# Business financial abuse and financial crime

**ISSN 1857-9787** **UDK 334.73]:343.9.024:336.7**

**Enida Cami, MSc**

SPAK- Specialist administrarive secretary
+3550682058006
thespotia_79yahoo.com

**Abstrakt**

**In the business, the basis of all corporate abuse of power and economic exploitation is stealing. The companes can made falsifying financials, laundering money, committing securities and commodities fraud, market manipulating and/or committing false advertising.**

**Falsifying financials occurs when corporations are involved in creating fake accounting entries and misrepresenting the corporation's financial situation. Examples include trades that falsely show an increase in profits or the hiding of losses, the covering up of transactions that should have been regulated by the government, insider trading, and the reporting of misleading asset values.**

**Money laundering is the process by which companies conceal money made illegally by making it appear legitimate. The goal of this white collar crime is to hide the illegal activity while evading taxes and making money. The crime is committed, the money is separated from the illegal activity, and the money is returned to the criminals from what appears to be a legal source.**

**Securities fraud can involve complex stock trading or small-scale borrowing to start a new business. In many cases, someone charged with securities fraud did not know that what they were doing was illegal. Securities fraud convictions can mean serious jail time and expensive financial penalties. Securities fraud involves misrepresentations in buying, selling, or trading stocks or commodities. Securities fraud is a broad term that may involve theft, embezzlement, or theft by false pretenses in stocks, trades, or investments. Securities can include stocks, financial interest in a company, and notes or certificates of interest.**

**Market manipulation refers to artificial inflation or deflation of the prices . Also known as price manipulation or stock manipulation, it involves the literal manipulation of a market for personal gain. Price manipulation, stock manipulation, and market manipulation they all mean the same thing: someone trying to influence the market to scam investors. In its simplest form, market manipulation is the intentional and artificial inflation or deflation of the price of a commodity, asset, or other product in order for the market manipulator to make a profit. Manipulation interferes with the free trade of assets, decreases market efficiency, and is dangerous for individual investors who are overextended in the asset that's being manipulated. It can happen to anyone, and it takes more than having a top stock broker to keep yourself safe.**

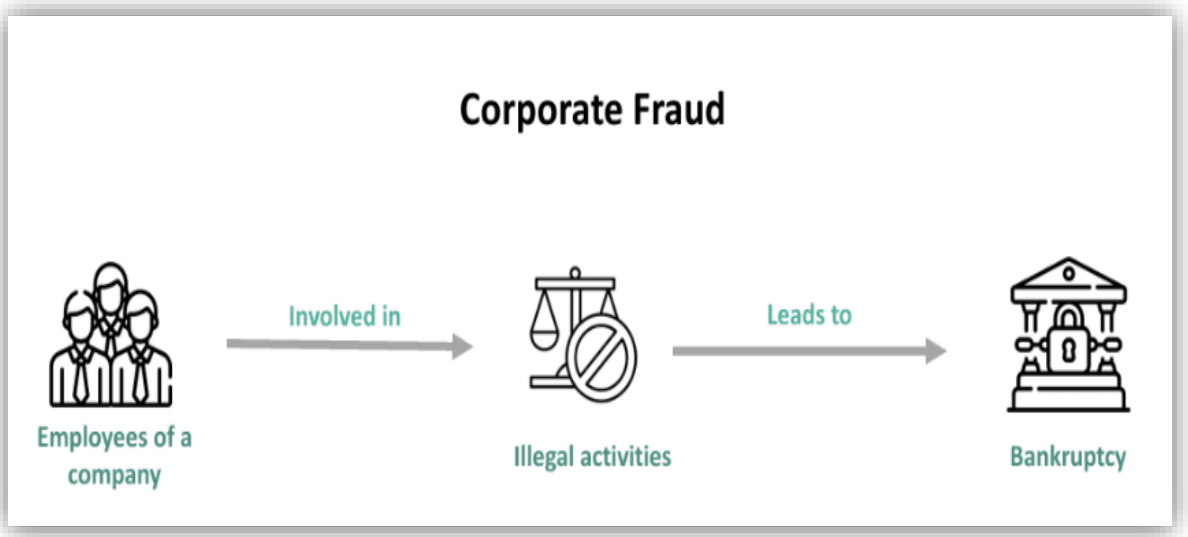
**False advertising applies to any promotions or advertising that misrepresent the, nature; quality; characteristics; and/or origin of commercial activities, goods, and/or services. A business who knowingly releases an ad that contains misleading, deceptive, and/or untrue statements in order to sell their product could be held liable for injuries resulting from false advertising.**

**Key words: corporations, inflation, deflation, efficiency, investors.**

## 1. TYPES OF CORPORATE FINANCIAL FRAUD

Corporate fraud, or white-collar crime, refers to fraud or illegal activities within a corporation or organization. The main purpose of indulging in such fraud is to earning some extra mone secretly without reporting it to the government. Corporate fraud scandals could occur due to various reasons and factors. Such fraud can be committed by any pillar of the organization, like directors, top executives, or others. As a result, it leads to financial, accounting, or data theft of the firm. Therefore, it becomes necessary to expose such corporate fraud cases. Otherwise, it may lead to bankruptcy:[1]

**Figure 1**




Source: WallStreetMojo, (2024), Corporate Fraud - Definition, Example, Type, Detection, Prevention, https://www.wallstreetmojo.com/corporate-fraud.

- Corporate fraud is a form of deceit (cheating) performed by the organization's board of directors or top executives while engaging in illegal activities. And the primary motive behind this idea is money. It can occur in any business, regardless of size or form.

[1] WallStreetMojo, (2024), Corporate Fraud - Definition, Example, Type, Detection, Prevention, https://www.wallstreetmojo.com/corporate-fraud.

- The intentions of individuals behind corporate fraud can be many. It includes corruption, conflicts of interest, bribery, and others. So, if an employee has a major conflict with the organization, they might leak sensitive data to the rival. Another case is when a firm illegally trades and does not show in the financial statements. They might bribe the employees or hide factual data from the public and the government. Thus, when a whistleblower exposes these activities, there are high chances of bankruptcy.
- The types of corporate fraud that prevail in the organizations:
  - ✓ Corruption. One of the major roots of corporate fraud is individuals' corrupt nature. It includes bribery, interest conflicts, extortion, and illegal gratuities. Executives try to conduct illegal activities in exchange for bribes. In addition, conflicts of interest also stand out. Individuals try to place their interests ahead instead of company.
  - ✓ Misappropriation. Corporations can conduct misappropriation either for cash, inventory, or assets. Here, individuals try to skip the record of cash which leads to theft. Likewise, firms also create fake sales invoices, asset theft, incorrect shipping, and inventory misuse. Other frauds include fraudulent issuance (release) salaries to employees, creating fake employees, fictitious expenses, etc.
  - ✓ Financial Statements Fraud. Financial statement fraud includes fake disclosure of financial items like revenue, assets, losses, liabilities, and others. Although strong regulatory compliances and authorities the cases still occur.
- Detection. The ways through which industry can detect corporate fraud cases:
  - ✓ Tip Lines. Usually, tip lines are numbers where anonymous persons can report these frauds through telephone to the authorities. So, in case authorities receive such tips, they can directly investigate with the internal auditor or legal department. As a result, proper action can be taken against the firm for any wrongdoing.
  - ✓ External And Internal Auditors. Auditors play an important role in detecting any fraudulent activities within the organization. Auditors to follow the standards and guidelines. They must report if they detect any misstatements or errors.
  - ✓ Fraud Triangle. The fraud triangle works best. It usually has three factors, pressure, opportunity, and rationalization. The former usually exists in a non-shareable problem where individuals need money to pay bills. In contrast, an opportunity incentivizes them to earn extra money, which is otherwise impossible. Employees perform it by violating the company's trust. However, rationalization is a mere excuse for committing fraud. Therefore, authorities can examine the activities of an organization through this framework.
  - ✓ Accident. Fraudsters often make some mistakes while committing fraud. And it can directly expose corporate fraud. However, passive detection occurs when fraudsters themselves confess their crime. As a result, it makes others aware of their irregularities.
  - ✓ Fraud Risk Assessment. Firms can conduct an assessment test to understand the efficacy within the organization. They can identify loopholes, bridge the gap between employees, and minimize the risk of errors.
- Prevention. The different methods to prevent corporate frauds within the organization:
  - ✓ Companies can establish a strong communication channel throughout the management. As a result, employees clearly understand the dos and don'ts of the organization.

- ✓ Assessing and evaluating the background of the new employees for safety standards can help prevent frauds.
- ✓ Reviewing the inventory control system and asset management can help check for any gaps or records that need to be added.
- ✓ Scanning all the financial statements and books of accounts also allows prevention. If there is a fake reimbursement or a hypothetical employee, conduct an urgent check.
- ✓ Delegating the activity among all employees. Thus, there will not be any supremacy over a particular employee. As a result, the appearance of fraud will be minimized.
- ✓ Establishing a tip line so that employees can anonymously report suspicious activities.
- ✓ Monitoring the bank statements and other sensitive information of the company.

Corporate fraud schemes are characterized by their intricacy and financial impact on the company, other employees, and external parties:[2]

1. Corporate fraud extend beyond the purported limits of an employee's job description.
   - ✓ When businesses participate in deceptive or unethical acts, such as fabricating accounting records or deliberately influencing commodities, products, and services, they are said to violate the law.
   - ✓ The illicit and ethically questionable operations that are conducted by anybody, person, group, or corporation, with the paramount aim of obtaining a competitive edge over other companies or individuals, is Corporate Fraud.
   - ✓ Fraud is a pervasive issue that undermines the integrity and trust within the business world.
   - ✓ Deliberate manipulation, misrepresentation, or concealment of financial or non-financial information are key areas for fraud to emerge from. This could stem from an individual or a corporation for personal gain or mislead stakeholders.

2. Corporate fraud encompasses various types of fraudulent activities, including financial fraud, asset theft, corruption and bribery, fraudulent vendors, tax fraud against small businesses, and wage and salary fraud:

**Figure 2**

[2] Wall Street Oasis, (2024), Corporate Fraud - Overview, Reasons, and Examples, https://www.wallstreetoasis.com/.../cor.


Source: Wall Street Oasis, (2024), Corporate Fraud - Overview, Reasons, and Examples, https://www.wallstreetoasis.com/.../cor.

- Financial Fraud. Accounting fraud is when an individual or an entire accounting staff manipulates your accounts payable or receivables to conceal their crime; Multiple check payments, fraud, lapping, false sales, and skimming are all examples of embezzlement.
- Asset Theft. It is considered financial fraud when a single individual or the entire accounting department in charge partakes in adjusting your accounts payable or receivables to disguise their larceny.
- Corruption and Bribery. Bribery and corruption not only constitute criminal activity, but they also have a negative impact on the image of the firm. Corruption and Bribery includes instances when an employee demands a bribe from an outsider in exchange for a service or undermines the company's position to get personal gain, as well as the establishment of shell companies to redirect the company's finances and assets.
- Fraudulent Vendors. Vendor fraud may occur when staff conspires with suppliers to allow for overbilling to gain an additional profit via fraudulent charging schemes, bribery, overbilling, and price manipulation.
- Tax Fraud Against Small Businesses. Small enterprises often do the majority of their operations in cash. Small firms often fail to disclose all money produced or paid to workers illegally in order to avoid complying with payroll tax obligations and other legal employment requirements.
- Wage and salary fraud. Payroll fraud is the most common sort of employee fraud. It includes timesheet fraud, in which workers falsify their work hours or conspire with the payroll department to perpetrate fictitious employee schemes, forgery of employee advances, and so on.

3. When an employee defrauds the firm of its assets, this is referred to as asset misappropriation. This might involve stealing merchandise, abusing corporate assets, or tampering with checks and invoices to exaggerate costs and purchases.

## 2. CORPORATE PAYMENT FRAUDS

With faster payments, open banking, and the accelerated release of new payments products and services, payments fraud has become a formidable threat to enterprises worldwide. Perpetrators of this fraud are continually casting a wider and wider net. This can be seen in the increasing shift in focus from primarily targeting banks, to aiming directly at businesses and enterprises:[3]

- Fraudsters are also becoming increasingly effective in their methods, achieving unprecedented success at circumventing corporate controls and probing deeper into systems to orchestrate and execute coordinated attacks.
- Simply put, corporate payments fraud involves falsely creating or diverting payments. There are multiple types of payments fraud, including creating bank accounts for the sole purpose of enabling the fraudulent payments to be made, social engineering (psychological manipulation of people), identity theft, impersonation of company officers by hackers, and access abuse by corporate employees.
- In fact, 95% of all security incidents involve human error. Cybercriminals are particularly adept at not only manipulating technology for executing attacks, but also at manipulating human vulnerabilities. They have proven to be very effective in duping company employees into unwittingly providing them access to sensitive information.

The landscapes in which most businesses operate are continually evolving, as is the underlying payment fraud . In just the same way that businesses have been able to embrace digitalization to evolve and provide more streamlined and personalized services, fraudsters have embraced digital technology to evolve the threat that they pose to businesses and the public. Today, the threat posed by fraudsters can be characterized by four key aspects:[4]

- Organization: Fraudsters are increasingly professional in approach, even dividing their operation into different functions
- Complexity: Methods of fraud-attack and the associated techniques used are increasingly sophisticated.
- Victims: Fraud attacks are increasingly targeted toward specific organizations and specific profiles of employees within.
- Speed of attack: A recurring theme for almost all corporate fraud is the aim to exfiltrate funds out of the target business as quickly as possible. External “mule” accounts are maintained to transfer funds in real time and reduce the opportunity for recovery.

Payment fraud is a type of financial fraud that involves the use of false or stolen payment information to obtain money or goods. Payment fraud can occur in a variety of ways, but it often includes fraudulent actors stealing credit card or bank account information, forging checks, or

[3] Verril, B., (2019), What is Corporate Payment Fraud, nsknox.net/blog/payment-fraud/.
[4] Goldman Sachs, (2023), The Evolving Landscape of Corporate Payments Fraud, https://www.goldmansachs.com/.../payments-fraud.pdf PDF file.

using stolen identity information to make unauthorized transactions.There are several methods that fraudulent actors use to commit payment fraud. Some of the most common tactics are:[5]

1. Phishing - Phishing is a type of social-engineering attack—a tactic that involves deceiving people through psychological manipulation—where fraudulent actors use fraudulent emails, text messages, or websites to trick individuals into disclosing sensitive information such as log-in credentials and credit card information.

- ✓ Phishing attacks are usually carried out through emails that look like they are from a trusted source, such as a bank or reputable online retailer. The email may ask the recipient to click on a link to update their account information, verify a recent transaction, or claim a prize. When the recipient clicks the link, they are directed to a fake website where they are prompted to enter their log-in credentials, credit card information, or other sensitive data.
- ✓ Phishing attacks can also be carried out through text messages, known as "smishing," or through social media platforms, known as "pharming." In these cases, the attacker sends a message or a link to a fraudulent website that appears to be legitimate, in order to steal personal information or infect the device with malware.

2. Skimming - Skimming occurs when a fraudulent actor uses a device, called a skimmer, to steal credit or debit card information. The fraudulent actor attaches a skimmer to a card reader at ATMs or point-of-sale terminals such as gas pumps, self-checkout lanes, and other payment terminals. The skimmer captures the card's magnetic stripe data, which can be used to create counterfeit cards or to make fraudulent purchases. In addition to skimmers, fraudulent actors may also use small cameras or overlays that fit over the ATM or payment-terminal keypad to capture the customer's PIN. This information is then used with the stolen card data to make unauthorized withdrawals or purchases.

3. Identity theft - Identity theft is a type of payment fraud where a fraudulent actor steals a person's personal information—such as their name, Social Security number, or credit card number—and uses it to make unauthorized purchases or open accounts in the victim's name. Identity theft can have serious financial and legal consequences for the victim and cause significant stress and anxiety. Identity theft is an umbrella term that describes a number of fraud tactics. Data breaches, where a hacker gains access to a company's database and steals personal information on a large scale, are also identity theft.

4. Chargeback fraud - Chargeback fraud—also referred to as "friendly fraud"—occurs when a customer disputes a legitimate transaction, claiming either they did not make the purchase themselves or that they did not receive the product or service they paid for. In some cases, the customer may receive a refund while keeping the product or service, resulting in a financial loss for the business. Chargeback fraud can have significant financial consequences for businesses: they may lose the revenue from the sale and be subject to chargeback fees and penalties. There are a few different ways that chargeback fraud can occur:

- ✓ The most common method is when a customer makes a legitimate purchase but later disputes the charge with their credit card company, claiming that the item was not as described or that they never received it.
- ✓ Another method is when a customer intentionally uses a stolen credit card to make a purchase and then disputes the charge as unauthorized.

---

[5] Stripe, (2024), Six types of payment fraud—and how businesses can prevent them, https://stripe.com/resources/more/six-types-of-payment-fraud.

5. Business email compromise - Business email compromise is a type of payment fraud where emails trick employees into transferring money to fraudulent accounts. In a Business email compromise scam, fraudulent actors gain access to a business email account, often through phishing or social-engineering tactics, and use it to send emails to employees or vendors requesting wire transfers or other payments. Business email compromise scams can take many forms. Often they involve a fraudulent actor who impersonates a high-level executive or vendor and requests an urgent payment or transfer. The email may look legitimate, using the company's branding and a familiar email address. But if the employee follows the directions in the email, they will transfer the money to a bank account controlled by the fraudulent actors.

6. Card-not-present fraud - Card-not-present fraud is a type of payment fraud that occurs when a fraudulent actor uses stolen credit card information to make purchases without physically presenting the card, usually online or over the phone. Card-not-present fraud fraud has become increasingly common with the rise of ecommerce, and it can have significant financial consequences for businesses, which may be liable for chargebacks or fraudulent purchases. Card-not-present fraud fraud usually occurs when a fraudulent actor obtains stolen credit card information through data breaches or other means and uses that information to make unauthorized purchases online.

7. Account Takeover – Account takeover is another type of payments fraud that can affect businesses. In this scheme, criminals steal or compromise an employee's login credentials for a company's online banking service(s). This allows the fraudsters to access account information, payment services, and even administrative functions, through which they can initiate fraudulent payments and tamper with access permissions for other company users.

## 3. CORPORATE FINANCIAL FRAUD

Corporate financial fraud refers to illegal, deceptive actions committed by a company or its employees.Common forms of corporate fraud include:[6]

- ✓ Financial statement fraud: Manipulating financial records to misrepresent a company's financial health.
- ✓ Insider trading: Illegally trading stocks based on non-public information.
- ✓ Embezzlement: Misappropriating company funds for personal gain.
- ✓ Bribery and corruption: Offering or accepting bribes to gain advantages.

Corporate financial fraud harms the interests of investors and affects the healthy development of the capital market. Understanding corporate financial fraud has important academic value and practical significance. Digital finance been rapidly developing over the past few years and scholars are investigating strategies for using digital finance as a tool to curb corporate financial fraud:[7]

- ➢ The breadth of coverage and depth of usage within digital finance show inhibitory effects on corporate financial fraud. This suggests that a combination of coverage and depth is needed to improve the success of digital finance on corporate financial fraud. The internal mechanisms suggest that digital finance inhibits corporate financial fraud

[6] CFI Team, (2024) Corporate Fraud - Overview, Reasons, corporatefinanceinstitute.com/resources/esg/corpor.
[7] Guanglin, S., (2023), Digital finance and corporate financial fraud – ScienceDirect, https://www.sciencedirect.com/science/article/pii/

by alleviating financing constraints, reducing corporate leverage, and decreasing costs.

- Digital finance promotes financial innovation, forming a financial format with wide coverage, high efficiency and low cost also affects the decision-making behavior of micro-enterprises. Digital finance is the product of the combination of digital technology and finance, and the empowering effect on the real economy can be divided into the contribution of digital technology and the contribution of financial development.
- The negative consequences of financial fraud can lead to the collapse of the company's stock price put the corporate in the risk of litigation, and cause investors to suffer huge losses:
  - ✓ The causes of financial fraud have been extensively researched and attributed to three factors: motivation, opportunity, and pretext, which is known as “fraud triangle theory”.
  - ✓ Among the fraud triangle theory, motivation factors include financing demand, growth rate of enterprises, and option incentive in executive compensation.
  - ✓ Opportunity factors mainly involve the corporate governance and internal control level of enterprises including the size of the board of directors and the proportion of independent directors.
  - ✓ Excuse factors refer to the factors that influence managers' attitude towards financial fraud, such as morality and values of management.
- In essence, the root cause of the repeated occurrence of corporate financial fraud lies in the constraints of technology and cost. External investors and financial institutions lack information on ways to evaluate the business ability and financial situation of enterprises besides financial statements.

## 4. FINANCIAL CRIME

Financial crime is generally defined as any activity involving fraudulent or dishonest behavior for personal financial gain. Financial crime refers to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else to obtain financial or professional gain. The two most significant types of financial crime are money laundering and the financing of terrorism:[8]

- ✓ Financial crime is a significant ongoing challenge for banks, institutions, and individuals. As regulators and financial authorities introduce new strategies to detect and prevent financial crime, criminals develop more sophisticated methodologies to evade legal scrutiny and commit offenses, including fraud, money laundering, and the financing of terrorism. Financial institutions are also expected to participate in the fight against financial crime by ensuring compliance with the authorities’ regulations at the risk of potentially severe penalties.

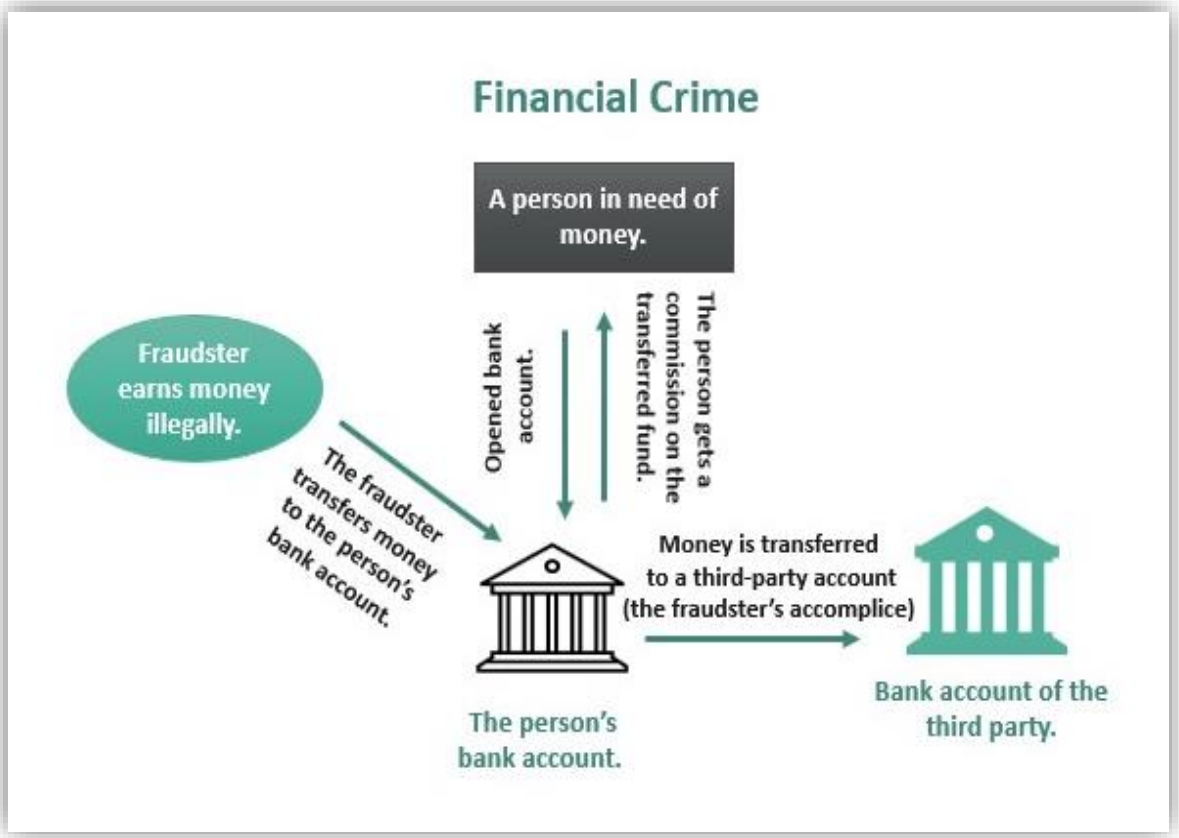
[8] Financial Crime Academy, (2024), What Is Financial Crime? AML Terms Explained, https://financialcrimeacademy.org/wha.

- ✓ Financial compliance is a significant international concern: the global cost of compliance in the financial sector is estimated to be around 180.9 billion U.S. dollars annually.
- ✓ Financial institutions spend lots of money to strengthen the internal controls and compliance culture to ensure that financial crime activities are prohibited within the organization. Internal controls mechanisms prevent the occurrence of external financial crime threats to which the institution is exposed.
- ✓ Criminals are very creative in developing methods to commit such crimes. They are heavily influenced by the economy, financial markets, and anti-money laundering or counter-financing of terrorism regimes where they operate. Many increasingly exploit the complex nature of financial services, making detection and prevention even more difficult. Furthermore, large-scale syndicates such as international organized crime groups take advantage of differences in national criminal legislation.
- ✓ The impact of financial crime on the economy, governance, and society is so significant that the survival of the whole financial system is put at stake because of complex criminal activities and structures built to perform these criminal activities. Financial crime has become a matter of concern to the States, and efforts are put in to protect the financial system's integrity and stability, cut off the resources available to terrorists, and identify those engaged in crimes or other criminal activities.

Financial crime is an illegal activity by organizations or individuals for monetary benefit. In the process, one party gains, and another party suffers a loss. Therefore, it is a significant threat to a country's economy, society, and global financial system, affecting its growth and stability. Financial crime is steadily rising in today's technologically developed world, resulting in massive losses:[9]

**Figure 3**

[9] Wallstreetmojo Team, (2023), Financial Crime, www.wallstreetmojo.com/financial-transaction/.




Source: Wallstreetmojo Team, (2023), Financial Crime, www.wallstreetmojo.com/financial-transaction/.

- Criminals are creating new deceptive tactics, and crime control authorities are devising ways to combat them. Such offenses may be related to cheques, credit cards, mortgages, property, terrorism financing, producing counterfeit goods or money, and even software and computer related.
- Financial crime is an unlawful practice that some entities or individuals conduct for monetary benefit. It affects not only society and nation but the entire global financial system.
- Financial crime is a growing concern for the various national governments. It can occur in banking, financial markets, medical and healthcare, real estate, or technology and communication-related fields.
- Financial crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and revenue of many organizations. In addition to the risk of losses from financial crime itself, companies also face spiraling costs in related areas.

## CONCLUSON

Economic or financial crime is an umbrella term that encompasses every type of criminal conduct that is linked to financial entities and markets, including banks, fintech companies, lenders, and so on. Additional examples often seen in recent years include pyramid schemes and pump-and-dumps affecting exchanges and retail investors. Financial crime can involve any type of dishonesty or fraudulent behavior, as well as misconduct and misuse of information, terrorism financing, and handling criminal proce.

All crime targeting financial organizations is financial crime in one way or another. In fact, sometimes this term is used to refer to all fraud that is related to money schemes, and thus encompasses an even wider range of behaviors. Some key types include: money laundering, tax evasion, embezzlement, forgery and counterfeiting, identity theft, bribery and corruption, terrorism financing,wash trading and pump-and-dumps,market abuse and insider trading.

## REFERENCE


1. CFI Team, (2024) Corporate Fraud - Overview, Reasons, corporatefinanceinstitute.com/resources/esg/corpor.
2. Financial Crime Academy, (2024), What Is Financial Crime? AML Terms Explained, https://financialcrimeacademy.org/wha.
3. Goldman Sachs, (2023), The Evolving Landscape of Corporate Payments Fraud, https://www.goldmansachs.com/.../payments-fraud.pdf PDF file.
4. Guanglin, S., (2023), Digital finance and corporate financial fraud – ScienceDirect, https://www.sciencedirect.com/science/article/pii/
5. Stripe, (2024), Six types of payment fraud—and how businesses can prevent them, https://stripe.com/resources/more/six-types-of-payment-fraud.
6. Verril, B., (2019), What is Corporate Payment Fraud, nsknox.net/blog/payment-fraud/.
7. WallStreetMojo, (2024), Corporate Fraud - Definition, Example, Type, Detection, Prevention, https://www.wallstreetmojo.com/corporate-fraud.
8. Wallstreetmojo Team, (2023), Financial Crime, www.wallstreetmojo.com/financial-transaction/.
9. Wall Street Oasis, (2024), Corporate Fraud - Overview, Reasons, and Examples, https://www.wallstreetoasis.com/.../cor.