How to be a FRAUD FIGHTER in your organization

To fight fraud in your organization, you first have to learn what fraud is, why it's important to stop it, red flags to look for and ways to prevent it.

ACFE
Association of Certified Fraud Examiners

International Fraud Awareness Week

What is fraud?

In the broadest sense, the term *fraud* encompasses actions that are meant to deceive for financial or personal gain. It's any intentional or deliberate act to deprive another of property or money by guile, deception or other unfair means. Occupational fraud is fraud committed by people who work for, or do business with, an organization. This specific form of fraud represents a real and large risk to any organization that employs individuals.

Why should we care about fraud?

Fraud costs billions of dollars in damage to companies, governments and individuals each year. Additionally, fraud can dramatically affect the quality of life of its victims — and the employees of its victims — resulting in job losses, the loss of savings and investments, weakened trust in public institutions and a significant strain on resources.

In the Association of Certified Fraud Examiner's (ACFE) *Occupational Fraud 2022: A Report to the Nations*, anti-fraud professionals estimate that the typical organization loses 5% of its revenue annually to fraud. Think about your organization. The loss of those funds in your company could mean fewer raises, potential layoffs, greater pressure to increase revenue or cut costs, or decreases in employee benefits. Occupational fraud also affects your company's reputation. Would you feel comfortable opening an account with a bank that had a reputation of being defrauded by its employees? Do you think investors want to put their money into companies that cannot properly protect their assets?

What constitutes occupational fraud?

The ACFE classifies occupational fraud into three main categories:

1

ASSET MISAPPROPRIATION

Schemes in which an employee steals or misuses an organization's assets. Common examples include skimming payments received from customers, intercepting outgoing vendor payments and overstating reimbursable expenses.

2

CORRUPTION

Schemes involving a fraudster wrongfully using their influence in a business transaction to obtain a personal benefit or a benefit for another person (e.g., their spouse, children, or friends). Examples of corruption schemes include failing to disclose conflicts of interest, accepting illegal gratuities and paying bribes for favorable business decisions.

3

FINANCIAL STATEMENT FRAUD

Schemes involving the intentional misreporting of an organization's financial information with the intent to mislead others (e.g., investors, debtors or government authorities). Examples include creating fictitious revenues and concealing liabilities or expenses.

What are some of the most common occupational fraud schemes committed by employees?

Some of the more common frauds committed by employees include the theft of company assets, such as cash or inventory, and the misuse of company assets, such as using a company car for a personal trip. Here are more details about the schemes.

Stealing cash

Unsurprisingly, most people prefer to steal cash because the theft of physical cash is easier to conceal than many other types of theft. Skimming is the process by which an employee removes cash from the business before it enters the accounting system. This includes not recording a sale, or recording a sale for a lower amount than its actual cost, and pocketing the unrecorded amount.

Payment tampering schemes

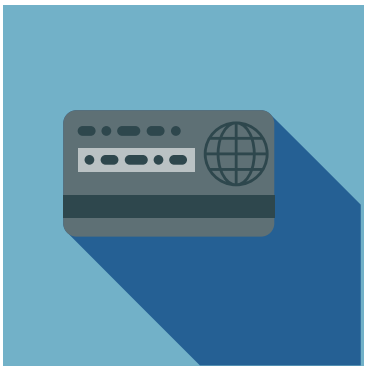
Payment tampering is a type of fraudulent disbursement scheme whereby an employee either prepares a fraudulent payment for their own benefit or intercepts a legitimate payment intended for a third party and converts it to their own benefit. In these schemes, fraudsters manipulate either traditional check payments or some form of electronic payments — such as automated clearing house (ACH) payments, online bill payments or wire transfers. Some fraudsters abuse their legitimate access to their employer's payment system. Others gain access through social engineering or password theft, or by exploiting weaknesses in their employer's internal control or payment system. Regardless of how they access the system, the perpetrators use this access to fraudulently disburse or divert payments to themselves or their accomplices.

Billing schemes

Billing schemes cause the victim organization to buy goods or services that are nonexistent, overpriced or unnecessary. In a typical scheme, the perpetrator creates false support for a fraudulent purchase. The fraudulent support documents, which can include invoices, purchase orders, purchase requisitions, receiving reports and others, cause the victim organization to issue a payment for the purchase. However, the fraudster directs the payment to their own address or bank account, thereby reaping an illegal gain.

Expense reimbursement schemes

Travel and expense budgets are common targets for occupational fraud. Employees might falsify information about their business expenses, enabling them to receive inflated expense reimbursements. Fraudsters can perpetrate this scheme by overstating real expenses or creating fictitious expenses in areas such as client entertainment and business travel.



Payroll schemes

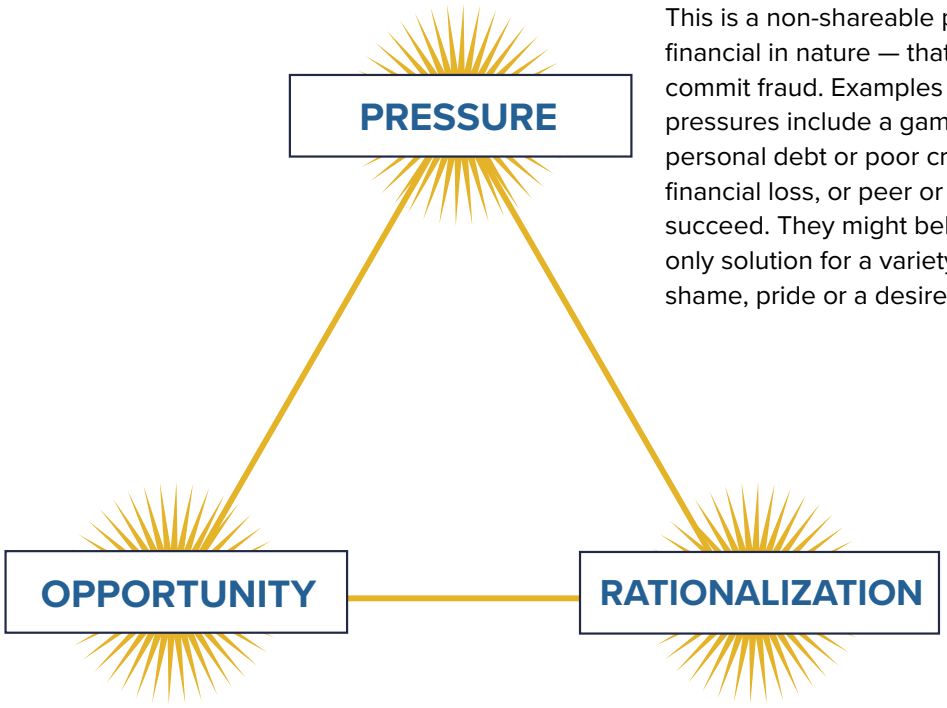
Payroll schemes occur when an employee fraudulently generates overcompensation on their behalf. These schemes are similar to billing schemes in that the perpetrator generally produces a false document or otherwise makes a false claim for a distribution of funds by their employer.

Inventory fraud schemes

Most inventory and warehousing frauds involve misappropriating or stealing inventory for personal use or resale. For example, an employee might order excess inventory and then resell that inventory at a discount to another business. Likewise, the personal use of company assets, such as consuming office supplies for non-work-related purposes, can develop into a fraud or an abuse situation if management does not address it.

Why do people commit fraud?

Dr. Donald Cressey was one of the first individuals to study how white-collar criminals differ from violent offenders. Part of Dr. Cressey's work on occupational fraud included the development of the Fraud Triangle. According to this theory, three elements must be present for occupational fraud to occur:



This is a non-shareable problem — typically financial in nature — that drives a person to commit fraud. Examples of these types of pressures include a gambling or drug habit, personal debt or poor credit, a significant financial loss, or peer or family pressure to succeed. They might believe fraud is the only solution for a variety of reasons, such as shame, pride or a desire to prove oneself.

This refers to the perceived ability to commit fraud. An employee must perceive that they have the opportunity to execute their scheme successfully. This opportunity could present itself as a lack in anti-fraud controls, like having no separation of duties, that they have discovered.

Offenders use rationalization to justify or excuse their criminal behavior and to maintain a positive image of themselves. People are often unwilling to view their behavior as bad or morally questionable. To keep a positive self-image, offenders rationalize their fraudulent actions in a variety of ways. They might tell themselves that they're only "borrowing" the money and will repay it at the first chance they get, or they could believe they're underpaid for their work and therefore deserve extra compensation.

What are behavioral red flags of fraud?

Fraud can be committed by anyone, making it important for all employees to be aware and observant of behavioral red flags that might indicate a potential fraudster. However, it is important to note that sometimes these indicators also apply to honest people, so their presence alone does not mean that someone is committing fraud. Based on ACFE research, here are the six most common behavioral red flags of fraud:

1

Living beyond means

Big spending is often an indicator of fraudulent behavior, especially if an employee's salary does not line up with their lifestyle.

2

Financial difficulties

Financial problems are often cited as a motivation by those who commit occupational fraud. Examples include high student loan debt, car loans, mortgages, taxes or high credit card debt.

3

A close personal relationship with vendors or customers

This might indicate a conflict of interest or collusion between an employee and a vendor or customer.

4

Control issues or an unwillingness to share duties

Fraudsters might fear that they will be caught if they share their job duties with another employee. They may not use their allotted time off, or they might come up with excuses to gatekeep information from their colleagues.

5

Irritability, suspiciousness or defensiveness

Fraudsters may act unusually paranoid or harsh with colleagues in order to project suspicion onto others or to discourage questions.

6

"Wheeler-dealer" attitude

A fraudster may display an attitude involving shrewd or unscrupulous behavior.

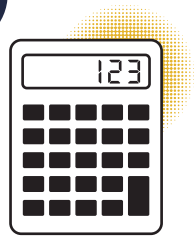
What can be done to prevent fraud?

Every employee, regardless of position, can help prevent fraud. Organizations should consider putting anti-fraud controls in place that are proven to reduce the cost of fraud. According to the *Report to the Nations*, the six anti-fraud controls that showed the greatest association with lower fraud losses were:

1

An established, company-wide code of conduct

2



An internal audit department

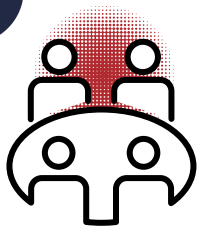
3

Management certification of financial statements

4

External audit of internal controls over financial reporting

5



Management review

6

Hotlines

What can I do to protect my organization?

In addition to organization-wide controls, individual employees are essential in preventing and detecting fraud. Here's how you, and your colleagues, can make a difference.

Conduct fraud training and raise awareness

Organizations that provided fraud training for employees saw a 38% reduction in the median loss per fraud instance. If your organization doesn't have dedicated anti-fraud professionals to lead trainings, you can take the initiative and share the free resources found on FraudWeek.com or ask a CFE to give a presentation at your organization. Even just starting conversations about fraud and raising awareness of the issue may dissuade potential fraudsters from acting.

Be aware of red flags and trust your instincts

Now that you have learned some of the red flags, you can remain vigilant. While the majority of employees are honest, if you observe something that does not seem right, you should evaluate the situation. Then, if you still have doubts or suspicions, it might be necessary to take action.

Report irregularities

Most companies have a reporting mechanism, such as a hotline, that allows employees to report wrongdoing anonymously. If your company does not have a hotline, or if you prefer not to use it, you could write an anonymous letter to the appropriate official in your company or to the internal audit or anti-fraud team if your organization has one. If the allegation involves the company's top management, it can be reported to the board of directors, the board's audit committee or the company's independent auditors.

Preventing fraud is not just the responsibility of management, the board of directors, the inspector general or the audit team.

Everyone has a role to play in the prevention of fraud. Help your organization protect its finances — and its reputation — from harm.

Be alert to potential fraud and educate your colleagues on how they can be fraud fighters too.

ACFE
Association of Certified Fraud Examiners

International Fraud Awareness Week

FraudWeek.com