



The Fraud Triangle: *A Core Foundation for Understanding Fraud*

For decades, infamous fraud scandals have unfolded in an all too familiar scenario; high-ranking execs across the world's most established institutions fly under the radar, until they don't. The sheer scale of their indiscretion, not only in losses they incur on the books, but also, in their audacity to defy most stringent compliance systems, is the stuff of Hollywood blockbusters. Often, their shock value inspired overarching scenarios on the whos, whys and hows behind the profitable business of deceit. But it also rallied businesses, governments and even the public around efforts to educate stakeholders and mitigate exposure to potential fraud risks, be they big or small.

In this article, we unearth the nuances and definitions of fraud in a deep dive into major categories and real-life case studies. We also dissect the "Fraud Triangle", a guiding framework to understand the reasoning, motive and patterns behind fraudulent behaviour and, in turn, the optimal course of action in addressing it.

What is Fraud?

Since the term was coined, fraud has been associated with moral and legal ambiguity that often rendered its regulation an after-the-fact affair. Many fraudulent acts had not been so until they set a precedent, often letting perpetrators run free as stakeholders rushed to clean up the mess. Still, the consensus, as the Black Dictionary sums it up well, is that fraud is “a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. It involves incompliance with a certain control (being it a law or a company policy) to make unjustified gain”.

Fraud involves malicious intent and legal misconduct, and results in action that exhibits both. Its spectrum, however, is far larger than this simple definition. Fraud is broad, debatable, multiform, and complex. It is a connected web of systems, individuals and technologies that work best together and seldom alone in cutting corners. And it is why governing bodies and regulators, particularly in the financial audit field, have placed considerable weight on outlining, at the very least, the parameters of this grey area.

Fraud Categories:

The Association of Certified Fraud Examiners (ACFE) classifies fraud under three main categories:

Corruption: Usually involves governmental employees and is difficult to detect, often entailing bureaucratic shortcuts that escape official processes and record.

Asset Manipulation: The outright theft of cash or inventory is a form of asset misappropriation. A less blatant example of asset manipulation could be overpaying vendors or employees, or paying vendors and employees that do not actually exist on a group/company, to siphon assets stolen from the system through the system itself.

Fraudulent Financial Statements: Usually more common in the private sector, and sometimes coined with the expression “cooking the books”. The company’s financial chiefs maliciously alter financial records and documents – such as balance sheets or income statements – in a misrepresentation of actual figures and a misleading view of the company’s standing and performance.

Additional examples of fraudulent acts include:

Kickbacks: Often interchangeably used with bribes, referring to the offering, acceptance and solicitation of illicit payments or gifts in exchange for facilitating or fast-tracking a process.

Identity Theft: Unlawfully claiming and using the identity of another person to have access to their financials, personal assets, and other entitlements in their name.

Embezzlement: Also known as theft, withholding or misappropriating assets or funds placed in one’s trust, often for personal interests and use.

Bid Rigging: The illegal collision of bidding parties to skew a tender in their favour against other bidders.

Payroll Fraud: Includes, as an example, employees faking attendance records to cheat the payroll system into exemptions from deductions and additional perks to which they are not entitled



While these categories offer a ‘feel’ of what constitutes fraud, case studies from the world’s high-profile corporates have come to highlight grave consequences of operating in a grey area – and on the very survival of these companies, at that.

Fraud Cases Company Level:

Take the 2001 case of Enron, a blunder of corporate corruption and accounting fraud that led to the energy giant’s bankruptcy, massive layoffs and billions of losses in pensions. It remains, to date, one of the most infamous cases of financial statement misrepresentation in the audit field. Its magnitude and importance fall back on three major factors and developments:

The scale of Enron: As one of the largest energy corporates at the time, Enron was the 7th biggest

company in the US in revenue terms during the late 1990s and early 2000, prior to its collapse in 2001, when it first filed for bankruptcy.

“It was on 2 December 2001, that Enron finally admitted it was bust. Its 20,000 employees were told they would lose their jobs, their health insurance, and their pensions. Its shareholders were told their investment was worthless,” recounted an article by The Independent in April 2006, titled “Enron: The Fraud that Changed everything”.

The involvement of audit giant Arthur Andersen: Arthur Andersen, which was considered among the biggest global audit firms back then, was explicitly accused of being a co-conspirator to Enron’s shady dealings.

According to a Wall Street Journal article titled: “Arthur Andersen Admits It Destroyed Documents Related to Enron Account”, Arthur Andersen “disclosed to federal agencies investigating the energy trading firm that individuals at the accounting firm in recent months disposed of ‘a significant but undetermined number’ of documents related to its work for Enron”.

The Sarbanes Oxley Act 2002: Enron’s fall from grace, along with other fraud scandals that unfolded in the period between 2000 and 2002, eventually led to the adoption of Sarbanes Oxley or SOX Act; a law that, till today, is considered to be the foundation for audit and governance best practices. The introduction of the law, as adopted in the United States Congress, stipulates that it is “an act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant

to the securities laws, and for other purposes”. The SOX Act, which was enacted on July 30, 2002, defined the reporting and control requirements to be applied by public companies, board of directors and audit firms. Another recent case that surfaced a few months ago in the United Arab Emirates (UAE) was that of NMC Health. In a region where fraud cases of such scandalous proportions are few and far between, the company fell under intense media scrutiny and public pressure. Initially incorporated by founder B. R. Shetty back in 1974, NMC Health had grown to become one of the biggest health institutions in the UAE, with sister companies operating across industries. Naturally, with great scale came even greater risk of misconduct. When first accused with fraud, the company, under the request of the London Stock Exchange, underwent an internal investigation that turned up a preliminary conclusion: “The company now believes its liabilities are at least \$6.6 billion — \$1.6 billion more than the previous estimate and more than three times its debts when investigations began in January. It has also identified about \$50 million in cheques that it believes were improperly written by group companies”, reported Gulf News on March 12, 2020, in an article titled “Fraud discovered at UAE’s NMC Health”. Several banks would then report on their risk exposure, in varying degrees, to NMC’s activities. They included powerhouse names such as HSBC Oman and Emirates NBD, as well several other international and regional financial institutions. A major aspect of the NMC Health case was financial misstatement, involving the use of wrong accounting/ control practices and methods to falsify and report inaccurate financial data on

the position and performance of the company. Effectively, several individuals at the scandal-laden holding group had misled creditors, investors, and regulatory bodies, by underreporting the amount of debt it held by some \$4.4 billion, later reported by The Guardian in an article titled: “Scandal-hit NMC Health on verge of liquidation”.

Fraud Cases Individual Level:

Individual fraudulent activities have also shown how people across organizational echelons can greatly impact business. In 2018, a bank manager at Webster Bank, USA, who has come to be known by the media as simply “Caesar”, single-handedly embezzled over half a million dollars from customer accounts without their knowledge and/ or consent. “Between 2003 and 2016, Cesar withdrew at least \$535,600 from account holders’ certificate of deposit (CD) accounts at Webster Bank, without the knowledge or consent of the account holders, used the embezzled funds for her own purposes, and took steps to conceal her misconduct”, revealed the United States Attorney’s office, District of Connecticut.

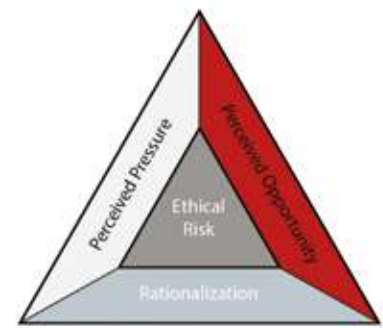
Government Level:

The long arm of fraud has gone far beyond commercial companies to reach high levels of the governmental sector. Corruption, a form of fraud, is strongly evident in the public sector, and more so within developing economies that remain riddled with regulatory loopholes. The corruption perception index scores and ranks governments/territories based on “how corrupt a country’s public

sector is perceived to be by experts and business executives. It is a composite index, a combination of 13 surveys and assessments of corruption, collected by a variety of reputable institutions”, as defined by Transparency International, a global movement working to fight corruption. In 2019, Denmark and New Zealand ranked first as the least corrupt governments, while Somalia, South Sudan, Syria, and Yemen, last as the most corrupt governments. Transparency International estimates the cost of corruption in EU member states to stand at approximately USD Billion 132 per year, while it this figure can considerably reach USD Trillion 1.26 per year among developing economies. This data suggests strong evidence that fraud can yield great adverse impact on individuals, businesses, communities and even countries. On the upside, these thorough studies by professionals and scholars show promise for existing frameworks that can be really useful in further understanding and tackling fraud at scale and at speed.

The Fraud Triangle:

In effect, extensive research on fraud, backed by empirical data, has led to universal guiding principles and frameworks among policymakers and regulators.



One such interesting and well-known framework that can help in understanding and addressing fraud is what is often referred to as the “Fraud Triangle”. It is a model that has stood the test of time, and is currently taught in many professional curricula and programs covering the fraud topic.

So, what is The Fraud triangle?

The idea of a fraud triangle was first brought forth in an article by criminologists Donald Cressey and Edwin Sutherland; the term was later coined by Steve Albrecht. Cressey developed the Fraud Triangle several decades ago. In his bid to examine the circumstances that led embezzlers to give in to temptation, he published the book titled “Other People’s Money: A Study in the Social Psychology of Embezzlement.” Cressey based his model on a rather elaborate hypothesis: “Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-sharable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property”. It is a dangerous combination of motive, knowledge, and logical fallacy.

Simply put, the triangle model suggests that individuals are motivated to commit fraud when three elements come together:

Pressure:
Perceived pressure, the motive/need for committing the fraud (e.g. need for money, addiction, etc.)

Opportunity:
Perceived opportunity, the situation that enables the fraud to occur, such as in the case of weak/non-existence internal controls (e.g. improper segregation of duties, weak access to rights controls, absence of records reconciliation, etc.).



Rationalization:
The ability to rationalize fraud as consistent with one’s values. In brief, it is the mindset of fraudsters that justifies their fraud with a clear conscience (e.g. “I’ll pay the money back, they will never notice the funds went missing”, etc.)

Take, for instance, the following fraud scenarios, where we analysed the contribution of each element in a given fraud act.

Scenario 1:

The premise: :
Marc works in a large-scale grocery store that operates 24/7, and he usually attends to night shifts alone. He has a severe gambling addiction that compromises his control over his own finances.

One night, Marc decides to take some money from the cash register for his personal use. With no cameras in place, and the cash check/inventory check being often carried out by Marc, and rarely by his supervisor, Marc has direct and unsupervised access to the cash register. Now, if we are to look at this premise through the fraud triangle framework, we can easily map out all three elements:

Pressure:
Marc’s gambling addiction is causing him to run through his own money and savings. He is now struggling to make ends meet and cover his day-to-day expenses.

Opportunity:
In the absence of periodic and regular inventory/cash counts attributing sales inventory to the money in the cash register, as well as of surveillance cameras, Marc’s indiscretion can go undetected for long periods of time.

Rationalization:
In a bid to clear his conscience, Marc would convince himself that a large grocery shop with probably millions of dollars in annual sales would not be severely affected by his petty cash theft – and neither would the business, its owners, or its employees.

Scenario 2:

The premise:
Rana is a governmental municipality employee who is tasked with preparing and approving invoices, as well as collecting cash in exchange for cleaning services rendered by the municipality within its jurisdiction.

Rana’s daughter wants to pursue her higher education studies at an international university. Rana is under immense pressure to source the funds for her daughter’s exorbitant tuition fees. She comes up with a small-scale scheme that can very well safeguard her daughter’s educational future. Rana decides to simply add 1\$ for each invoice she is issuing/collecting, particularly when dealing with elderly citizens. She would need to keep this scheme going for one year if she were to collect funds of USD 100,000 – just enough for her daughter’s tuition fees. Similarly, by dissecting the above scenario based on the fraud triangle framework, the following can be understood:

Pressure:
Rana’s pressure to provide funding for her daughter’s education is posing daily psychological, emotional, and not to mention financial pressure on Rana. She has to think and act fast to secure her daughter’s place in a top-brass university.

Opportunity:
The fact that Rana was authorized to prepare and approve invoices, and at the same time, collect the corresponding cash amounts is a major control weakness – in this case, known as the absence of segregation of duties.

Rationalization:
Rana logically reasons that adding 1\$ to each invoice will not have a major impact on taxpayers’ lives, finances or wellbeing. Rather, these taxpayers would be indirectly contributing to the educational future of her well-deserving and ambitious daughter.



If the scenarios above are anything to go by, fraud operates, thrives and is often justified in the grey area of moral logic. The consensus, however, is that fraud is wrong. Small fraudsters who cheat the system and go undetected and unpunished often graduate to high-level embezzlers. Look around you, and you will find many cases that very well fit the fraud triangle framework. And when you do, be sure to be part of the solution, rather than turn a blind eye on the problem.

“Rather fail with honor rather than succeed by Fraud.”

In the upcoming article, we will address key challenges governmental bodies may face in breaking down the fraud triangle, and practical strategies and tools that can be applied to overcome such challenges. As the ancient Greek dramatist Sophocles once so well put it: “Rather fail with honour rather than succeed with Fraud.”

Jointly with



Maher El Khatib, CFE, CIA, CISA, CRMA
Group Internal Audit Manager
Governance, Risk & Compliance Department
Chedid Capital



Bassel Khreiss, MSc
Consulting Professional