most improper asset valuations involve the fraudulent overstatement of inventory or receivables, again with the goal being to strengthen the appearance of the balance sheet. Other improper asset valuations include manipulation of the allocation of the purchase price of an acquired business to inflate future earnings, misclassification of fixed and other assets, or improper capitalization of inventory or start-up costs. Improper asset valuations usually take the form of one of the following classifications:" • "Inventory valuation" • "Accounts receivable" • "Business combinations" • "Fixed assets" "In many countries, changes in required methods of accounting for goodwill have decreased the incentive for companies to minimize the amount allocated to goodwill that previously was required to be amortized against future earnings. However, Companies might still be tempted to over-allocate the purchase price to in-process research and development assets so that they can then write them off

Fraud Risk Exposure and Description
immediately. Alternatively, they might establish excessive reserves for various expenses at the time of acquisition, intending to release those excess reserves into earnings at a future date" (p.1.223, 1.226). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Improper Asset Valuation "One way to commit financial statement fraud is to manipulate the valuation of a company's assets. Typically, a fraudster artificially increases asset accounts to strengthen the company's balance sheet and its financial ratios. In some cases, however, a fraudster might want to record false revenues, and overstated assets are simply a by-product of that scheme. With the exception of certain securities, asset values are generally not increased to reflect current market value. It is often necessary to use estimates in accounting. For example, estimates are used in determining the residual value and the useful life of a depreciable asset, the uncollectible portion of accounts receivable, or the excess or obsolete portion of inventory. Whenever estimates are used, there is an additional opportunity for fraud by manipulating those estimates. Many schemes are used to inflate current assets at the expense of long-term assets. In the case of such schemes, the net effect is seen in the current ratio, which divides current assets by current liabilities to evaluate a company's ability to satisfy its short-term obligations. By misclassifying long-term assets as short-term, the current ratio increases. This type of misclassification can be of critical concern to lending institutions that often require the maintenance of certain financial ratios. This is of particular consequence when the loan covenants are on unsecured or under-secured lines of credit and other short-term borrowings. Sometimes these misclassifications are referred to as window dressing" (p.1.222-223). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
"**Refreshed" Receivables** In order to mask rising account receivable balances (including known or suspected uncollectible balances) while avoiding increasing the bad debt provision, a company may "refresh" the aging of receivables and improperly represent A/R balances as being current in nature instead of showing the true age of the receivables. This may occur with exchange transactions with customers, where customers can receive "credits" to their accounts and allowed to repurchase goods where little, if any, physical transfer of merchandise occurs. Some schemes may simply modify or edit dates of invoices in the A/R system that results in a "restart" of the aging process for the modified receivables. Schemes

Fraud Risk Exposure and Description
may involve the falsification or improper modification of accounting documentation (invoices, purchase orders, change orders, shipping reports, etc.) to cover up the fraud scheme. [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Misstated Inventory Quantities or Values "Under many countries' accounting standards, including U.S. GAAP and IFRS, inventory should be recorded at the lower of cost or net realizable value. This means that inventory must be valued at its acquisition cost, except when the cost is determined to be higher than the net realizable value, in which case it should be written down to its net realizable value or written off altogether if it has no value. Failing to write down or write off inventory results in overstated assets and the mismatching of cost of goods sold with revenues. Other methods by which inventory can be improperly stated include manipulation of the physical inventory count, inflation of the unit costs used to price out inventory, and failure to adjust inventory for the costs of goods sold. Fictitious inventory schemes usually involve the creation of fake documents, such as inventory count sheets and receiving reports. Many inventory reports are kept electronically, which allows the fraud examiner to total columns and perform data analysis techniques to detect these types of inventory fraud schemes" (p. 1.223-224). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Misstated Accounts Receivable "Accounts receivable are subject to manipulation in the same manner as sales and inventory, and, in many cases, the schemes are conducted together. The two most common schemes involving overstated accounts receivable are recording fictitious receivables and the failure to properly account for uncollectible customer accounts" (p. 1.224). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Misstated Merger and Acquisition Values

Fraud Risk Exposure and Description
"Companies are required to allocate the purchase price they have paid to acquire another business to the tangible and intangible assets of that business. Any excess of the purchase price over the value of the acquired assets is treated as goodwill. In many countries, changes in required methods of accounting for goodwill have decreased the incentive for companies to minimize the amount allocated to goodwill that previously was required to be amortized against future earnings. However, companies might still be tempted to over-allocate the purchase price to in-process research and development assets so that they can then write them off immediately. Alternatively, they might establish excessive reserves for various expenses at the time of acquisition, intending to release those excess reserves into earnings at a future date" (p.1.226). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Improper Capitalization of Intangible Items "Interest and finance charges incurred in the purchase are excluded from the recorded cost of a purchased asset. For example, when a company finances a capital equipment purchase, monthly payments include both principal liability reduction and interest payments. On initial purchase, only the original cost of the asset should be capitalized. The subsequent interest payments should be charged to interest expense and not to the asset. Without a reason for intensive review, this type of fraud can go unchecked" (p.1.227). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Changing or Manipulating Depreciation Methods "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 retroactively restate financial statements 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 lives 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" (p.1.236).

Fraud Risk Exposure and Description
"In some cases, as with some government-related or government-regulated companies, it is advantageous to understate assets. Additional funding is often based on asset amounts. This understatement can be done directly or through improper depreciation" (p.1.227). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table

Failure to Recognize Impaired Assets

Assets are said to be impaired when their net carrying value, (acquisition cost - accumulated depreciation), is greater than the future undiscounted cash flow that these assets can provide and be disposed for.

Under U.S. GAAP impaired assets must be recognized once there is evidence of a lack of recoverability of the net carrying amount. Once impairment has been recognized it cannot be restored. Analysts must know that some foreign countries and the IASB allow companies to recognize increases in previously impaired assets.

Asset impairment occurs when there are:

- Changes in regulation and business climate
- Declines in usage rate
- Technology changes
- Forecasts of a significant decline in the long-term profitability of the asset

Once a company has determined that an asset is impaired, it can write down the asset or classify it as an asset for sale. Assets will be written down if the company keeps on using this asset. Write-downs are sometimes included as part of a restructuring cost. It is important to be able to distinguish asset write-downs, which are non-cash expenses, from cash expenses like severance packages.

Write-downs affect past reported income. The loss should be reported on the income statement before tax as a component of continuing operations. Generally impairment recognized for financial reporting is not deductible for tax purposes until the affected assets are disposed of. That said, in most cases recognition of an impairment leads to a deferred tax asset.

Impaired assets held for sale are assets that are no longer in use and are expected to be disposed of or abandoned. The disposition decision differs from a write-down because once a company classifies impaired assets as assets for sale or abandonment, it is actually severing these assets from assets of continuing operations as they are no longer expected to contribute to ongoing operations. This is the accounting impact: assets held for sales must be written down to fair value less the cost of selling them. These assets can no longer be depreciated.

Effects on Financial Statements and Ratios include:

- Past income statements are not restated. The current income statement will include an impairment loss in income before tax from continuing operations. Net income will also be lower.

Fraud Risk Exposure and Description
• On the balance sheet, long-term assets are reduced by the impairment. A deferred-tax asset is created (if there was a deferred tax liability it is reduced). Stockholders' equity is reduced as a result of the impairment loss included in the income statement. • Current and future fixed-asset turnover will increase (lower fixed assets). • Since stockholders' equity will be lower, debt-to-equity will be lower. • Debt-to-assets will be higher. • Cash flow based ratios will remain unaffected (no cash implications). • Future net income will be higher as there will be lower asset value, and thus a smaller depreciation expense. • Future ROA and ROE will increase. • Past ratios that evaluated fixed assets and depreciation policy are distorted by impairment write-downs. [**Source:** Investopedia, https://www.investopedia.com/exam-guide/cfa-level-1/assets/asset-impairment.asp] Return to Table
Unrealistic or Unsupported Estimates "In preparing financial statements, management is responsible for making a number of judgments or assumptions that affect significant accounting estimates and for monitoring the reasonableness of such estimates on an ongoing basis. Fraudulent financial reporting often is accomplished through intentional misstatement of accounting estimates. Intent is often difficult to determine, particularly in matters involving accounting estimates and the application of accounting principles. For example, unreasonable accounting estimates may be unintentional or may be the result of an intentional attempt to misstate the financial statements." [**Source:** PCAOB, AS 2401: Consideration of Fraud in a Financial Statement Audit; https://pcaobus.org/Standards/Auditing/Pages/AS2401.aspx] Return to Table
Unrealistic or Unsupported Adjustments to Estimates Adjustments to Estimates - Estimates are common throughout the accounting process and can be manipulated to impact revenues, expenses, asset valuations, and/or liabilities. Management is often in a position where it can influence or bias estimates. Common fraud schemes involve the reduction of accruals or reserves in order to increase earnings in the current period, and may involve the earlier creation of excess reserves or "cookie-jar reserves" when the company was in a financial position to create a "cushion" against future losses. [**Source:** Deloitte, Sample Listing of Fraud Schemes]

Fraud Risk Exposure and Description
Return to Table
Misclassification of Assets "To meet budget requirements—and for various other reasons—assets are sometimes misclassified into general ledger accounts in which they don't belong. For example, fixed assets might be fraudulently reclassified as current assets. The manipulation can create misleading financial ratios and help the company comply with loan covenants or other borrowing requirements" (p.1.227). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Manipulating the Value of Investments Designed to overstate assets and earnings, schemes can deliberately overstate existing investments or create fictitious investments. Investments may also be intentionally misclassified resulting in the improper recognition of gains or failure to recognize losses. Other schemes are designed to hide or defer losses from sales or permanent writedowns from impairments. [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Inappropriate Depreciation Methods "Depreciation is an accounting method of allocating the cost of a tangible asset over its useful life. Businesses depreciate long-term assets for both tax and accounting purposes. For tax purposes, businesses can deduct the cost of the tangible assets they purchase as business expenses; however, businesses must depreciate these assets in accordance with IRS rules about how and when the deduction may be taken." "Depreciation may be a simple concept, but inappropriate methods, and overestimation of asset life, can seriously distort both profit and loss accounts and budgets. Attempts to avoid 'loss on disposal can sometimes even have serious operational effects, by (for example) inhibiting the acquisition of possibly much-needed replacement systems." [**Source:** Investopedia - Depreciation https://www.investopedia.com/terms/d/depreciation.asp#ixzz58F3w3gkN

Fraud Risk Exposure and Description
Source: Chartered Institute for Business - http://www.bcs.org/content/conWebDoc/5953] Return to Table
Recording Fictitious Assets "One of the easiest methods of asset misrepresentation is the recording of fictitious assets. This false creation of assets affects account totals on a company's balance sheet. The corresponding account commonly used is the owners' equity account. Because company assets are often physically found in many different locations, this fraud can sometimes be easily overlooked. One of the most common fictitious asset schemes is to simply create fictitious documents. In other instances, the equipment is leased, not owned, and this fact is not disclosed during the audit of fixed assets. Fictitious fixed assets can sometimes be detected because the fixed asset addition makes no business sense" (p.1.226). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
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 actually 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 since the missing transactions leave no audit trail" (p.1.228). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Concealed Liabilities and Expenses: Omission "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

Fraud Risk Exposure and Description
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" (p.1.228-229). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Sales Returns and Allowances and Warranties "Improper recording of sales returns and allowances occurs when a company fails to properly record or present the expense associated with sales returns and customer allowances stemming from customer dissatisfaction. It is inevitable that a certain percentage of products sold will, for one reason or another, be returned." [**Source:** Forensic Accounting Club, Financial Statement Fraud: Concealed Liabilities and Expenses; http://www.forensicaccounting.club/financial-statement-fraud-concealed-liabilities-and-expenses/] Return to Table
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. When this happens, 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. 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)" (p.1.233). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Concealed Liabilities and Expenses: Capitalization of Operating Expenses "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 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" (p.1.230-231). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Concealed Liabilities and Expenses: Tax Liability Manipulation "The Internal Revenue Code allows taxpayers to deduct certain expenses from their gross income before calculating their tax liability. Many tax deductions involve conduct that the government wants to encourage, such as allowing an employer to deduct the cost of certain benefits provided to employees. The more deductions a taxpayer claims, the less tax they owe. Overstatement of tax deductions accounted for only about $17 billion of the 2006 tax gap, according to the IRS, but it is among the most common incidents of tax fraud." [**Source:** Justia, Tax Fraud; https://www.justia.com/criminal/offenses/white-collar-crimes/fraud/tax-fraud/] Return to Table

Fraud Risk Exposure and Description
Concealed Liabilities and Expenses: Off-Balance-Sheet Entities and Liabilities Some schemes involve the use of "off-balance-sheet" vehicles or special purposes entities to conceal liabilities. Off-balance-sheet vehicles may be allowable [in some countries]; however, some schemes are designed to utilize these entities or transactions to conceal debt and misstate liabilities on the balance sheet and may also have income statement impact as well. [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Improper or Unjustified Consolidation Entries "Some schemes occur during the financial closing and consolidation process and involve un-justified or fictitious consolidation entries. Often there is limited accounting documentation or explanations for consolidation entries and activities." [**Source:** Deloitte, Sample Listing of Fraud Schemes https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Corporate%20Governance/Audit%20Committee/in-gc-fraud-schemes-questions-to-consider-noexp.pdf] Return to Table
Intercompany Manipulations Similar to other accounting schemes involving consolidations, intercompany manipulations may have limited documentation or explanations for inter-company entries and activities. Schemes may occur to over/understate balances or may involve the creation of fictitious transactions. [**Source:** Deloitte, Sample Listing of Fraud Schemes https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Corporate%20Governance/Audit%20Committee/in-gc-fraud-schemes-questions-to-consider-noexp.pdf] Return to Table
Sham Related-Party Transactions "… sham transactions refer specifically to sales schemes that appear genuine but actually are rigged for the purpose of letting the seller recognize revenue. Other indicators that fraudulent financial reporting might exist include bogus shipping dates, revenue figures that always meet analysts' expectations and transactions with unusual payment terms."

Fraud Risk Exposure and Description
[**Source:** Journal of Accountancy, Hocus-Pocus Accounting, Douglas R. Carmichael; https://www.journalofaccountancy.com/issues/1999/oct/carmichl.html] Return to Table
Disclosure Frauds "Fraudulent disclosures may include providing false information or the failure to disclose required information. Schemes may involve a company's failure to disclose certain transactions with related parties, material asset impairments, unrecorded liabilities or accounting practices that violate…GAAP." [**Source:** Deloitte, Sample Listing of Fraud Schemes] Return to Table
Top-Side Entries/Adjustments "Widely considered among the riskiest types of journal entries in accounting, topside entries occur when a corporate entity makes financial entries on its subsidiaries journals. While topside entries can be legitimate and coincide with generally accepted auditing standards, they can also be used to make fraudulent transactions appear legitimate." [**Source:** Miranda Morley, What is a Topside Entry in Accounting?] Return to Table
Inappropriately Approved and/or Masked 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 likely 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. In addition, the disclosed information must not be misleading" (p.1.233-234).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Liabilities Omissions "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 as long as 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 taken out by an officer or a private company controlled by an officer is an example of a contingent liability. Under generally accepted accounting principles, the company's potential liability must be disclosed if it is material" (p.1.234). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
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" (p.1.234). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Related-Party Transactions "Related-party transactions 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, as long as they are fully disclosed. If the transactions are not fully disclosed, the company might injure shareholders by engaging in economically harmful dealings without their knowledge.

Fraud Risk Exposure and Description
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 he/she/it does 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. While these transactions are sometimes conducted at arm's length, often they are not" (p.1.235). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
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 retroactively restate financial statements 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 lives 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" (p.1.236). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Management Frauds Uncovered "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 likely also involve lying to auditors, an illegal act in itself" (p.1.235). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Backdating Transactions "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" (p.1.236). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Cookie Jar Accounting/ Cookie Jar Reserves "A disingenuous accounting practice in which periods of good financial results are used to create reserves that shore up profits in lean years. "Cookie jar accounting" is used by a company to smooth out volatility in its financial results, thus giving investors the misleading impression that it is consistently meeting earnings targets. This reliable earnings performance is generally rewarded by investors, who assign the company a premium valuation. Regulators frown on the practice since it misrepresents a company's performance, which may be very different in reality from what it purports to be. The term may be derived from the fact that a company which employs this practice dips into the "cookie jar" of reserves whenever it feels like it. But the company may have to pay a steep price if it is caught with its hand in the proverbial cookie jar." [**Source:** Investopedia, Cookie Jar Accounting; https://www.investopedia.com/terms/c/cookiejaraccounting.asp] Return to Table
Management Override Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status. [**Source:** 2013 COSO Framework] Management may override controls to intentionally misstate the nature and timing of revenue or other transactions by (1) recording fictitious business events or transactions or changing the timing of

Fraud Risk Exposure and Description
recognition of legitimate transactions, particularly those recorded close to the end of an accounting period; (2) establishing or reversing reserves to manipulate results, including intentionally biasing assumptions and judgments used to estimate account balances; and (3) altering records and terms related to significant or unusual transactions. [**Source:** Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention.] Return to Table
Concealing Misappropriation of Assets "Misappropriation of assets involves the theft of an entity's assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management, who is usually better able to disguise or conceal misappropriations in ways that are difficult to detect. Misappropriation of assets can be accomplished in a variety of ways including the following: • Embezzling receipts (for example, misappropriating collections on accounts receivable or diverting receipts from written-off accounts to personal bank accounts) • Stealing physical assets or intellectual property (for example, stealing inventory for personal use or for sale, stealing scrap for resale, or colluding with a competitor by disclosing technological data in return for payment) • Causing an entity to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the entity's purchasing agents in return for approving payment at inflated prices, or payments to fictitious employees) • Using an entity's assets for personal use (for example, using the entity's assets as collateral for a personal loan or a loan to a related party) Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorization." [**Source:** Paragraph .11 of AU-C sec. 240, Consideration of Fraud in a Financial Statement Audit https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00240.pdf#http://www.aicpa.org/Research/Standards/] Return to Table
Concealing Unauthorized Acquisition, Disposition, and Use of Assets "Asset requisitions and other documents that allow noncash assets to be moved from one location in a company to another can be used to facilitate the theft of those assets. Employees use internal transfer paperwork to gain access to merchandise that they otherwise might not be able to handle without raising suspicion. These documents do not account for missing merchandise the way false sales do, but they allow a person to move the assets from one location to another. In the process of this movement, the thief steals the merchandise.

Fraud Risk Exposure and Description
The most basic scheme occurs when an employee requisitions materials for some work- related project and then makes off with those materials. In some cases, the employee simply overstates the amount of supplies or equipment it will take to complete his work and pilfers the excess. In more ambitious schemes, the employee might invent a completely fictitious project that necessitates the use of certain assets he intends to steal. Dishonest employees sometimes falsify asset transfer forms so they can remove inventory from a warehouse or stockroom. The false documents allow the employee to remove merchandise from the warehouse, but instead of using it for a work-related purpose, the perpetrator simply takes it home. The obvious problem with this type of scheme is that the person who orders the merchandise will usually be the primary suspect when it turns up missing." (p. 1.506). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Misappropriation of Tangible Assets "There are basically two ways a person can misappropriate a company asset. The asset can be misused or it can be stolen. Simple misuse is obviously the less egregious of the two. Assets that are misused but not stolen typically include company vehicles, company supplies, computers, and other office equipment." (p. 1501). "Though the misuse of company property might be a problem, the theft of company property is obviously of greater concern. Losses resulting from larceny of company assets can run into the millions of dollars. Most schemes where inventory and other noncash assets are stolen fall into one of four categories: larceny schemes, asset requisition and transfer schemes, purchasing and receiving schemes, and false shipment schemes." (p. 1502). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Cash Theft "In the occupational fraud setting, *cash larceny* is defined as the intentional taking of an employer's cash 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 involves the theft of money that has already appeared on the victim company's books. Accordingly, these schemes are much harder to get away with—they leave an audit trail." (p. 1.320).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Sales Register Manipulation "Some employees might ring a "no sale" or another non-cash transaction to mask the theft of sales. The false transaction is entered on the register so that it appears as if a sale is being rung up. The perpetrator opens the register drawer and pretends to place the cash he has just received in the drawer, but in reality he pockets the cash. To the casual observer it looks as though the sale is being properly recorded." (p. 1.324). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
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 cash has been stolen. This is the primary advantage of a skimming scheme to the fraudster." (p. 1.301). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
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 actually collected. One way employees commit understated sales schemes is by altering receipts or preparing false receipts that misstate sales amounts." (p. 1.307). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Theft of Checks Received 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 simply steals one or more incoming checks instead of posting them to customer accounts. 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." (p. 1.301). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Lapping "Lapping customer payments is one of the most common methods of concealing receivables skimming. Lapping is the crediting of one account through the abstraction of money from another account. It is the fraudster's version of "robbing Peter to pay Paul." 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 his account will be credited with the payment he has made. If the payment has not been posted by the time A's next statement is mailed, he will see that the payment was not applied to his 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 is behind. 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." (p. 1.313) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Collection Procedures "Poor collection and recording procedures can make it easy for an employee to skim sales or receivables." (p. 1.306). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Check for Currency Substitution "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 put his hands on 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, he 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. 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 still 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 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." (p. 1.311). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
False Entries to Sales Accounts "Intercepting the customer's statements will keep him unaware of his account's status, but as long as the customer's payments are being skimmed, his account is slipping further and further past due. The perpetrator must bring the account back up-to-date to conceal his 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." (1.315). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
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. If this sale is not recorded, however, the shoes are not removed from the perpetual inventory records. Thus, there is one less pair of shoes on hand 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 serve as 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." (1.316). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Theft of Cash from Register

Fraud Risk Exposure and Description
"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 as a cover for cash theft. In a flurry of activity, with money being passed back and forth between customer and employee, an employee can often slip cash out of the register and into his pocket undetected. The most straightforward cash larceny scheme is to simply open the register and remove currency or checks. (See the "Cash Larceny from the Register" flowchart that follows.) The theft is often committed as a sale is being conducted so that it appears to be part of the transaction. In other circumstances, the perpetrator waits for a slow moment when no one is around to notice him digging 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, on the other hand, 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 arrive at a 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." (1.321). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
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 up-to-the minute reconciliation of the deposits to the bank statement—and if daily receipts do not drop precipitously—he might be able to avoid detection for a period of time. Lapping is discussed in more detail in the "Skimming" section." (p. 1.328). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
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 hasn't yet 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." (1.329). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Insider Trading Buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information. [**Source:** Securities and Exchange Commission, "Fast Answers"] Return to Table
Fraudulent Disbursements "In fraudulent disbursement schemes, an employee makes a distribution of company funds for a dishonest purpose. Examples of fraudulent disbursements include forging company checks, the submission of false invoices, altering timecards, and so forth. On their face, 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 runs a fake invoice through the accounts payable system, the victim organization cuts a check for the bad invoice right along with all the legitimate payments it makes. The perpetrator has taken money from his 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." (1.401). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
False 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, he removes $100 from the register. Two things result from 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 actually returned. The result is that the company's inventory balance on the books is overstated by the amount of the excess refund." (p. 1.402). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
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 first thing the perpetrator needs is the customer's copy of the sales receipt. Typically, when an employee sets about processing a fictitious void, the employee simply 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." (p. 1.404). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Small Disbursements

Fraud Risk Exposure and Description
"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 simply process numerous refunds that are small enough that they do not have to be reviewed." (1.407). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Check Tampering "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 himself by submitting some false document to the victim organization, such as an invoice or a timecard. 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 himself 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. Because many business payments are currently 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, 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 will be discussed in a separate section at the end of this chapter." (1.410). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Billing Schemes

Fraud Risk Exposure and Description
"The asset misappropriation schemes discussed up to this point—skimming, larceny, register schemes, and check tampering—all require the scheme's perpetrator to physically take cash or checks from his employer. The next three sections will cover a different kind of asset misappropriation scheme, one which allows the perpetrator to misappropriate company funds without ever actually handling cash or checks while at work. These schemes succeed by making a false claim for payment upon the victim organization. This group consists of billing schemes (which attack the company's purchasing function), payroll schemes, and expense reimbursement schemes. The most common of these is the billing scheme. Billing schemes are a popular form of employee fraud mainly because they offer the prospect of large rewards. Since most businesses' disbursements are made in the purchasing cycle, larger thefts can be hidden through false-billing schemes than through other kinds of fraudulent disbursements. There are three principal types of billing schemes: false invoicing via shell companies, false invoicing via nonaccomplice vendors, and personal purchases made with company funds." (p. 1.436). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Personal Purchases with Company Funds "Instead of undertaking billing schemes to generate cash, many fraudsters simply purchase personal items with their company's money. Company accounts are used to buy items for employees, their businesses, their families, and so on. This type of scheme is classified as a fraudulent billing scheme rather than theft of inventory. The heart of the scheme is not the theft of the items but rather the purchase of them. The perpetrator causes the victim company to purchase something it did not actually need, so the damage to the company is the money lost in purchasing the item." (p. 1.444). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Returning Merchandise for Cash "The fraudulent purchase schemes discussed to this point have all involved false purchases of merchandise for the sake of obtaining the merchandise. In some cases, however, an employee buys items and then returns them for cash." (p. 1.449). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Creation of False or Fictitious Vendors, Suppliers, or Subcontractors "A common procurement scheme is to set up phony vendors or suppliers in the accounts payable system or approve payments for services that are received by the employee or co-conspirator. " [**Source:** Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Corporate%20Governance/Audit%20Committee/in-gc-fraud-schemes-questions-to-consider-noexp.pdf]
False Shipments of Inventory and Other Assets "To conceal thefts of inventory and other assets, employees sometimes create false shipping documents and false sales documents to make it appear that the inventory they take was sold rather than stolen. The document that tells the shipping department to release inventory for delivery is usually the packing slip. By creating a false packing slip, a corrupt employee can cause inventory to be fraudulently delivered to himself or an accomplice. The "sales" reflected in the packing slips are typically made to a fictitious person, a fictitious company, or the perpetrator's accomplice. "One benefit of using false shipping documents to misappropriate inventory or other assets is that the product is removed from the warehouse or storeroom by someone other than the perpetrator. The victim organization unknowingly delivers the targeted assets to the perpetrator of the scheme. "False packing slips allow inventory to be shipped from the victim company to the perpetrator, but they do not conceal the fact that inventory has been misappropriated in and of themselves. To hide the theft, fraudsters might create a false sale on the books so it appears that the missing inventory was shipped to a customer. Depending on how the victim organization operates, the perpetrator might have to create a false purchase order from the "buyer," a false sales order, and a false invoice along with the packing slip to create the illusion of a sale. "The result is that a fake receivable account goes into the books for the price of the misappropriated inventory. Obviously, the "buyer" of the merchandise will never pay for it How do employees deal with these fake receivables? In some cases, the employee simply lets the receivable age on his company's books until it is eventually written off as uncollectible. In other instances, he might take affirmative steps to remove the sale-and the resulting delinquent receivable--from the books." [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Payments for Services Not Received

Fraud Risk Exposure and Description
Causing an entity to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the entity's purchasing agents in return for approving payment at inflated prices, or payments to fictitious employees). (p. 4.522). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Payroll Fraud "Payroll schemes are similar to billing schemes. The perpetrators of these frauds produce false documents, which cause the victim company to unknowingly make a fraudulent disbursement. In billing schemes, the false document is usually an invoice (coupled, perhaps, with false receiving reports, purchase orders, and purchase authorizations). In payroll schemes, the perpetrator typically falsifies a timecard or alters information in the payroll records. The major difference between payroll schemes and billing schemes is that payroll frauds involve disbursements to employees rather than to external parties. In general, payroll schemes fall into three categories: ghost employee schemes, falsified hours and salary schemes, and commission schemes." (p. 1.456). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Ghost Employees "The term ghost employee refers to someone on the payroll who does not actually work for the victim company. Through the falsification of personnel or payroll records, a fraudster causes paychecks to be generated to a non-employee, or ghost. The fraudster or an accomplice then converts these paychecks. (See the "Ghost Employees" flowchart that follows.) The ghost employee might be a fictitious person or a real individual who simply does not work for the victim employer. When the ghost is a real person, it is often the perpetrator's friend or relative. For a ghost employee scheme to work, four things must happen: (1) the ghost must be added to the payroll, (2) timekeeping (for an hourly employee) and wage rate information must be collected, (3) a paycheck must be issued to the ghost, and (4) the check must be delivered to the perpetrator or an accomplice." (1.456). "Timekeeping records can be maintained in a variety of ways. In many organizations, computer systems are used to track employees' hours. Alternatively, employees might manually record their hours on timecards or might punch time clocks that record the time at which a person starts and finishes his work. When a ghost employee scheme is in place, someone must create documentation for the ghost's hours. This essentially amounts to preparing a fake timecard showing when the ghost was

Fraud Risk Exposure and Description
allegedly present at work. Depending on the normal procedure for recording hours, a fraudster might log into the computerized system and record the ghost employee's hours, create a timecard and sign it in the ghost's name, punch the time clock for the ghost, or so on. Preparation of the timecard is not a great obstacle to the perpetrator. The real key to the timekeeping document is obtaining approval of the timecard. A supervisor should approve the timecards of hourly employees before paychecks are issued. This verifies to the payroll department that the employee actually worked the hours that are claimed on the card. A ghost employee, by definition, does not work for the victim organization, so approval will have to be fraudulently obtained. Often, the supervisor himself is the one who creates the ghost. When this is the case, the supervisor fills out a timecard in the ghost's name and then affixes his own approval. The timecard is thereby authenticated and a paycheck will be issued. When a non-supervisor is committing a ghost employee scheme, he will typically forge the necessary approval and then forward the fraudulent timecard directly to payroll accounting, bypassing his supervisor. In computerized systems, a supervisor's signature might not be required. In lieu of the signature, the supervisor inputs data into the payroll system and the use of his password serves to authorize the entry. If an employee has access to the supervisor's password, he can input data for the ghost, which will appear in the payroll system with a seal of approval. If the perpetrator creates ghosts who are salaried rather than hourly employees, it is not necessary to collect timekeeping information; salaried employees are paid a certain amount each pay period regardless of how many hours they work. Because the timekeeping function can be avoided, it might be easier for a perpetrator to create a ghost employee who works on salary. However, most businesses have fewer salaried employees and they are more likely to be members of management. The salaried ghost might therefore be more difficult to conceal." (p. 1.459). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Failure to Remove Terminated Employees from Payroll "Instead of adding new names to the payroll, some employees undertake ghost employee schemes when they fail to remove terminated employees' names. Paychecks to the terminated employee continue to be generated even though the employee no longer works for the victim organization. The perpetrator intercepts these fraudulent paychecks and converts them for his personal use." (p. 1.458). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Falsified Hours and Salary or Pay Rate "The most common method of misappropriating funds from the payroll is the overpayment of wages. For hourly employees, the size of a paycheck is based on two factors: the number of hours worked and the rate of pay. Therefore, for hourly employees to fraudulently increase the size of their paycheck, they must either falsify the number of hours they have worked or change their wage rate. (See the "Falsified Hours and Salary" flowchart that follows.) Because salaried employees do not receive compensation based on their time at work, in most cases these employees generate fraudulent wages by increasing their rates of pay. When discussing payroll frauds that involve overstated hours, one must first understand how an employee's time at work is recorded. Time is generally kept by one of three methods. Time clocks might be used to mark the time when an employee begins and finishes work. The employee inserts a card into the clock at the beginning and end of work, and the clock imprints the current time on the card. In more sophisticated systems, computers might automatically track the time employees spend on the job based on login codes or some other similar tracking mechanism. Finally, paper or computerized timecards showing the number of hours an employee worked on a particular day are often prepared manually by the employee and approved by his manager." (p. 1.461). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Failure to Report Leave Taken "One form of control breakdown that often occurs is the failure to maintain proper control over timecards. In a properly run system, timecards that have been authorized by management should be sent directly to payroll. Those who prepare the timecards should not have access to them after they have been approved. Similarly, computerized timesheets should be blocked from modification by the employee once supervisor authorization has been given. When these procedures are not observed, the person who prepared a timecard can alter it after the supervisor has approved it but before it is delivered to payroll. Another way hours are falsified is in the misreporting of leave time. This is not as common as timecard falsification, but it does occur with some frequency. Incidentally, it is one instance in which salaried employees commit payroll fraud by falsifying their hours. A leave time scheme is very simple. An employee takes a certain amount of time off of work as paid leave or vacation, but does not report this leave time. Employees typically receive a certain amount of paid leave per year. If a person takes a leave of absence but does not report it, those days are not deducted from his allotted days off. In other words, he gets more leave time than he is entitled to. The result is that the employee shows up for work less, yet still receives the same pay." (p. 1.464). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Commission Sales "Commission is a form of compensation calculated as a percentage of the amount of transactions a salesperson or other employee generates. It is a unique form of compensation that is not based on hours worked or a set yearly salary, but rather on an employee's revenue output. A commissioned employee's wages are based on two factors: the amount of sales he generates and the percentage of those sales he is paid. In other words, there are two ways an employee on commission can fraudulently increase his pay: (1) falsify the amount of sales made or (2) increase his rate of commission. (See the "Commission Schemes" flowchart that follows.)" (p. 1.465). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Expense Reimbursement Fraud Employees can manipulate an organization's expense reimbursement procedures to generate fraudulent disbursements. Companies usually pay expense reimbursements in this manner: "An employee submits a report detailing an expense incurred for a business purpose, such as a business lunch with a client, airfare, and hotel bills associated with business travel, and so on. In preparing an expense report, an employee usually must explain the business purpose for the expense, as well as the time, date, and location in which it was incurred. Attached to the report should be support documentation for the expense—typically a receipt. In some cases, canceled checks written by the employee or copies of a personal credit card statement showing the expense are allowed. The report usually must be authorized by a supervisor in order for the expense to be reimbursed. The four most common types of expense reimbursement schemes are mischaracterized expenses, overstated expenses, fictitious expenses, and multiple reimbursements." (p. 1.473). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Mischaracterized Expenses "Most companies only reimburse certain employee expenses. Which expenses a company will pay for depends to an extent upon policy, but in general, business-related travel, lodging, and meals are reimbursed. One of the most basic expense reimbursement schemes is perpetrated by simply

Fraud Risk Exposure and Description
requesting reimbursement for a personal expense by claiming that the expense is business related. (See the "Mischaracterized Expenses" flowchart that follows.) Examples of mischaracterized expenses include claiming personal travel as a business trip, listing dinner with a friend as "business development," and so on. Employees submit the receipts from their personal expenses along with their expense reports, but concoct business reasons for the incurred costs. The false expense report induces the victim organization to issue a check, reimbursing the perpetrator for his personal expenses. In cases involving airfare and overnight travel, a mischaracterization can sometimes be detected by simply comparing the employee's expense reports to his work schedule. Often, the dates of the so-called "business trip" coincide with a vacation or day off. Detailed expense reports allow a company to make this kind of comparison and are therefore very helpful in preventing expense schemes." (p. 1.473). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Overstated Expenses "Instead of seeking reimbursement for personal expenses, some employees overstate the cost of actual business expenses. (See the "Overstated Expenses" flowchart that follows.) This can be accomplished in a number of ways." (p. 1.477). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Fictitious Expenses "Employees sometimes seek reimbursement for wholly fictitious expenses. Instead of overstating a real business expense or seeking reimbursement for a personal expense, an employee just invents an expense and requests that it be reimbursed." (p. 1.478). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Multiple Reimbursements

Fraud Risk Exposure and Description
"The least common of the expense reimbursement schemes involves multiple reimbursements. This type of fraud involves the submission of a single expense more than one time. The most frequent example of a multiple reimbursement scheme is the submission of several types of support for the same expense. In cases where a company does not require original documents as support, some employees even use several copies of the same support document to generate multiple reimbursements. Rather than file two expense reports, employees might also charge an item to the company credit card, save the receipt, and attach it to an expense report as if they paid for the item themselves. The victim organization therefore ends up paying twice for the same expense." (p. 1.481). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Loan Fraud "Loan fraud is a multifaceted activity that includes several types of criminal activities. Larger loan fraud schemes often involve real estate lending and collusion between insiders and outsiders. Loan fraud represents the highest risk area for financial institutions. Although the number of occurrences might be small, the dollar amount per occurrence tends to be large." (p. 1.905). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Loans to Nonexistent Borrowers "False applications, perhaps with inaccurate financial statements, are knowingly or unknowingly accepted by loan officers as the basis for loans. These types of loan fraud can be perpetrated by people either external to the lending institution ("external fraud") or by officers, directors, or employees of the victim institution ("internal fraud")." (p. 1.905). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Double Pledged Collateral

Fraud Risk Exposure and Description
"Borrowers pledge the same collateral with different lenders before liens are recorded and without telling the lenders." (p. 1.905). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
False Application Information "Perpetrators might apply for a new card using information stolen from a wallet, purse, or the garbage. Additionally, they might steal a preapproved credit card application from the victims' mail or trash, or they might use credit card applications that are prominently featured in store displays." (p. 1.1016). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Construction Loans "Construction lending has different vulnerabilities than other permanent or interim lending. More risks are associated with construction projects than with already-built projects." (p. 1.906). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Real Estate Fraud "Real estate scams are easily recognized. There is almost always an element of time pressure, with the victims being convinced they are participating in an "once-in-a-lifetime, now-or-never" deal. Perpetrators mislead victims into thinking they will miss the opportunity to make a fortune if they do not act fast. Companies tout the riches available in real estate through seminars and books that claim to offer secret ways to cash in. The customer pays for the secret info and gets worthless tips in return." (p.1.1326). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
False Appraisal Value "Appraisal fraud is often associated with money laundering schemes. Money launderers might purchase properties to launder money or might use illicit funds to service the interest on the debts. Such schemes can conceal the true identity of the property owners and the true origin of the funds used in the transaction. Appraisal fraud occurs where appraisers fail to accurately evaluate the property, or when the appraiser deliberately becomes party to a scheme to defraud the lender, the borrower, or both. A common technique is the over- or under-valuation of property, which consists of buying/selling property at a price above/below its market value. In addition to manipulating appraisals, money launderers also over-value property through a series of subsequent sales, each time at a higher price, which tend to conceal the true purposes of the transactions." (p. 2.611). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Fraudulent Appraisal "Fraudulent appraisals result from any number of situations, some of which are: • Intentional use of an incompetent appraiser • Giving the appraiser improper or false assumptions to use in arriving at the value, such as: o Assuming zoning will be changed for a higher and better use when in fact zoning will not be changed o Assuming unrealistically low vacancy and expense rates (or unrealistically high vacancy and expense rates for a short sale) o Assuming unrealistically high income, selling prices, or absorption—the rate at which vacant space will become rented o Otherwise influencing the appraiser—for example, paying above-market fee or promising future business o Direct collusion with the appraiser to commit fraud" (p. 1.920). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Wire Transfer Fraud "Wire transfers are used to quickly move funds between financial institutions. Wire transfers requested before 2 p.m. are typically completed the same day. Fees for wire transfers are often much higher than those for ACH or other types of transfers. The speed of wire transfers makes them an attractive target for fraudsters. According to the AFP's 2017 Payments Fraud and Control Survey, wire transfers were second only to traditional check fraud as the most common payment method subjected to fraud. Wire fraud has been driven in recent years by the rise of business email compromise (BEC) schemes." (p. 1.1038). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
System Password Compromise "In this type of scheme, people who have legitimate access to sensitive account and daily code information for a limited time (for example, computer consultants) effect improper transfers through unauthorized access." (p.1.1007). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Forged Authorizations "Bank officers' and customers' authorization, whether oral or written, is improperly obtained or forged. People forge orders to transfer money to their own accounts when the recipient account is actually in someone else's name." (p. 1.941). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
False or Unauthorized Transfers from Internal Accounts

Fraud Risk Exposure and Description
"There are several types of normal transfers using internal accounts, especially in operating account and general ledger account transactions. A person with the ability to make such transactions might substitute a personal account for one of the internal accounts." (p. 1.902). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
ATM Fraud "An ATM is a dispensing facility from which a debit or credit card holder can withdraw cash. Some types of prepaid cards can also be used at ATMs. The facility can also perform other services, such as depositing funds and verifying account balances, but the most common use is to dispense funds. Fraud schemes have been perpetrated involving the unauthorized use of ATM facilities. Schemes include: - Theft of card and/or unauthorized access to PINs and account codes for ATM transactions by unauthorized persons - Employee manipulation - Counterfeit ATM cards - Counterfeit ATMs - Magnetic strip skimming devices - ATM deposit fraud" (p. 1.944). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Check and Credit Card Fraud **Check Fraud** "Despite the declining use of checks overall, check fraud remains a significant factor in the payment fraud landscape. Check fraud endures primarily because payment by check continues to account for a

Fraud Risk Exposure and Description
significant proportion of all business-to-business payments made in the United States. According to the Association for Financial Professional's (AFP's) 2017 Payments Fraud and Control Survey, 75 percent of companies that reported actual or attempted payment fraud encountered check fraud, an increase from the 71 percent reported in 2016. After years of decline in check fraud, the sudden increase is thought to be a result of the massive increase in business email compromise (BEC) schemes that commonly target checks. Payment by check was still the most frequently used payment method in this study and, consequently, the most vulnerable to fraud." (p. 1.1001). **Credit Card Fraud** "Credit card fraud is the misuse of credit card information to make purchases without the cardholder's authorization. Credit card fraud is successful because the chances of being caught are small and prosecution is not ensured. Retailers have identified credit card thieves and contacted law enforcement, but they often receive little or no response regarding the crime." (p. 1.1014). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Counterfeiting Checks "An effective check counterfeiting operation can turn a small financial investment into a fortune within a short time frame. This can be done without high levels of computer expertise or expensive software. Often, all that is required is a quality computer, a color inkjet printer, check format and MICR font software, magnetic ink cartridges, and paper stock. Check counterfeiters commonly recruit other individuals to cash the fraudulent checks. This allows the suspects to distance themselves from the transaction and avoid being identified by law enforcement. In many cases, the people presenting the checks have no identifying information about the actual counterfeiters." (p. 1.1002). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Check Theft "Three types of check theft are: using stolen canceled checks and statements to obtain new checks, check washing, and stealing blank check stock. - Stolen canceled checks and statements—Although a stolen canceled check cannot be negotiated, it does have fraud implications. Using a stolen canceled check or check statement, a fraudster can order checks from a mail-order check printer and have them sent to a mail drop address. Checks can then be

Fraud Risk Exposure and Description
written on the new stock and cashed using false identification. - Check washing—Check washing is a type of check fraud that involves using acid-based chemicals found in common household products to erase particular pieces of information, such as payee name or amount, being careful not to alter the check issuer's signature. The check is allowed to dry, after which a new payee and payment amount are inscribed. Fraudsters who perpetrate check washing schemes usually write the checks for relatively modest amounts to decrease scrutiny and reduce the chance of exceeding the check issuer's account balance. Because checks written using colored inks and ball-point pens tend to be most susceptible to the chemicals used in these schemes, experts recommend using black ink and gel pens. - Stolen check stock—Professional thieves using sophisticated methods steal blank check stock already encoded with customer account information, which makes passing the check even easier. Corporate checks are the most likely target since they are easily cashed and deposited." (p. 1.1004). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Stop Payment Orders "Stop payment orders involve individuals who use a check to purchase an expensive item from a retail establishment and then notify their bank to stop payment on the check. Savvy check fraudsters might even contact the merchant, saying the item was defective and that the establishment can expect to hear from the customer's legal representative. Meanwhile, the check passer sells the item for a profit. In another scenario, after purchasing the item and notifying the bank to stop payment, the fraudster goes back to the store to return the item and receive a full refund. The merchant refunds the amount in cash but never receives payment from the fraudster's bank. " (p. 1.1004). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Unauthorized Use of a Lost or Stolen Card Fraudulent activity normally occurs within hours of the loss or theft, before most victims have called to report the loss. Victims are commonly unaware that their credit cards are being used fraudulently until they review their monthly statement. It is important that victims report the loss or theft of their card within 60 days of receiving the statement with the fraudulent charges to avoid being held responsible for more than $50 worth of charges made during that time frame. If the credit card number

Fraud Risk Exposure and Description
is compromised but the physical card is not stolen, the consumer is not liable for any charges if reported within 60 days. If the credit card company is not notified of the theft and the card is used, the customer is liable for any charges." (p. 1.1014). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Counterfeit Credit Cards "Another type of bankcard fraud involves the illegal counterfeiting of credit cards. Known as blank plastic cards, this scheme uses credit-card-sized plastic with embossed account numbers and names. This scheme works in conjunction with a corrupt and collusive merchant or a merchant's employee. Other counterfeit cards are wholly manufactured using high-speed printing facilities and are used in association with organized crime groups." (p. 1.1015). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Mail Theft "Mail theft is another method that identity thieves use to obtain personal and business information. Fraudsters can steal mail from public mailboxes or the private mailboxes of individuals and businesses. Private mailboxes are often unsecured, making mail theft easy. Public mailboxes usually have security features, such as locks and specially designed mail slots, but determined thieves can circumvent these features. In addition, mail carriers and other postal workers are sometimes accomplices in mail theft schemes. Both incoming and outgoing mail can provide useful information for identity thieves. Incoming mail might contain bills, financial statements, insurance information, or solicitations for pre-approved credit cards. Outgoing mail often contains checks or other payments, along with statements that include the customer's account, bank, or credit card number. A lucky fraudster might even find a money order in outgoing mail." (p. 1.809). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Insurance Fraud "The insurance business, by its very nature, is susceptible to fraud. Insurance is a risk distribution system that requires the accumulation of liquid assets in the form of reserve funds, which are in turn available to pay loss claims. Insurance companies generate a large steady flow of cash through insurance premiums. Steady cash flow is an important economic resource that is very attractive and easily diverted. Large accumulations of liquid assets make insurance companies attractive for takeover and loot schemes. Insurance companies are under great pressure to maximize the return on investing the reserve funds, thus making them vulnerable to high-yielding investment schemes." (p. 1.1101). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Cash, Loan, and Dividend Payments "A company employee requests cash, a loan, or a dividend payment without the knowledge of an insured or contract holder and either deposits the money into his bank account or into a fictitious account. To minimize his chances of being detected committing a fraudulent act, the employee might change the company policyholder's address of record to either his address or a fictitious address. Once the payment is issued, the address is then changed back to the previous address." (p. 1.1102). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Settlement Checks "Company employees can misdirect settlement payments such as Matured Endowment, Paid Up, etc., to the branch office, to their homes, or to fictitious addresses. The employee can easily create a payment defalcation by changing the address of record prior to the settlement payment issue date, thus misdirecting the payment in question. Also, an orphan contract holder might be transferred to his agency periodically, affording the opportunity to improperly request the issuance of a settlement payment. An orphan contract holder is a policyholder or contract holder who has not been assigned to a servicing agent or the whereabouts of whom are unknown. The servicing agent attempts to locate this family group and can possibly influence them to purchase additional insurance.

Fraud Risk Exposure and Description
A clerical support employee might receive notification that the orphan contract holder does not reside at the given address. This will give the support staffer an opportunity to change the address to either his home or a fictitious address and possibly create a fraud." (p. 1.1102). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Premium Diversion "An agent collects the premium but does not remit the payment to the insurance company. Thus, the insured unknowingly has no coverage available upon a qualifying event." (p. 1.1102). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Fictitious Payee "An agent or a clerk can change the beneficiary on record to a fictitious person and subsequently submit the necessary papers to authorize the issuance of a payment." (p. 1.1103). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Fictitious Death Claim An agent or employee obtains a fictitious death certificate and requests that a death claim payment be issued. The agent then steals the payment. The sales representative can also write a fictitious application and, after the contestable period (two years), submit a phony death claim form and obtain the proceeds. The agent, by investing a small amount, could receive a much larger sum in misappropriated claims. A company is particularly vulnerable to this scheme if the perpetrator has knowledge of the underwriting procedures, such as the limits under which insurance can be written without a medical exam and what should be submitted on a death claim." (p. 1.1103).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Underwriting Misrepresentation "Misrepresentation might occur if a sales representative knowingly makes a false statement with the intent to deceive the prospective insureds in order to obtain an unlawful gain." (p. 1.1104). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Vehicle Insurance — Staged Accidents "This scheme involves the fabrication of an automobile accident that only exists on paper. When the repair costs are small (e.g., less than $1000), many insurance companies do not bother to send an investigator to examine the vehicle. Because this is a low-risk endeavor and the authorities are not involved, this scheme is very popular within organized crime rings." (p. 1.1106). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Vehicle Insurance — Inflated Damages "The business environment and the competition for work in the automobile repair industry have motivated a scheme where some establishments inflate the estimated cost to cover the deductible. The insured is advised by the repair shop that the shop will accept whatever the company authorizes." (p. 1.1108). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Rental Car Fraud

Fraud Risk Exposure and Description
"A person does not need to own a vehicle to commit automobile fraud. There are several schemes that can be perpetrated using rental cars. The most prevalent involve property damage, bodily injury, and export fraud." (p. 1.1108). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Pension Fraud "Pension fraud involves the use of deceit or misrepresentation in connection with a pension claim. Pension fraud frequently involves one of two situations: • Fraud involved in the providing of pension benefits or payments • Fraud aimed at stealing a person's pension funds The first type of pension fraud generally involves conflicts between a worker and their employer. The dispute may involve claims that the employer has acted fraudulently in providing or denying pension benefits." [**Source:** Legal Match, https://www.legalmatch.com/law-library/article/pension-fraud.html] Return to Table
Inflated Final Income Used in Benefit Calculation The annual pension benefit is calculated based on the multiplication of three factors: "final average income" (depending on the pension system), "benefit percentage," and "years of plan membership." However, inserting inflated final income, which is not true to the specific income measurement in the formula leads to a higher pension benefit amount payable to employees. [**Source:** National Public Pension Coalition, https://protectpensions.org/2016/06/30/pension-benefits-calculated] Return to Table
Under-Reported Income in Years Not Used for Benefit Calculation Failing to report all incomes in years and inconsistently using a different total amount of income for favorable benefit calculation.

Fraud Risk Exposure and Description
[**Source:** Sapling, **https://www.sapling.com/5647261/calculate-pension-benefits**] Return to Table
False Service Reported for Service Purchase "A member's retirement allowance is based in part on the amount of service credit posted to the member's account at the time of retirement. It may be beneficial, therefore, to purchase eligible service credit in order to enhance retirement benefits or to qualify for certain types of retirement." Therefore, people report false service to add more service credit and increase more benefit qualification. [**Source:** EPBAM, http://www.state.nj.us/treasury/pensions/epbam/pensions/purchases/purchase.htm] Return to Table
Enrolling Ineligible Persons "A broker might seek to add ineligible family members, partners, or associates to a group policy by representing them as employees" (p.1.1259). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Not Enrolling All Eligible Persons Although some employees are eligible for a pension, a company or an employer does not enroll persons who qualify for the defined benefit retirement plan. [**Source:** The Balance, https://www.thebalance.com/how-do-i-get-a-pension-2388814] Return to Table
Inventory Fraud "Employees target inventory, equipment, supplies, and other noncash assets for theft in a number of ways. These schemes can range from stealing a box of pens to the theft of millions of dollars' worth of

Fraud Risk Exposure and Description
company equipment. The term inventory and other assets is meant to encompass the misappropriation schemes involving any assets held by a company other than cash" (1.501). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Off-Site or Fictitious Inventory "Fictitious inventory schemes usually involve the creation of fake documents, such as inventory count sheets and receiving reports. Many inventory reports are kept electronically, which allows the fraud examiner to total columns and perform data analysis techniques to detect these types of inventory fraud schemes" (p.1.224). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Purchasing and Receiving Falsification "Dishonest employees can also manipulate the purchasing and receiving functions of a company to facilitate the theft of inventory and other assets" (p.1.506). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Misuse of Inventory "There are basically two ways a person can misappropriate a company asset. The asset can be misused or it can be stolen. Simple misuse is obviously the less egregious of the two. Assets that are misused but not stolen typically include company vehicles, company supplies, computers, and other office equipment" (p.1.501). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Theft of Inventory "Though the misuse of company property might be a problem, the theft of company property is obviously of greater concern. Losses resulting from larceny of company assets can run into the millions of dollars. Most schemes where inventory and other noncash assets are stolen fall into one of four categories: larceny schemes, asset requisition and transfer schemes, purchasing and receiving schemes, and false shipment schemes" (p.1.502). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
False Shipments "To conceal thefts of inventory and other assets, employees sometimes create false shipping documents and false sales documents to make it appear that the inventory they take was sold rather than stolen. The document that tells the shipping department to release inventory for delivery is usually the packing slip. By creating a false packing slip, a corrupt employee can cause inventory to be fraudulently delivered to himself or an accomplice. The "sales" reflected in the packing slips are typically made to a fictitious person, a fictitious company, or the perpetrator's accomplice" (p.1.507-508). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Concealing Inventory Shrinkage "When inventory is stolen, the perpetrator's key concealment issue is shrinkage. Inventory shrinkage is the unaccounted-for reduction in the company's inventory that results from error or theft. For instance, assume a computer retailer has 1,000 computers in stock. After work one day, an employee loads ten computers into a truck and takes them home. Now the company only has 990 computers, but since there is no record that the employee took ten computers, the inventory records still show 1,000 units on hand. The company has experienced inventory shrinkage in the amount of ten computers.

Fraud Risk Exposure and Description
Shrinkage is one of the red flags that signal fraud. The perpetrator's goal is to proceed with his scheme undetected, so it is in his best interest to prevent anyone from looking for missing assets. This means concealing the shrinkage that occurs from asset theft" (p.1.511). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Theft of Intellectual Property "Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions—known as "intellectual property"—which can include everything from trade secrets and proprietary products and parts to movies, music, and software." [**Source:** FBI, https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft Return to Table
Espionage "Espionage refers to the use of illegal, clandestine means to gather information; therefore, it does not cover legitimate intelligence collection and analysis using legal means. Espionage, however, can be further subdivided into two categories: traditional and industrial. Traditional espionage refers to government-sponsored or sanctioned espionage conducted to collect protected information from a foreign government. Industrial espionage (also known as corporate espionage) is the term used to describe the use of illegal, clandestine means to acquire information for commercial purposes" (p.1.702). "Organizations that perform research and development (R&D) are at risk of corporate espionage because the value of R&D data depends on its exclusivity. Often, intelligence professionals target R&D employees because their positions generally involve the communication of information. For example, many R&D employees attend or participate in trade shows, conferences, or other industry functions where it is common to network with other professionals in their field and exchange ideas. Such events provide intelligence spies with the opportunity to learn key product- or project-related details simply by listening to a presentation or asking the right questions. R&D employees' publications are also a good source of information for intelligence professionals. Researchers sometimes inadvertently include sensitive project details when writing articles about their findings for industry journals or other mediums. This is particularly true in the case of academic professionals who might be hired by a company to perform research or conduct a study. If a company hires an academician to conduct research, management must make sure that the academician understands the need to keep the results confidential. In addition, management must make sure that the academician's use of teaching assistants or graduate students is kept to a minimum and that those individuals understand the confidentiality requirements." (p. 1.713).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Spying

"A spy is an individual who is intentionally placed in a situation or organization to gather intelligence. A well-placed corporate spy can provide intelligence on a target organization's product development, product launches, and organizational developments or changes. Spies are common in foreign, business, and competitive intelligence efforts" (p.1.738).

"Often, a corporate spy will try to obtain information by recruiting an existing insider to act as his agent on the inside. An employee recruited to spy against his employer is known as a mole. The mole agrees to betray his employer's trust by handing over confidential information that belongs to his or her organization."

"A corporate spy might recruit a mole through any of the following techniques:"

- "Bribe the target."
- "Extort (blackmail) the target."
- "Use romantic or sexual seduction."
- "Exploit the target's strong social or political feelings."
- "Convince the target that spying is moral or justified. These attacks often target people who feel like victims. An employee who is bitter at having been passed over for a promotion, for example, is a good target. Other typical targets include employees who resent their employers because they feel underpaid or unrecognized."
- "Trap a target so that he is essentially forced to spy on his employer."

"Because corporate spies use complex methods to turn employees into moles, management must train employees, especially key employees with access to valuable information, to report any suspected recruitment effort made against them as early as possible. Specifically, management must train key employees to be wary of people who:"

- "Encourage and finance an employee's vice."
- "Express a great deal of sympathy for a cause that is important to an employee."
- "Offer to help an employee with a serious financial problem."
- "Attempt to seduce an employee."
- "Attempt to blackmail an employee" (p.1.715-716).

[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Return to Table

Fraud Risk Exposure and Description
Informants "Spies might develop a network of paid informants who can obtain transactional intelligence on their behalf. These informants come from a wide range of businesses and include:" • "Travel agents" • "Airline reservation personnel" • "Major credit card companies" • "Staff at major Internet providers" • "Employees at video, music, and other entertainment outlets" • "Staff of adult entertainment providers that the target frequents" • "Telephone company employees with access to telephone records" • "Employees of commercial database providers such as Dialog and Dun & Bradstreet who have access to transactional records" "These informants will, for a fee, provide transactional intelligence on a subject that can tell a corporate spy about:" • "A person's vices" • "Details of a target's business travel" • "Hotels where the target stayed and where he is likely to stay again in the future (this can be useful for setting up surveillance)" • "Whom the target has called" • "Interests and hobbies (another way to edge into the target's confidence)" • "Companies or subjects the target has researched" (p.1.718-719) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Infiltration "Corporate spies might use physical infiltration techniques to obtain sensitive information. Physical infiltration is the process whereby an individual enters a target organization to spy on the organization's employees. Often corporate spies use physical infiltration when there is a tight time schedule, a lack of available recruits, or expense constraints; however, a spy might also use physical infiltration when he has specialized knowledge that makes him the best spy for the job. Generally, spies with advanced technical knowledge are the best at committing such campaigns" (p.1.717). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Loss of Information "Information thieves use a wide variety of methods—not all of which are legal—to gain access to an organization's business secrets. The following are common ways for information to fall into the wrong hands:" • "Accident and negligence" • "Loss of physical media" • "Poor information security procedures" • "Improper disposal of documents and media" • "Malicious insiders" • "Insider spies (moles)" • "Sleepers" • "Computer attacks" • "Physical infiltration" • "Transactional intelligence" • "Social engineering" • "Physical surveillance" • "Technical surveillance" (p.1.713-714) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Trash and Waste Disposal Searches "Intelligence professionals can obtain sensitive information by dumpster diving, a practice that involves looking through someone else's trash (e.g., via dumpsters and other trash receptacles). A company's dumpsters might contain financial statements or other confidential documents" (p.1.706) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Surveillance

Fraud Risk Exposure and Description
"Intelligence professionals can conduct surveillance-the planned observation of people, places, or objects-to obtain information about targets" (p.1.706). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Destruction of Customer Goodwill "Goodwill may be defined as the attractive force that brings in customers and adds to the value of a business. It includes a business's reputation and its relations formed with its customers. It may arise from the nature or location of the business. IP and goodwill are particularly vulnerable to being stolen or damaged by rogue or opportunistic employees, because of the knowledge they obtain in their employment. There are many cases where employees have caused grave damage to their employer's business by setting up their own business in competition and pinching their employer's IP and customers." **[Source:** B2B Lawyers, http://www.b2blaw.com.au/insights/14-protecting-ip-and-goodwill-from-rogue-employees-3-december-2012] Return to Table
Compromising Vendor Relationships "Contracting with an outside third party subjects organizations to risks with the potential for significant financial and reputational harm, such as from fraud, breach of contract, error, breach of confidentiality, data loss and so on. The risks associated with vendor relationships, however, can be unique and vary depending on the vendor as well as the service or process outsourced. Common areas for vendor risks include" • Strategic risks • Reputation risks • Industry risks • Geographical risks • Compliance risks (e.g., the Sarbanes-Oxley Act, the Foreign Corrupt Practices Act, the UK Bribery Act, the Health Insurance Portability and Accountability Act) • Operational risks • Transaction risks • Credit risks [**Source**: ACFE, http://www.acfe.com/fraud-examiner.aspx?id=4294972428] Return to Table
Proprietary Business Opportunities

Fraud Risk Exposure and Description
"A proprietary deal lets a specific vendor have a first chance to obtain business opportunities before these opportunities are presented to other vendors by a firm. Proprietary business opportunities are often presented to specific vendors based on their perceived fit with the company. While they can be cost effective and closed more quickly than an auctioned process, the total contract value and/or overall deal structure may not maximize value for the entity." [**Source:** Divestopedia, https://www.divestopedia.com/definition/721/proprietary-deal] Return to Table
Corruption "Corruption is a term used to describe various types of wrongful acts designed to cause an unfair advantage. It can take on many forms, including bribery, kickbacks, illegal gratuities, economic extortion, and collusion. Generally, it involves the wrongful use of influence to procure a benefit for the actor or another person, contrary to the duty or the rights of others. The various forms of corruption are often used in combination, which reinforces the schemes' potency and makes them more difficult to combat. Corruption can be found in any business or organization, and it is one of the three major categories of occupational fraud and abuse (along with asset misappropriation and fraudulent statements). The most common area for corruption in an organization is in the purchasing environment, and most corruption schemes involve employees acting alone or in collusion with vendors/contractors. Corruption is a significant problem for organizations, particularly due to the drive for growth in international markets. Despite the multitude of anti-corruption legislation and increased enforcement efforts around the world, corruption is still prevalent" (p.1.601). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Bribery and Illegal Gratuities "Bribery is a form of corruption that may be defined as the offering, giving, receiving, or soliciting of anything of value to influence an act or a decision. Bribery schemes are classified into two types: official bribery and commercial bribery" (p.2.205). "Illegal gratuities are items of value given to reward a decision, often after the recipient has made the decision. Illegal gratuities are similar to official bribery schemes, and most illegal gratuity laws outlaw gratuities in the public sector." "In general, the elements of an illegal gratuity are:"

Fraud Risk Exposure and Description
• "A thing of value" • "Given, offered, or promised to (or demanded, sought, received, or accepted by)" • "A (present, former, or future) public official" • "For or because of any official act performed or to be performed by that public official" "The major difference between an official bribe and an illegal gratuity is that an illegal gratuity charge does not require proof that the gratuity was given for the purpose of influencing an official act. That is, an illegal gratuity charge only requires that the gratuity be given for, or because of, an official act" (p.2.207). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Commercial Bribery "Commercial bribery refers to the corruption of a private individual to gain a commercial or business advantage. That is, in commercial bribery schemes, something of value is offered to influence a business decision rather than an official act" (p.2.206). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Official Bribery/Bribery of Public Officials "Official bribery refers to the corruption of a public official to influence an official act of government. Illegal payments to public officials can be prosecuted as official bribery, and they can give rise to stiff penalties. The elements of official bribery vary by jurisdiction, but generally include:" • "The defendant gave or received (offered or solicited) a thing of value." • "The recipient was (or was selected to be) a public official." • "The defendant acted with corrupt intent." • "The defendant's scheme was designed to influence an official act or duty of the recipient" (p.2.205). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table

Fraud Risk Exposure and Description
Receipt of Bribes, Kickbacks, and Gratuities "Employees from contractors and vendors receive money, gifts, or gratuities in order to influence a business transaction and to be rewarded for providing favorable treatment or services to another party. These schemes Involve collusion between employees and third parties and usually attack the purchasing function of the victim company. They can be very difficult to be detected" (p.1.602-603). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Kickbacks "Bribery often takes the form of kickbacks, a form of negotiated bribery in which a commission is paid to the bribe-taker in exchange for the services rendered. Thus, kickbacks are improper, undisclosed payments made to obtain favorable treatment. In the government setting, kickbacks refer to the giving or receiving of anything of value to obtain or reward favorable treatment in relation to a government contract. In the commercial sense, kickbacks refer to the giving or receiving of anything of value to influence a business decision without the employer's knowledge and consent" (p.1.602). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Overbilling Schemes "In overbilling schemes, the payer adds a corrupt payment to a legitimate business expense or trade payable. And subsequently, a cooperative third party then either forwards the excess payment directly to the intended recipient or returns it, usually in cash, to the payer for distribution. Thus, illicit funds might be added to legitimate payments for goods or services provided by actual suppliers, subcontractors, engineers, and agents, with the additional amounts being passed on by the supplier or returned to the payer (usually in cash) for distribution" (p.1.622). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Illegal Payments: Gifts, Travel, Entertainment

Fraud Risk Exposure and Description
"Often, corruption schemes involve corrupt payments—items of value paid to procure a benefit contrary to the rights of others. There are various ways to make corrupt payments, and many do not involve money. Any tangible benefit given or received with the intent to corruptly influence the recipient can be an illegal payment, but there are certain traditional methods of making corrupt payments that fall into the following hierarchical categories." "Gifts, Travel, and Entertainment" "Most bribery and corruption schemes begin with gifts and favors. Common early gifts and favors include:" • "Wine and liquor (consumable)" • "Clothes and jewelry for the recipient or spouse" • "Sexual favors" • "Lavish entertainment" • "Paid vacations" • "Free luxury transportation" • "Free use of resort facilities Gifts of the briber's inventory or services, such as construction of home improvements by a contractor" (p.1.609). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Loans "Corrupt payments often take the form of loans. Three types of loans often turn up in corruption cases:" • "An outright payment that is falsely described as an innocent loan" • "A legitimate loan in which a third-party—the corrupt payer—makes or guarantees the loan's payments" • "A legitimate loan made on favorable terms (e.g., an interest-free loan)" (p.1.610) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Credit Card Payments for Personal Items "A corrupt payment can be in the form of credit card use or payments toward a party's credit card debt. The payer might use a credit card to pay a recipient's transportation, vacation, or entertainment

Fraud Risk Exposure and Description
expenses, or the payer might pay off a recipient's credit card debt. In some instances, the recipient might carry and use the corrupt payer's credit card" (p.1.610). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Transfers for Other than Fair Value "Corrupt payments might occur in the form of transfers for a value other than fair market. In such transfers, the corrupt payer might sell or lease property to the recipient at a price that is less than its market value, or the payer might agree to buy or rent property from the recipient at inflated prices. The recipient might also "sell" an asset to the payer but retain the title or use of the property" (p.1.610). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Favorable Treatment "Corrupt payments might come in the form of promises of favorable treatment. Such promises commonly take the following forms:" • "A payer might promise a government official lucrative employment when the recipient leaves government service." • "An executive leaving a private company for a related government position might be given favorable or inflated retirement and separation benefits." • "The spouse or other relative of the intended recipient might also be employed by the payer company at an inflated salary or with little actual responsibility" (p.1.610-611). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Conflicts of Interest "A conflict of interest occurs when an employee or agent—someone who is authorized to act on behalf of a principal—has an undisclosed personal or economic interest in a matter that could

Fraud Risk Exposure and Description
influence his professional role. These schemes involve self-dealing by an employee or agent and can occur in various ways. For example, a conflict might occur when an employee accepts inappropriate gifts, favors, or kickbacks from vendors, or when an employee engages in unapproved employment discussions with current or prospective contractors or suppliers." "Conflict of interest schemes generally constitute violations of the legal principle that an agent or employee must act in good faith, with full disclosure, and in the best interest of the principal or employer. An agent is any person who, under the law, owes a duty of loyalty to a principal or employer. Agents include officers, directors, and employees of a corporation; public officials; trustees; brokers; independent contractors; attorneys; and accountants. A principal is an entity that authorizes an agent to act on its behalf. In a principal-agent relationship, the agent acts on behalf of the principal. The agent should not have a conflict of interest in carrying out the act on the principal's behalf." "Conflicts of interest do not necessarily constitute legal violations, as long as they are properly disclosed" (p.1.627, 1.629). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Purchases "Many times, conflicts of interest arise in the purchasing process. A corporate employee or agent who has an undisclosed, potentially adverse interest in a customer or supplier might be tempted to favor his own or the third party's interests over the corporation's interests" (p.1.630-631). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Sales "There are two principal types of conflict schemes associated with sales of goods or services by the victim company: underselling and writing off sales." "Also, many employees who have hidden interests in outside companies sell goods or services to these companies at below-market prices. This results in a diminished profit margin or even a loss for the victim organization, depending upon the size of the discount" (p.1.633).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Business Diversion "A number of employees end up starting their own businesses that compete directly with their employers, and when this occurs, such employees might begin siphoning off clients for their own business. This activity clearly violates the employee's duty of loyalty to the employer, and frequently violates the company's internal policies. There is nothing unscrupulous about free competition, but while a person acts as a representative of his employer, it is improper for him to try to take his employer's clients. Normal standards of business ethics require employees to act in the best interests of their employers" (p.1.634). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Resourcing "Some employees divert the funds and other resources of their employers to the development of their own businesses. This kind of scheme involves elements of both conflicts of interest and fraudulent disbursements" (p.1.635). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Financial Disclosure of Interest in Vendors/Suppliers "Sometimes an employee has a direct or indirect financial interest in a company (vendors or suppliers) under his supervision." "Management has an obligation to disclose to the shareholders significant fraud committed by officers, executives, and others in positions of trust, but misplaced loyalties might prevent management from making such disclosures." "The inadequate disclosure of conflicts of interest is among the most serious of frauds. Inadequate disclosure of related-party transactions is not limited to any specific industry; it transcends all business types and relationships" (p.1.635).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Bid Rigging "In simple terms, bid rigging is fraud which involves bidding. It is an agreement among competitors as to who will be the winning bidder. Bid rigging occurs when a purchaser solicits bids to purchase goods or services. The bidders agree in advance who will submit the winning bid. The purchaser, which depends on competition between the bidders to generate the lowest competitive price, receives instead a "lowest bid" that is higher than the competitive market would bear." [**Source:** Department of Justice, https://www.justice.gov/atr/preventing-and-detecting-bid-rigging-price-fixing-and-market-allocation-post-disaster-rebuilding] Return to Table
Embezzlement "Embezzlement is the wrongful appropriation of money or property by a person to whom it has been lawfully entrusted (or to whom lawful possession was given). Embezzlement involves a breach of trust, although it is not necessary to show a fiduciary relationship—a relationship of confidence, trust, or good faith—between the parties. The elements of embezzlement vary somewhat by jurisdiction, but generally are:" "The defendant took or converted" "Without the knowledge or consent of the owner" "Money or property of another" "That was entrusted to the defendant (the defendant had lawful possession of the property)" (p.2.211) [**Source**: Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
False Accounting Entries "Some employees are in positions of trust in which they have the ability to use or relocate funds on behalf of customers or the financial institution itself. In false accounting entry schemes, employees

Fraud Risk Exposure and Description
debit the general ledger to credit their own accounts or cover up a theft from a customer account" (p.1.901). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Unauthorized Withdrawals "In a relatively simple scheme, employees make unauthorized withdrawals from customer accounts. These schemes are hard to conceal because the customer will complain, but the subject might plan to flee once the funds are transferred or target a customer who is unlikely to notice the missing funds right away" (p.1.902). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Unauthorized Disbursements "Employees might abuse their authority to approve fraudulent (counterfeit, forged, stolen, etc.) instruments or otherwise make an unauthorized disbursement of funds to an outsider. While the employee often has a financial incentive for doing so, there have been many cases where the employee made an improper disbursement in a misguided attempt to be cooperative with customers" (p.1.902-903). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Paying Personal Expenses from Bank Funds "An officer or employee causes the bank to pay personal bills and then causes amounts to be charged to bank expense accounts" (p.1.903).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Unrecorded Cash Payments "A director, officer, or employee causes cash to be disbursed directly to himself or accomplices and does not record the disbursements" (p.1.903). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Theft of Physical Property "Employees or contractors remove office equipment, building materials, and furnishings from bank premises" (p.1.903). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Moving Money from Dormant Accounts "Persons with apparent authority create journal entries or transfer orders not initiated by customers to move money among accounts. The accounts used are typically dormant or inactive accounts, which are those accounts that show little or no activity. Often, contact with the account holder by confirmation, letter, or telephone is not possible. Such accounts are to be transferred to dual control and recorded in an inactive accounts ledger." "Dormant funds are highly susceptible to embezzlement. The rationale is that funds embezzled from active accounts are likely to be missed quickly, while dormant account holders are less likely to report problems. Many financial institutions lock dormant accounts after a certain time period (e.g., one year of inactivity), requiring manual override to conduct additional transactions. However, this process can be manipulated. Typically, the perpetrator first identifies accounts that are or are about to be dormant. Next, he might somehow manipulate the account to make it appear that it is not dormant, such as by creating a nominal and fictitious transaction. Then, the employee creates journal entries or transfer orders to move the funds into an account that the employee controls (often a shell organization)" (p.1.903).

Fraud Risk Exposure and Description
[**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Contract, Grant, and Procurement Fraud "The procurement system is the collection of processes, procedures, and entities involved in purchasing goods and services by public or private entities. And because the primary objective of an effective procurement policy is to achieve the best value of money, it is important that procurement processes avoid incidences of fraud." [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] **Note**: Many of the frauds schemes discussed elsewhere can also occur in the procurement process. In particular, many of the Corruption schemes involve the procurement process. Return to Table
Comingling of Contracts "Dishonest contractors can submit multiple bills on different contracts or work orders for work performed or expenses incurred only once. A contracting official can facilitate the scheme and share in the profits by writing similar work orders under different contracts and accepting the multiple billings." [**Source:** IACRC, The Most Common Procurement Fraud Schemes and Their Primary Red Flags, W. Michael Kramer; http://iacrc.org/procurement-fraud/the-most-common-procurement-fraud-schemes-and-their-primary-red-flags/ Return to Table
Product Substitution Nonconforming goods or services fraud, also known as product substitution or failure to meet contract specifications, refers to attempts by contractors to deliver goods or services to the procuring entity that do not conform to the underlying contract specifications. Once contractors deliver goods that do not

Fraud Risk Exposure and Description
conform to the contract, they bill and receive payment for conforming goods or services without informing the purchaser of the deficiency. These schemes can involve a wide variety of conduct, but generally they include any deliberate departures from contract requirements to increase profits or comply with contract time schedules. An unintentional failure to meet contract specifications is not fraud, but it might constitute a breach of contract. But a contractor who knowingly delivers goods or services that do not meet specifications might be guilty of fraud if he falsely represents that he has complied with the contract or deliberately conceals his failure to do so." (p. 1.1524). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
False or Inflated Invoices or Claims **Submitting False Invoices** "Once a shell company has been formed and a bank account has been opened, the corrupt employee begins billing his employer. Invoices can be easily generated on a personal computer. False invoices do not have to be of professional quality to generate fraudulent disbursements." (p. 1.439). **False Claims and Statements** "Though there is a statute specifically designed to combat false claims in connection with health care benefits programs, the federal false claims statutes may be used to combat certain types of health care fraud. Some examples of false claims and statements include: - Falsified contractor qualifications - False certifications or assurances - False records or invoices - Invoices from nonexistent companies - Claims made in duplicate or altered invoices - Billing for fictitious employees - Billing for goods and services not provided - Inflated costs or substitution of cheaper goods Although these statutes are discussed in more detail in the Law section of the Fraud Examiners Manual, this discussion will provide a brief overview of the main false claims and statements statutes used to combat health care fraud, including: false statements under Section 1001, the criminal False Claims Act, and the Civil False Claims Act." (1.1212). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Change Order Abuse

Fraud Risk Exposure and Description
"In the course of many projects, such as road repair or building construction, unanticipated changes in conditions can result in the parties agreeing to amend the contract terms after signing, perhaps to increase their scope or cost. This is known as a change order. Change orders can have the same impact on a project as altering the original documents. As with anything that is contracted for on a bid basis, change orders could also be an indication of collusive bidding. A common change order abuse scenario involves collusion between the contractor and personnel from the procuring entity. The corrupt contractor submits an artificially low bid to ensure that he is awarded the contract (often with inside knowledge of competing bid amounts), but after the procuring entity awards the contract, the corrupt contractor increases the contract price with subsequent change orders. Furthermore, change orders might be an indication that the original project was not feasible and that shortcuts are shoring up other problem areas. Change orders should be approved by the architect and engineer on the project in addition to the lender's inspector. Loan fraud schemes involving project management often involve the use of change orders, so it is important to be able to recognize red flags in this area. The necessity for change orders can vary widely, depending on the type of project. Ultimately, the key characteristic that the fraud examiner should look for in change orders is abnormality, which can come in many forms. Change orders are often submitted along with draw requests. Although many times the change orders represent legitimate construction changes (for design, cost, or other things), they can also be indicators of fraud schemes. An increasing trend in the number of change orders or amounts on change orders might be an indication that construction changes have taken place that would alter the originally planned project to such an extent as to render the underwriting inappropriate. Alternatively, some projects—especially large projects—tend to have many change orders. It might be more abnormal in situations like these to have few change orders or none at all than to have many. For instance, a lack of change orders for a large project might suggest that progress is not actually being made. Fraud examiners should discover what the normal trend for change orders is in terms of both quantity and content with the particular type of industry and project, and then they can look for deviations from those trends. Change orders generally receive less scrutiny than the process used to acquire the underlying contract, making them a popular way to fraudulently access funds or generate funds for kickbacks. Even though change orders are often inevitable and can develop for legitimate reasons (e.g., change in scope, weather delays, building code changes), fraud examiners should review all contract change orders carefully." (p. 1.912). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Cost Mischarging

Fraud Risk Exposure and Description
"Cost mischarging schemes, which take place during the performance stage of the procurement process, occur when a contractor charges the procuring entity for costs that are not allowable, not reasonable, or cannot be allocated to the contract directly or indirectly. Often, contractors contend that a cost mischarge was merely a mistake, and the issue as to whether a mischarge was a mistake or a crime often depends on the contractor's intent. Thus, when investigating cost mischarging schemes, fraud examiners should investigate the issue of intent. Here are some common methods contractors use to mischarge costs: • Charging the same cost to more than one contract • Charging nonexistent costs or costs at inflated amounts • Charging unallowable costs (e.g., entertainment or advertising) to the contract • Charging costs to the wrong category or contract • Failing to disclose discounts and credits • Using outdated standard costs • Colluding with contractors directly to charge high prices and rebating part of the price increase without disclosure • Using phantom suppliers to inflate costs • Falsifying supporting documentation" (p. 1.1529). [**Source:** Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Multiple Claims – the requesting of payment for a single cost on different contracts or multiple times on the same contract. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Failure to Credit/Refund – the requesting of payment without reducing the amount equal to the credit or refund when required under the contract. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table

Fraud Risk Exposure and Description
Fraudulent Indirect Cost – is knowingly charging costs that are not "allowable, allocable or reasonable" in accordance with the cost accounting standards (CAS). [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Defective Manufacturing - knowingly providing a product that was not manufactured as required under the terms of the contract. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Anti-Competitive or Anti-Trust Schemes [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Bid-Rotation – a conspiracy by bidders to submit a pattern of bids that allow their pre-selected contractor to win the contract on a rotating basis. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Complementary Bidding – all bidders secretly agree to submit high cost bids. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Market Sharing – several bidders divide-up competitive markets or product lines and agree to not compete against each other. [**Source:** Procurement Integrity Consulting Services, LLC]

Fraud Risk Exposure and Description
Return to Table
Bid Suppression - one or more contractors convince other competitors from bidding. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Proposal Schemes [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Altering/Changing Submission – the modification of a proposal by an insider to ensure the selection of a preferred contractor. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Accepting Late Proposal – allowing the preferred contractor to submit a proposal after the due date for the purpose of sharing other bidders' information. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Unnecessary Rebidding – for the purpose of sharing other bidder's proposal information by an insider thereby allowing the preferred contractor to be selected. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Limiting Days to Submit - for the purpose of cutting down on potential competitors. [**Source:** Procurement Integrity Consulting Services, LLC]

Fraud Risk Exposure and Description
Return to Table
Unnecessary Pre-Qualification Criteria – to limit competition or disqualify potential competitors. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Unbalanced Proposal – when a bidder manipulates line item prices knowing the requirements for the line item will change after contract award. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Scoring Proposal – when a corrupt insider creates a scoring matrix that advantages the preferred contractor. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Contract Specifications/Requirements Schemes (Excluding/Including Bidders) [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Narrowing Requirements – a corrupt insider unduly narrows requirements allowing only a preferred contractor to be the logical selection. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Narrowing Specifications – a corrupt insider unduly narrows specifications allowing only a preferred contractor to be the logical selection.

Fraud Risk Exposure and Description
[**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Broadening Requirements – a corrupt insider unduly broadens requirements to qualify an otherwise unqualified bidder. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Broadening Specifications – a corrupt insider unduly broadens specifications to qualify an otherwise unqualified bidder. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Advertisement Schemes (Limiting Competition) [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Inadequate or Vague Publication Synopsis – by making the advertisement unclear qualified competitors will not dedicate corporate funds to prepare a proposal. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Using Obscure Publications – by using unknown publications or websites only those with insider information will learn of the solicitation. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table

Fraud Risk Exposure and Description
Advertisement during Holiday – by advertising over the holiday fewer qualified competitors will have an opportunity to submit a proposal. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Limiting days to Advertise - by limiting the days of advertisement fewer qualified competitors will have an opportunity to submit a proposal. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
False Representation Schemes [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
False Statement/Certification – a contractor knowingly makes a "material" false representation during some portion of the contracting process. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Defective Pricing – the failure to disclose accurate, current and complete pricing data in a contract proposal on cost type contract. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Progressive Payment – a contractor request payment for goods or services they intend to obtain or complete, but represent them as already purchased or completed.

Fraud Risk Exposure and Description
[**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Purchasing Schemes [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Purchases for Personal Use or Resale - an insider purchases items that are intended for his/her own use or for resale. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Purchase in Excess – the purchase of good or services in excess to help the seller in getting additional profit based on contracting conditions. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Split Purchases - an insider splits a single purchase into two or more purchases to remain below upper level review or competitive bidding thresholds. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Unnecessary Purchases – the purchasing of good or services without a valid requirement to help the seller in getting additional profit based on contracting conditions. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table

Fraud Risk Exposure and Description
Pass-through Purchases – an insider buying merchandise and reselling it to their own organization with inflated price. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Phantom Vendor – bids and proposals from non-existent competitors for the purpose of suggesting multiple vendors. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Leaking of Acquisition – acquisition sensitive information is secretly provided to a preferred contractor. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Unjustified Sole Source - an insider deliberately writes a non-supportable sole source justification to avoid a competitive selection. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Manipulation of Delivery - delaying the contract deliverable to allow unnecessary cost to be incurred. [**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Influence through Authority – using ones position within the organization to improperly direct procurement decisions over those with the true authority to decide.

Fraud Risk Exposure and Description
[**Source:** Procurement Integrity Consulting Services, LLC] Return to Table
Foreign Corrupt Practices Act (FCPA) Violations "The United States Congress originally enacted the Foreign Corrupt Practices Act (FCPA) in 1977 to prohibit making corrupt payments to foreign officials or political organizations. Since its enactment, the FCPA has had an enormous impact on the way organizations around the world conduct business. While only enforced by the United States, the FCPA is a law with international reach because businesses within its scope may violate the statute anywhere in the world. The FCPA has two principal components: the anti-bribery provisions and the accounting provisions" (p.2.234). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Anti-Bribery Provisions The FCPA's anti-bribery provisions make it unlawful for regulated parties (i.e., any citizen, national, or resident of the United States; any U.S. business entity; any company that has securities registered in the United States or is required to file reports with the Securities and Exchange Commission (SEC); and foreign nationals and businesses taking action in the United States) to bribe foreign government officials to obtain or retain business. Specifically, the provisions prohibit corrupt offers or payments to foreign government officials, political parties, political party officials or candidates, or to any person for payment to such foreign officials for an improper advantage" (p.2.234). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Books and Records Violations "The first major requirement of the accounting provisions is that all issuers must accurately record all transactions, keep receipts and other support for transactions, and keep records in a manner consistent with overall document retention and recordkeeping policies" (p.2.238). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.]

Fraud Risk Exposure and Description
Return to Table
Internal Control Weaknesses "The internal controls provision is designed to prevent unauthorized or unrecorded transactions. Under the internal controls provision, a company must maintain robust compliance policies and must take reasonable steps to ensure that its affiliates maintain suitable internal control" (p.2.238). "The SEC has considered several factors to determine the adequacy of a system of internal controls. The factors include:" • "The role of the board of directors" • "Communication of corporate procedures and policies" • "Assignment of authority and responsibility" • "Competence and integrity of personnel" • "Accountability for performance and compliance with policies and procedures" • "Objectivity and effectiveness of the internal audit function" (p.2.239) [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Money Laundering "Money laundering is the process of disguising the origins of illicit funds (e.g., illegal drug proceeds or unreported taxable income) and integrating them back into financial streams to make them appear legitimate. This process may involve anything from depositing illicit funds in secret offshore accounts to channeling the money through a legitimate "front" business" (p.2.373). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
False Statements "False Statements—18 U.S.C. § 1001" "Persons who violate the Bank Secrecy Act and other reporting laws might also be guilty of violating 18 U.S.C. § 1001, which is the principal federal false statements statute. Because most of the obligations imposed by the BSA involve recordkeeping and reporting, many BSA violations might also constitute false statements. Section 1001 prohibits knowingly falsifying,

Fraud Risk Exposure and Description
concealing, covering up, or making a false, fictitious, or fraudulent statement or representation in any matter within the jurisdiction of any U.S. department or agency. Violations of this section are often charged when an individual is stopped at the border with a large amount of unreported cash and responds falsely to the questions of customs officers or inspectors. It has been used to prosecute individuals for structuring a transaction so that it deceives a financial institution into filing a false report" (p.2.651). [**Source:** Association of Certified Fraud Examiners, *Fraud Examiners Manual.* Austin, TX: ACFE, 2018.] Return to Table
Aiding and Abetting Fraud by Other Parties (Customers, Vendors) **"Aiding and Abetting (18 U.S.C. § 2)"** "Section 2 of Title 18, U.S. Code, is the federal aiding and abetting statute, which provides that anyone who induces another to commit an offense or who aids in its commission may himself be charged and convicted of the underlying offense and subject to its penalties" (p.2.381). In this case, anyone including customers or vendors who induce or aid employees of an entity to commit an offense or fraud are subject to the title 18, U.S.C & 2. [**Source**: Association of Certified Fraud Examiners, Fraud Examiners Manual. Austin, TX: ACFE, 2018.] Return to Table
Insider Trading Buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information. [**Source:** Securities and Exchange Commission, "Fast Answers"] Return to Table
Health Care Fraud Return to Table

Fraud Risk Exposure and Description
Home Health Agency Billing Schemes There are many Home Health agencies that do not provide the care they bill for. Some even solicit names and demographics from hospital workers to use for additional services not received. [**Source:** Jerri Rowe MBA, CFE, RHIA, CPC, CRC] Return to Table
Durable Medical Equipment (DME) Billing Schemes DMEs can bill for equipment not issued. When billings are inconsistent with other known information about the DME, it can trigger further investigation. A raid or surveillance can reveal "store-front" operations with no actual medical equipment or supplies at the site. [**Source:** Jerri Rowe MBA, CFE, RHIA, CPC, CRC] Return to Table
Speech Therapy Billing Schemes Recently, an owner (a licensed therapist) of a speech therapy clinic was sentenced for fraud because she billed Medicaid millions for speech therapy provided to children that was actually provided by "aides" she "trained." The children were not getting therapy from licensed therapists because that would cost have the owner too much. [**Source:** Jerri Rowe MBA, CFE, RHIA, CPC, CRC] Return to Table
Addiction Treatment Billing Schemes In the addiction treatment industry, un-supervised and untrained interns sometimes provide therapy when they are not credentialed or qualified to do so. The requirements of licensure boards entail that interns must be supervised by an approved, licensed professional and the cases must be discussed and overseen by a licensed supervisor. There are facilities knowingly submitting these services to insurance companies for reimbursement and providing documentation claiming that all requirements of submission have been met, which they know is not true. In addition to the cost to insurance companies, this vulnerable population is being denied the level of expertise they deserve and have paid for. The crisis of addiction has become a health crisis in this country and recovering from addiction requires support and properly credentialed treatment. [**Source:** Mary Lynn Rapier, PhD, MSCJ, AAP]

Fraud Risk Exposure and Description
Return to Table
Time & Effort Reporting Schemes These schemes entail any billings for services on an hourly basis based on inflated or non-existent time and effort reports. These schemes can occur at all levels in a provider organization and also through subcontracted organizations or practitioners. [**Source:** Patrick Guilfoyle BA, RN, BSN,CFE, CHPC] Return to Table
Kickback Cover-up Schemes These schemes entail leasing medical space to other providers at above Fair Market Value (FMV) to conceal kickbacks for referrals. [**Source:** Patrick Guilfoyle BA, RN, BSN,CFE, CHPC] Return to Table
"Rent-a-Patient" Schemes These complex schemes require cooperating providers (medical and facility), professionals, inside employees, possibly cooperating regulators, and access to insurance/PHI, which is inappropriately shared/disclosed in order to recycle the patient throughout their various facilities. Recruiters and call centers are often used with a kickback system. Medical necessity is often not met, and the patient is recycled based on the strength of the insurance plan and benefit payout. This scheme has become rampant in the addiction treatment industry and can be viewed as possible provider fraud or part of a larger organized crime scheme. [**Source:** Mary Lynn Rapier, PhD, MSCJ, AAP] Return to Table
Recruited Patient Schemes These schemes entail finding people with some type of insurance coverage such as private coverage, Medicare, Medicaid, or VA. Once the coverage information is obtained, a fraudulent provider bills for services not actually provided or for services in excess of services actually provided. The recruited patients may or may not be involved in the fraudulent billings and may or may not receive a portion of the fraudulent revenue. [**Source:** Jacqueline Nash Bloink, MBA, RHIA, CFE, CHC, CPC-I/CPC, CMRS] Return to Table

Fraud Risk Exposure and Description
Patient Brokering Schemes—Opiod Addiction Treatment These are schemes in which individuals known as patient or body brokers exploit men and women who are seeking treatment for their opioid addictions. These patient brokers allegedly rely, in part, on call centers and call aggregators to generate leads on potential patients. Rather than focus on the health needs of the individuals who are seeking treatment, however, the emerging patient brokering industry view potential patients as commodities that can be bought, sold, or traded. One of the ways that patient brokers can generate leads on potential clients is through phone hotlines that connect to call centers that, in turn, are essentially collecting leads for treatment centers that are willing to pay a price for these referrals. Reportedly, the call centers will prescreen potential patients, focusing on their insurance plans, with the goal to ultimately sell the patient's information to the highest bidder. Others reportedly engage in deceptive tactics to hide the fact that they refer patients to treatment facilities that pay for referrals or to facilities owned by the same company that is operating the hotline. Patient brokers are predominantly paid in one of two ways, a per-head fee that can range from $500 to $5,000 for each patient who successfully enters a treatment center, or monthly treatment facility fees that are based on the broker meeting a quota of patients and can result in earnings in tens of thousands of dollars. In an effort to lure patients to these facilities, perks are sometimes offered, such as "scholarships" to go into rehab, free housing, unlimited free cigarettes, lavish food, hair and massage services. According to recent House hearings, some patient brokers contact patients after discharge, and offer them drugs in exchange for an agreement to return to treatment. Clearly this incentive for relapse contributes to the recycling of the patient into designated treatment facilities, while simultaneously ramping up the risk to life for those needing help and a continuity of care in order to save their lives. Exposure to this corruption is critical, followed by regulation and legal deterrence. The House of Energy and Commerce Committee has been working with the National Association of Addiction Treatment Providers (NAATP), along with a number of nationally known treatment centers and licensed medical/clinical providers to fully understand the scheme. Further investigation on a bi-partisan basis is much needed; to unearth the fuel this corruption has provided to the opioid crises that is ravaging the lives of so many in our country. [**Source:** Mary Lynn Rapier, PhD, MSCJ, AAP; and public court records] Return to Table
Kickback Schemes Concealed/Disguised Through Office Rentals In these schemes, a health care provider overpays doctors and then provides these doctors with free or below-market office space and other perks so that these doctors refer more patients to the health care provider. This "behavior may violate the federal Stark Law, Anti-Kickback Statute and False Claims

Fraud Risk Exposure and Description
Act, as it affected claims made to Medicare, Medicaid and TRICARE programs…. The Anti-Kickback Statute prohibits offering, paying, soliciting or receiving remuneration to induce patient referrals covered by Medicare and Medicaid. The Stark Law prohibits a hospital from billing Medicare for services referred by doctors with whom the hospital has an improper financial arrangement, such as excessive compensation." [**Source:** See Detroit Free Press article: Beaumont Health] [**Source:** Jerri Rowe MBA, CFE, RHIA, CPC, CRC] Return to Table
Pharmacy Fraud Pharmacy fraud takes different forms including: • Billing insurance providers for nonexistent prescriptions or for false prescriptions. • Billing multiple different payers for the costs of the same medication. • Billing insurers or patients for name-brand medications while dispensing generic medications to patients. • Providing a patient with a lesser quantity of a drug than the quantity prescribed and paid for. • Substituting more expensive medications for lower-cost drugs and billing insurers or patients for the more expensive medications. In any situation in which a pharmacy or a pharmacist submits a claim to an insurer or a bill to a patient containing false or misleading statements, accusations of pharmacy fraud may be made. Paying or accepting illegal kickbacks– such as compensating doctors for referring patients to the pharmacy or accepting payments from drug companies to prescribe particular medications– is also illegal behavior. [**Source:** NYCriminal Defense.] Return to Table
Pharmacy Fraud: Kickback Law One common method that pharmaceutical companies utilize to gain a competitive advantage in the prescription drug marketplace is to provide "kickbacks" to health care professionals in exchange for an agreement to prescribe or purchase their highly profitable drugs. These kickbacks can range from straight up cash payments to free vacations to honorariums for serving on a sham "Speaker's Bureau." Pharmaceutical companies that provide kickbacks are very likely to be in violation of the Federal Anti-Kickback Statute and other federal and state laws. The Federal Anti-Kickback Statute criminalizes the offering or receipt of kickbacks involving goods and services for which payment will be made through a government health care program such as Medicare, Medicaid, or TRICARE. Violations of the Anti-Kickback Statute may form the basis for a qui tam lawsuit under the False Claims Act because claims submitted for payment to government health care programs are considered false claims under the False Claims Act when the underlying transactions are illegal under the Anti-Kickback Statute. Real World Examples of Recent Pharmaceutical Kickback False Claims Act Cases:

Fraud Risk Exposure and Description
• 2010: Alpharma paid $42.5 million to settle a False Claims Act lawsuit in which it was alleged that the company paid kickbacks and made misrepresentations about the safety of its drug, Kadian. The suit, brought by a whistleblower, specifically alleged that Alpharma paid health care providers to promote and prescribe Kadian. The whistleblower received $5.33 million from the settlement. • 2009: Pfizer and its subsidiary paid $1 billion to settle kickback and off-label promotions claims in whistleblower lawsuits brought under the False Claims Act. The whistleblower suits alleged, in part, that Pfizer paid kickbacks to health care providers for the purpose of inducing the providers to prescribe Pfizer's drugs. Six whistleblowers shared in an award of more than $102 million as a result. [**Source:** NYCriminal Defense.] Return to Table
Pharmacy Fraud: Best Price Rule Fraud The Medicaid Drug Rebate Program requires that as a prerequisite for obtaining Medicaid coverage for their drugs, pharmaceutical companies must enter into an agreement guaranteeing to provide Medicaid with the same type of rebates and discounts on drugs as those that are provided to private marketplace purchasers. The price that Medicaid pays for a drug is based on the "Best Price" and the "Average Manufacturer's Price" (AMP), both of which the pharmaceutical companies must report to Medicaid. "Best price" is the lowest price paid for a drug by any retailer or other purchaser. Best price includes cash discounts, volume discounts, rebates, and the value of free goods provided. Best price does not include discounts that are "nominal in amount." AMP is the average price paid by wholesalers for a drug. Under the program, Medicaid is guaranteed a rebate for each drug equal to a percentage (varying from 13% to 23.1% depending on the type of drug) of the AMP or the difference between the AMP and the best price, whichever is greater. This rule ensures that Medicaid will pay at least the lowest price offered to any other purchaser. Sometimes, pharmaceutical companies will offer private purchasers lower prices than the prices they report and offer to Medicaid. This is a violation of the companies' agreement with Medicaid, and this type of fraud has resulted in some of the largest False Claims Act settlements and judgments. **Real World Examples of Recent Best Price Rule Fraud False Claims Act Cases:** • 2012: As part of the largest health care fraud settlement in history, GlaxoSmithKline paid $300 million to settle claims arising from four whistleblower lawsuits that it reported false drug prices, resulting in underpayment to Medicaid, by failing to properly report discounts in contingent arrangements with purchasers. • 2008: Merck & Company paid over $650 million to settle two whistleblower lawsuits brought by a former Merck employee and a physician in which it was alleged that Merck failed to provide proper rebates to Medicaid and paid kickbacks to health care providers. With regard to the best price rule violations, Merck failed to report discounts given to hospitals, wrongly characterizing those discounts as "nominal in amount." The former employee whistleblower received more than $68 million as a result of the settlement. [**Source:** NYCriminal Defense.]

Fraud Risk Exposure and Description
Return to Table
Pharmacy Fraud: Inflated Pricing Fraud One of the most common schemes that pharmaceutical companies use in defrauding the federal and state government health care programs is inflating the "Average Wholesale Price" (AWP) for their drugs. The AWP is the average price for which drug wholesalers sell a specific drug to their customers, such as hospitals, physicians, and pharmacies. Medicare bases its reimbursement for each drug on the AWP reported by pharmaceutical companies. Some pharmaceutical companies inflate the reported AWP for their drugs as a means of inducing pharmacies and other potential customers to purchase their drugs over their competitors'. This scheme is commonly called "marketing the spread." The larger the difference between the AWP and the actual cost paid by a health care provider (i.e., the "spread"), the higher the incentive is to purchase the drug. Essentially, this scheme operates as a kickback to health care provider purchasers in the form of the potentially large profit that they will gain from Medicare's reimbursement based on the inflated AWP. Inflating the AWP can be a violation under the Federal Anti-Kickback Statute and, in turn, the Federal False Claims Act if the inflated prices cause false claims to be submitted to Medicare and other government health care programs. Pharmaceutical misconduct of this type has resulted in some of the largest settlements and judgments under the False Claims Act, with the federal government having recovered over $2 billion from pharmaceutical companies who have engaged in drug pricing fraud. **Real World Examples of Recent Inflated Pricing Fraud False Claims Act Cases:** • 2012: Actavis Group paid $118.6 million to the U.S. and four states to settle claims arising out of whistleblower lawsuits that the company reported inflated prices of their drugs. The whistleblower was awarded $15.6 million as a result of the amount recovered by the federal government in the settlement. • 2010: Dey Inc., a pharmaceutical company, paid $280 million to resolve allegations in a whistleblower lawsuit brought under the False Claims Act that the company intentionally reported inflated prices for four of their drugs in order to market and sell those drugs. The whistleblower, a health care company itself, received over $67 million as an award for bringing the lawsuit. • 2010: Three pharmaceutical manufacturers, Abbott Laboratories Inc., B. Braun Medical Inc., and Roxane Laboratories Inc., paid $421 million to resolve allegations that the companies reported false and inflated prices for a number of their drugs as an inducement to health care providers to purchase those drugs. The whistleblower, who brought the lawsuits pursuant to the False Claims Act, received over $88 million as a result of the settlements. [**Source:** NYCriminal Defense.] Return to Table
Pharmacy Fraud: Good Manufacturing Practices Pharmaceutical companies must comply with "Good Manufacturing Practice" (GMP) regulations. These regulations, promulgated and enforced by the FDA, ensure that a drug is safe for use and not adulterated or defective in any manner. The GMP regulations "contain the minimum current good

Fraud Risk Exposure and Description
manufacturing practice for methods to be used in, and the facilities or controls to be used for, the manufacture, processing, packing, or holding of a drug." Pharmaceutical companies that do not comply with the GMP regulations and sell adulterated drugs will be in violation of the Federal Food, Drug and Cosmetic Act, and can face criminal penalties. Furthermore, companies that knowingly fail to comply with GMP regulations may be in violation of the False Claims Act if false claims for payment were submitted to programs like Medicare, Medicaid, and TRICARE, for the adulterated drugs. **Real World Examples of Recent Good Manufacturing Practices Violation Fraud False Claims Act Cases:** • 2010: A subsidiary of GlaxoSmithKline, PLC paid $600 million to settle False Claims Act and state law claims stemming from a whistleblower lawsuit brought by a former employee. The whistleblower asserted that the company sold drugs that were significantly below the quality of that specified in documents submitted to the FDA and, thus, knowingly cause the submission of false claims to government health care programs. Specifically, it was alleged that GlaxoSmithKline failed to make certain that drugs were free from contamination, had defects in manufacturing that caused tablets to split which rendered them ineffective, commingled different types of drugs, and did not always produce drugs that contained the correct mix of active ingredients as dictated by the FDA. As a result of the settlement, the former employee whistleblower received over $96 million. [**Source:** NYCriminal Defense.] Return to Table
Pharmacy Fraud: Pharmacy Benefit Manager Fraud Many major insurance companies, including those offering Medicare Part D Prescription Drug Plans, use pharmacy benefit managers (PBMs) to process their prescriptions. The advantage is that PBMs can use their size to negotiate better prices on prescription drugs. PBMs make much of their profits by operating mail order pharmacies which are owned by the PBMs themselves and are in direct competition with other "in network" pharmacies. **Types of PBM fraud can include:** • Shorting medications • Switching drugs • Failing to offer negotiated prices • Paying kickbacks or offering inducements to providers and manufacturers • Making inappropriate formulary decisions • Dispensing expired or adulterated drugs • Reshipping/recycling drugs which had been returned by mail order customers • Retaining manufacturers rebates instead of passing the savings on to the patient • Using undisclosed "Locked-in" pricing These fraudulent practices, and others, may constitute the basis for a whistleblower lawsuit under the Federal False Claims Act (FCA).

Fraud Risk Exposure and Description
[**Source:** NYCriminal Defense.] Return to Table

Home Healthcare Fraud

Home health care providers perform important services for elderly, disabled, and other patients who need services provided in-home. However, like some hospitals, some home health care providers put their desire to maximize profits ahead of the interests of patients and taxpayers.

Home health care providers can defraud the government and violate the False Claims Act in nearly countless ways. One way home health care providers may attempt to defraud the Government is by billing government health care programs for services provided to patients who do not meet the qualifications for home health care under those programs. One important qualification under Medicare for payment of home health care services is that the patient must be certified as homebound. In general, a patient is considered homebound if leaving their home requires considerable and taxing effort or if it is not recommended that the patient leave home because of their condition. A home health care provider submits a false claim when it bills Medicare for services provided to a patient that is not actually homebound.

Some of the other types of fraudulent schemes that home health care providers may engage in include:

- Billing for medically unnecessary procedures
- Billing for procedures not actually performed
- Providing incorrect billing codes for the purpose of increasing reimbursement (i.e., upcoding)
- Paying or receiving kickbacks for referrals of patients and services in violation of the Federal Anti-Kickback Statute
- Engaging in improper financial relationships with other health care providers who refer patients in violation of the Stark Act
- 2012: Odyssey Health care, a subsidiary of Gentiva, paid $25 million to resolve civil liability under the federal False Claims Act arising from its billing of claims for certain hospice services. The settlement resolved allegations that Odyssey performed continuous home health care services for palliative hospice care that were unnecessary or that were not performed in accordance with Medicare requirements between January 2006 and January 2009. Odyssey had submitted claims for continuous home care services at the highest reimbursement rate rather than for routine care level of service, which would have been justified. The continuous home care services reimbursement rate was higher than the routine care rate by several hundred dollars per day, per patient. The whistleblowers, all former employees of Odyssey, received payments totaling more than $4.6 million for their action.
- 2011: LHC Group Inc., one of the largest home health care providers in the United States, paid $65 million to settle claims that it submitted false claims to the government when it billed government health care programs for non-medically necessary services and for services provided to patients who were not homebound. The whistleblower received over $12 million as his share of the recovery.
- 2011: Hospice Home Care, Inc. paid $2.7 million to settle a lawsuit filed by whistleblower under the False Claims Act in which it was alleged that the company overbilled Medicare by billing for a higher level of care than that which was actually provided or required.

[**Source:** USAFraudAttorneys.com]

Fraud Risk Exposure and Description
Return to Table
Durable Medical Equipment Fraud Durable Medical Equipment (DME) is defined by the Federal Government as "equipment which can withstand repeated use," *and* "is primarily and customarily used to serve a medical purpose," *and* "generally is not useful to a person in the absence of an illness or injury," *and* "is appropriate for use in the home." Under this broad definition, Durable Medical Equipment can include a vast array of items such as powered and manual wheelchairs, medical beds, oxygen equipment, and walkers. For some DMEs to be covered by a government health program, a Certificate of Medical Necessity (CMN) must be signed by a treating physician and presented by an equipment supplier or manufacturer. DME suppliers are often among the most brazen and notorious perpetrators of fraud, waste, and abuse in the health care sector, and consequently are often the targets of FCA lawsuits and prosecutions. According to the Government Accounting Office (GAO), in 2010, DME and medical facilities cases combined made up about 40% of all criminal cases brought under the FCA. Durable Medical Equipment suppliers can defraud the government in numerous ways, some of which include: • Billing for medically unnecessary equipment • Billing for equipment or supplies that were never provided to patients • Billing for services, such as periodic maintenance of medical equipment, that never was performed • Billing for equipment provided to patients who do not qualify for the equipment under a government health program • Billing for different, more expensive equipment than that which was provided to the patient (i.e., upcoding) • Providing equipment that is known to be defective • Forging physician signatures on CMNs • Paying kickbacks to physicians for referrals or for physicians' signatures on CMNs • Engaging in improper financial relationships with physicians who refer patients These fraudulent practices, and others, may constitute the basis for a whistleblower lawsuit under the False Claims Act. [**Source:** USAFraudAttorneys.com] Return to Table
Medical Device Fraud

Fraud Risk Exposure and Description
A "Medical Device" is defined by the FDA as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is: • recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, • intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, • and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes." This broad definition means that medical devices can include items ranging from pacemakers to tongue depressors. Medical devices are regulated by the FDA and grouped into three different classes. Class I devices are subject to the fewest regulations because they pose the lowest risk to patients. Class III devices, on the other hand, are subject to the strictest regulations because they pose the highest risk of harm. Manufacturers of medical devices can defraud the federal government in a number of ways. For instance, medical device manufacturers may pay kickbacks to doctors to induce them to prescribe their products, or they may market their products for uses that have not been approved. Further, manufactures of medical devices may fail to use current good manufacturing practices in making their products. These and other activities by manufacturers of medical devices can form the basis for claims under the False Claims Act. Real World Examples of Recent Medical Device False Claims Act Cases: • 2012: Orthofix agreed to pay the government over $34 million to resolve allegations that the company engaged in a number of schemes to defraud the government, including waiving patient co-payments thereby causing the government to overpay, giving kickbacks to physicians to induce them to use the company's devices, and failing to advise patients of their right to rent devices rather than purchase them. The whistleblower received over $9 million as a result of the settlement. • 2011: Medtronic paid over $23 million to settle two False Claims Act lawsuits alleging that the company improperly used fees in post-market studies and device registries as a means of providing kickbacks to doctors to induce them to implant the company's pacemakers and defibrillators. The two whistleblowers shared in an award of nearly $4 million. [**Source:** NYCriminal Defense.] Return to Table
Medical Coding Fraud One of the more common ways that health care providers can defraud the Government is through coding violations. In order to bill either a private insurance company (such as Blue Cross Blue Shield) or a government health care program (such as Medicare, Medicaid, or TRICARE) for payment, a health care provider must enter a numerical "Procedure Code" [generally a CPT ("Current Procedural Terminology") code or HCPCS ("Health Care Common Procedure Coding System") code] that

Fraud Risk Exposure and Description
corresponds with the specific type of care provided to the patient. Government health care programs, such as Medicare, Medicaid, and TRICARE, pay a set amount for each code entered. Two types of coding violations that often form the basis for claims under the False Claims Act are "*upcoding*" and "*unbundling*." Upcoding is the fraudulent practice of entering a procedure code for a more expensive type of treatment than that which was really provided. This practice is being utilized with increasing prevalence by physicians and other health care providers and has cost Medicare and Medicaid billions of dollars. "Unbundling" is the billing of separate procedures or tests that are typically performed together, rather than entering one procedure code that covers all of the procedures. The combined reimbursement of the separate procedures is typically higher than the reimbursement for the one comprehensive code, and, thus, government programs end up paying more for procedures when health care providers engage in this fraudulent billing practice. Real World Examples of Recent Health Care Coding Violation False Claims Act Cases: • 2012: NextCare paid $10 million to settle a whistleblower False Claims Act lawsuit alleging that the company engaged in upcoding and billed Medicare and Medicaid for medically unnecessary procedures. The whistleblowers, one of which was represented by the Rabon Law Firm, shared in a $1.6 million award as a result of the settlement. • 2011: The City of Dallas paid $2.47 million to resolve a lawsuit filed under the False Claims Act and state law alleging that over a four year period the city upcoded ambulance transport claims submitted to Medicare and Medicaid. Specifically, the city coded every 911-dispatched transport at the advanced life support level rather than the basic life support level, regardless of the patient's condition or the type of care given. A former employee of the city filed the whistleblower lawsuit. [**Source:** NYCriminal Defense.] Return to Table
Lab Services Fraud Fraudulent billing by clinical laboratories has been a major concern for government payors such as Medicare, Medicaid, and TRICARE since the early 1990's. Types of Laboratory Services Fraud include: • Double billing • "Unbundling" lab services • Billing for medically unnecessary lab tests • Billing for tests not performed • Billing for tests which were not ordered These fraudulent practices, and others, may constitute the basis for a whistleblower lawsuit under the False Claims Act. [**Source:** NYCriminal Defense.] Return to Table

Fraud Risk Exposure and Description
Medically Unnecessary Services Fraud Government health care programs, such as Medicare, Medicaid, and TRICARE, will not make payments to health care providers for procedures or treatments that are not "medically necessary." As a condition to payment for services, health care providers must certify that the services for which they seek payment were necessary and can be supported by medical evidence. Some health care providers may intentionally provide medically unnecessary treatments or procedures to patients as a means of increasing their reimbursement from the government. This type of fraud is in violation of the False Claims Act and can serve as the basis for a qui tam lawsuit under the act. **Recent Real World Examples of Medically Unnecessary Services False Claims Act Cases:** • 2012: NextCare Inc., an urgent care provider, paid $10 million to resolve allegations that the company submitted false claims to federal and state health care programs by fraudulently billing for medically unnecessary allergy tests, H1N1 virus tests, and respiratory panel tests. The initial whistleblower, represented by the Rabon Law Firm, shared in an award of over $1.6 million as a result of the settlement. • 2010: FORBRA Holdings LLC, a national dental management company, paid $24 million to settle claims that it caused false claims to be submitted to Medicaid by billing for medically unnecessary services provided to indigent children. The medically unnecessary services that were allegedly provided to children and later billed to Medicaid included pulpotomies ("baby root canals"), anesthesia such as nitrous oxide, and extracting teeth, among others. The three whistleblowers who filed qui tam lawsuits received over $2.4 million. [**Source:** NYCriminal Defense.] Return to Table
Medicare Part D Plan Fraud The Medicare Part D Program for senior citizens was enacted in 2003 and went into effect on January 1, 2006. The program provides access to prescription drug coverage for Medicare recipients. Tens of millions of Americans are covered under Part D plans each year. Under the Part D program, seniors pay a premium to Part D plan sponsors in exchange for coverage, or partial coverage, of prescription drugs and access to negotiated pricing of prescription drugs. Across the United States, there are nearly 1,500 Part D Prescription Drug Plans. However, out of all of the plans offered, the majority of the Part D plan market is controlled by just a few of the largest companies. Because of the significant sums of government money available and the sheer volume of participants in the program, sometimes Part D plan sponsors and/or their Pharmacy Benefit Managers (PBMs) engage in fraudulent practices that result in the improper claims for payment to federal programs, and can therefore form the basis for claims under the False Claims Act. **Real World Examples of Recent Medicare Part D Fraud False Claims Act Cases:** • 2012: RxAmerica paid over $5 million to settle False Claims Act lawsuits in which it was alleged that the company misrepresented the cost of prescriptions on the Medicare Prescription Drug Plan Finder on the Centers for Medicare & Medicaid Services' website.

Fraud Risk Exposure and Description
The whistleblowers, two of which were represented by The Rabon Law Firm, shared in an award of $900,000. [**Source:** NYCriminal Defense.] Return to Table
Anti-Kickback Act Fraud The Federal Anti-Kickback Statute, enacted as part of The Medicaid and Medicare Patient Protection Act of 1987, and codified at 42 U.S.C. §1320a-7b, criminalizes certain conduct affecting reimbursable services under Medicare and Medicaid, and other federally-funded programs. Specifically, the statute prohibits the solicitation to pay, offer to pay, or receipt of payments, bribes, or rebates, in connection with the referral of individuals for medical services or goods, and all aspects of transactions involving goods, facilities, or services, for which payments may be made in whole or in part by Medicare and Medicaid or other federally-funded programs such as TRICARE. At its core, the Anti-Kickback Statute prohibits bribes, payments or rewards (directly or indirectly) – or the solicitation or offers of such remuneration – in connection with practically every aspect of health care delivery when any portion of those goods or services are paid for with federal dollars. Violations of the Anti-Kickback Statute can result in a felony conviction for the offenders, fines of up to $25,000, and imprisonment for up to five years. As with the Stark Act, compliance with the provisions of the Anti-Kickback Statute is a condition of payment within Medicare and Medicaid, and other federally-funded programs. Anti-Kickback Statute violations can create liability under the False Claims Act when persons or entities submit or cause others to submit claims for payment to Medicare or Medicaid with knowledge that the underlying transactions were in violation of the Anti-Kickback Statute prohibitions. **Real World Examples of Recent Anti-Kickback Statute Violation False Claims Act Cases:** • 2011: Cardinal Health, Inc. paid $8 million to settle a whistleblower lawsuit claiming violations of the Federal Anti-Kickback Statute. One of the whistleblowers, a pharmacy owner, alleged that Cardinal Health violated the Anti-Kickback Statute by paying him $440,000 to purchase prescription drugs from Cardinal Health. The whistleblowers received $760,000 as a result of the settlement. • 2009: Healthways, Inc. paid $40 million to resolve a whistleblower case in which it was alleged that Healthways' subsidiary paid kickbacks to more than 200 physicians for patient referrals. The whistleblower, a former employee of Healthways' subsidiary, received more than $7 million. [**Source:** NYCriminal Defense.] Return to Table

Fraud Risk Exposure and Description
Stark Act Fraud The Stark Act, codified under the federal statutes governing Social Security and found at 42 U.S.C. §1395nn, prohibits certain physician "self-referrals" to entities in which the physician (or a member of their immediate family) has a financial interest, due to the inherent conflict of interest in such situations. The prohibition originally applied only to clinical laboratory services, but later was broadened to include a long list of designated health services, including: • Clinical laboratory services • Physical therapy (PT), Occupational therapy (OT), speech language pathology services • Radiology services, including magnetic resonance imaging (MRI), computerized axial tomography (CT) scans, and ultrasound services • Radiation therapy services and supplies • Durable medical equipment • Parental and enteral nutrients, equipment and supplies • Prosthetics, orthotics and prosthetic devices • Home health services • Outpatient prescription drugs • Inpatient and outpatient hospital services Generally speaking, Stark Act liability may apply when four conditions are met: First, the referral must have been made with regard to a Medicare or Medicaid patient by a physician or an immediate member of that physician's family. Second, the referral must have been made with regard to a designated health service. Third, there must be a financial relationship between the referring physician or an immediate member of that physician's family and the referred entity. Fourth, there must be no statutory exceptions that apply to protect the referral arrangement from liability. If all the above conditions are met, then the referral may violate federal law, subjecting the physician and entity to civil penalties, denial of payments for the services rendered in violation of the Stark Act, and exclusion from the federal health care provider system. The Stark Act applies regardless of good or bad intention. Compliance with the provisions of the Stark Act is a condition of payment within Medicare and Medicaid, and other federally-funded programs. Stark Act violations can create liability under the False Claims Act when persons or entities submit or cause others to submit claims for payment to Medicare or Medicaid with knowledge that the underlying transactions were in violation of the Stark Act prohibitions. **Real World Examples of Recent Stark Act Violation False Claims Act Cases:** • 2012: Hospital chain Hospital Corporation of America (HCA) paid $16.5 million to resolve claims arising out of a whistleblower lawsuit that its subsidiaries violated the Stark Law by entering into improper financial transactions with a physician practice, such as leasing office

Fraud Risk Exposure and Description
space for a price well below fair market value, with the intention of inducing the referral of patients. The whistleblower received over $3 million as a result of the settlement. • 2011: Midtown Imaging LLC, a radiology clinic, paid $3 million to settle a lawsuit brought under the False Claims Act in which it was alleged that the company violated the Stark Law and the Anti-Kickback Statute. Midtown Imaging violated the Stark Law by receiving referrals from physician groups with whom the clinic had a financial relationship. The whistleblowers were two former physician employees of Midtown Imaging, and they received $600,000 as an award. [**Source:** NYCriminal Defense.] Return to Table
Off Label Marketing Fraud Off label marketing fraud occurs when a drug company or medical device manufacturer markets and promotes the use of an FDA-approved controlled substance (a prescription drug) or device for a purpose other than that for which FDA approval was obtained. The Food and Drug Administration, through the Food and Drug Administration Center for Drug Evaluation and Research (CDER), receives and reviews a company's application for new prescription drugs (a "New Drug Application," or NDA), based upon extensive research data and clinical trials. The reason for this review and approval by the FDA is to ensure that the new prescription drug is safe and effective for its intended purpose, and that the manufacturer provides appropriate and accurate language describing safe dosage, route of administration, drug storage, and other important information about the drug that relates directly to patient safety. As part of the approval process, the FDA must approve patient inserts and labels for every prescription drug. The approvals constitute the only approved usages for the particular prescription drug, and cannot be substantively changed or altered without FDA approval. Both physicians and patients rely upon the FDA approval process and the purpose and usages for a drug, according to the FDA approved uses. A physician may lawfully prescribe an FDA-approved prescription drug for a use or treatment other than that for which it was approved by the FDA. However, a drug company is absolutely forbidden from marketing and promoting and therefore may not market and promote a prescription drug for a use other than that for which it was approved via the FDA drug approval process. Similarly, a medical device manufacturer is also forbidden from marketing and promoting and therefore may not market and promote a medical device for a use other than that for which it was approved by the FDA. When this happens, it is referred to as "Off-Label Marketing." Due to the enormous profits that drug companies medical device manufacturers can reap when they believe that their FDA-approved drugs or devices are effective for other, unapproved uses, many companies are tempted to engage in off-label marketing, which is illegal and may endanger patient safety. Many of the very largest False Claims Act cases resolved the last decade concerned off-label marketing violations. **Real World Examples of Recent Off-Label Marketing False Claims Act Cases:** • 2012: Abbott Laboratories, Inc. paid $800 million to settle whistleblower lawsuits alleging that the company marketed the drug Depakote for uses other than those approved by the FDA.

Fraud Risk Exposure and Description
Depakote was only approved for treatment of epilepsy, bipolar mania, and migraines. However, Abbott Laboratories promoted the drug to treat both agitation and aggression in dementia patients and schizophrenia. The whistleblowers received $84 million from the federal government as a result of the settlement. • 2012: GlaxoSmithKline, LLC paid $1.043 billion to settle four whistleblower lawsuits alleging that it engaged in in the off-label marketing of the drugs Paxil, Wellbutrin, Advair, Lamictal, and Zofran. The allegations included that the company marketed Zofran, which the FDA only approved to treat post-operative nausea, for the treatment of morning sickness in pregnant women and that the company improperly marketed the epilepsy drug, Lamictal, for psychiatric and pain treatment. • 2010: Novartis Pharmaceuticals Corporation paid $237.5 million to settle civil lawsuits alleging that the company engaged in off-label marketing with 6 of its drugs, resulting in the submission of false claims to the government. Specifically, regarding the drug, Trileptal, a drug approved to treat epilepsy, Novartis marketed the drug for both psychiatric and pain treatment, uses not approved by the FDA. The civil lawsuits were brought by former employees of Novartis, and the whistleblowers received over $25 million as their share of the recovery under the False Claims Act. • 2010: Allegan, Inc. paid $225 million to settle civil lawsuits with federal and state governments in which it was alleged that the company promoted its product, Botox, for uses not approved by the FDA, resulting in false claims submitted to the government. Allergan promoted and marketed Botox's off-label uses in a variety of ways, including conducting workshops teaching physicians and their staffs how to bill for Botox's off-label uses. The civil lawsuits were initiated by five whistleblowers, who shared in $37.8 million awarded to the Relators. [**Source:** NYCriminal Defense.] Return to Table