Fraud Terminology

What is Fraud Risk?

According to the Fraud Triangle theory there are three elements motivating fraud: (1) perceived pressure that drives a person to commit fraud, (2) a perceived opportunity that enables them to commit the fraud, (3) the ability to rationalize the fraudulent behavior as not being incompatible with the person's values.

The fraud risk is the vulnerability that an organization faces from individuals capable of combining all three of these elements. Fraud risk can arise from internal and external sources.

Internal Fraud Schemes:

Corruption: employee misuses their influence in a business transaction in a way that violates their duty to the employer to gain a direct or indirect benefit.

Conflict of interest: undisclosed personal or economic interest of an employee in a matter that could influence their professional role.

Bribery: The offering, giving, receiving, or soliciting of any item of value to influence an action or a decision.

Invoice Kickbacks: improper, illegal, undisclosed payments intended as a compensation for a favorable treatment.

Bid Rigging: competitors agree in advance as to who will be the winning bidder.

Illegal Gratuities: gift received in response to an action or a decision.

Economic Extortion: The wrongful use of actual or threatened force, demanding a payment or some other consideration to make a specific business decision.

Asset Misappropriation: Scheme in which an employee steals or misuses the employing organization's resources.

Theft of Cash on Hand: Perpetrator misappropriates cash kept on hand at the victim organization premises.

Skimming: A scheme in which an incoming payment is stolen from an organization before it is recorded on the organization's books and records.

Unrecorded Sales: Employee sells goods or services to a customer, steals the payment, and does not record the sale.

Understated Sales: Employee records the sale for a lower amount than what was paid by the customer.

Lapping Schemes: Employee alters financial records to hide stolen cash.

Fraud Terminology

Cash Larceny: incoming payment is stolen from the victim company after it has been recorded on the organization's books and records.

Fraudulent Disbursements: employee makes a distribution of an organizational funds or manipulates a disbursement/payment function for a dishonest purpose.

Billing Schemes: fraudulent disbursement scheme in which a person causes their employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

Shell Company: business entities without active businesses operations, offices, or employees.

Personal Purchases: employee buys personal items with the company's card.

Payroll Schemes: employee causes their employer to issue a payment by making false claims for compensation.

Ghost Employee: refers to someone on the payroll who does not actually works for the victim company.

Falsified Wages: employee either manipulates the number of hours worked or changes their wage rate.

Commission Schemes: employee either manipulates the number of sales made or increases their rate of commission.

Expense Reimbursement Schemes: employee makes a claim for reimbursement of fictitious or inflated business expenses.

Mischaracterized Expenses: employees submit a claim for reimbursement for a personal expense by saying the expense is business related.

Overstated Expenses: employee overstates the cost of an expense.

Fictitious Expenses: employee request the reimbursement of a fictitious expense.

Multiple Reimbursements: request the reimbursement of the same expense multiple times.

Check and Payment Tampering: employee steals their employer's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts.

Register Disbursements: employee makes false entries on a cash register to conceal the fraudulent removal of cash.

False Voids: a legitimate sale is made; the employee fraudster void it and keep the proceeds of the sale.

False Refunds: employee creates a false refund as if the customer were returning merchandise.

Asset Larceny: theft of an asset with a felonious intent.

bank prov.

Fraud Terminology

Asset Requisition and transfers: the use of internal documents by an employee to gain access to the merchandise, and to steal it while it is being moved from one location to another.

False Sales and Shipping: employee creates false shipping documents and false sales documents to conceal the fraud and to cover up the theft.

Purchasing and receiving schemes: employee manipulates a company's purchasing and receiving records to steal the incoming merchandise.

Financial Statement Fraud: employee intentionally causes a misstatement or omission of material information in the organization's financial reports.

Net Worth/ Net Income Overstatements: Intentional overstatement of the net income.

Timing Differences: deliberate recording of revenues or expenses in improper periods.

Fictitious Revenues: Artificially inflating a company's profits by recording fictitious sales of goods or services that were never delivered.

Improper Asset Valuations: improper valuation of inventory, account receivable, fixed assets and intangibles or other assets.

Improper Disclosures: misrepresentation of financial information using incomplete or falsified financial documents

Net Worth/ Net Income Understatements: Intentional understatement of net income.

External Fraud Schemes:

Identity theft: Fraudster uses victim's personal identifying information without authorization to commit crimes.

Account takeover fraud: Occurs when the fraudster gains access of a legitimate account.

Impersonation: Fraudster pretends that he is someone else to obtain payments from its victim.

Social Engineering: Fraudster manipulates its victim to give up confidential information.

Business Email compromise: Criminal send an email that appears to come from a known source making a legitimate request, tricking the victim into transferring funds or revealing sensitive information.

Fraud Terminology

Phishing: Fraudster claims to be a reputable company and tricks the victim into providing passwords, account numbers and other sensitive information. (Mostly done by email)

Smishing: Fraudster sends text message to trick the victim into providing passwords, account numbers and other sensitive information. (Mostly done by email)

Vishing: Fraudster tricks victim into calling an 1-800 number and records information entered by the customer.

Pharming: Fraudster redirect website traffic to an attacker-controlled website.

Check fraud: involve making the unlawful use of checks to illegally acquire or borrow funds that do not exist within the account balance or account-holder's legal ownership.

Counterfeit checks: Counterfeit checks include any checks that have been created fraudulently with the purpose of stealing money from someone. This category can include fake cashier's checks, money orders, personal checks, and business checks.

Forged checks: describe a check on which the drawer's signature is forged or unauthorized.

Check Kitting: taking advantage of the float time to make use of non-existent funds, covering a bad check from one bank account to another.

Payment card fraud: misuse or a debit or credit card to make purchases without the cardholder's authorization.

Stolen Card numbers: stolen card numbers are commonly obtained though skimming and sold on the dark net or by unscrupulous brokers.

Counterfeit Cards: fraudster skims or copies the data held on the magnetic stripe of a legitimate credit or debit card and creates a fake plastic card, which contains the real cards details.

False applications: fraudster applies for a card using stolen information.

Brute force attack: A brute-force attack is when a fraudster uses an auto-dialer to steal the card numbers issued within the BIN. These attempts will typically be on one merchant as they test cards to try to get authorizations.

Skimming or Shimming: theft of credit and debit card data and PIN numbers when the user is at an ATM or point of sale (POS).

Consumer fraud schemes:

Advance Fee schemes: A victim pays money to someone in anticipation of receiving something of greater value - such as a loan, contract, investment, or gift - and then receives little or nothing in return.

Fraud Terminology

Scavenger or revenge scheme: the company who initially conned the victim presents itself under a different name and ask the victim if they would like help to put the fraudulent company out of business and get their money back. The consumer will be asked an up-front fee to finance the investigations and therefore, will be scammed twice.

Sweepstakes or prizes schemes: victim is being told that they won a prize and will receive it upon paying the taxes owed on it. As soon as the make the payment the fraudster will cease contact with the victim.

Credit Repair schemes: Fraudster tricked the victim in believing that they can repair their credit and eliminate their debt. They will require an up-front fee for their services.

Government imposter schemes: fraudster poses as a government official and claims the victim owes a debt that must be paid immediately in order to avoid being arrested.

Romance scheme: Fraudster adopts a fake online identity to gain a victim's affection and trust. They target lonely person, emotionally fragile, especially a widow or widower The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

Elder fraud: The wrongful or unauthorized taking, withholding, appropriating or use of money, assets or property of an eligible adult. Financial exploitation includes but is not limited to: The use of deception, intimidation, or undue influence by a person or entity in a position of trust and confidence with an elderly person or a vulnerable adult to obtain or use the property, income, resources, or trust funds of the elderly person or the vulnerable adult for the benefit of a person or entity other than the elderly person or the vulnerable adult.

Telemarketing fraud: fraudster communicate with its victim over the phone and makes false promises or materially misleading statements in order to obtain funds.

Ponzi schemes: investment fraud that pays existing investors with funds collected from new investors.

Fraud Terminology

Fraud Tree: