



Unpacking Fraud

In the South African context fraud is defined as:

“The unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another.”


Therefore, Fraud comprises the following four elements:

- Unlawfulness – the action must be seen to be wrong in the eyes of society
- Misrepresentation – a false statement made by one person to another
- The misrepresentation may take the form of words; words & conduct; or just conduct
- A misrepresentation may also be a failure to disclose certain information in circumstances where there is a duty to do so.
- Intent – the person making the misrepresentation must have intended, or foreseen that the victim would be deceived.
- Prejudice – the victim would have suffered prejudice by reason of altering his position to his detriment after relying upon the misrepresentation. Potential prejudice is also sufficient if it is reasonably possible that the victim, relying on the misrepresentation, would have suffered harm.

We can then say that in the broadest sense, fraud can encompass any crime for gain that uses deception as its principal modus operandi.

Fraud Categories

Forum Partners: Association of Certified Fraud Examiners of SA (ACFE SA), Corruption Watch, The Ethics Institute, Institute of Directors of Southern Africa (IoDSA), Institute of Internal Auditors of South Africa (IIA SA), Institute of Risk Management of South Africa (IRMSA), South African Institute of Chartered Accountants (SAICA) and South African Institute of Professional Accountants (SAIPA).



There are primarily two types of fraud victims; individuals and organisations. Fraud against organisations can be committed either internally by employees, managers, officers, or executives/owners of the organisation, or externally by customers, suppliers, organised crime syndicates or competitors.

1. Fraud against individuals

The most common schemes to defraud individuals are Identity theft, Ponzi schemes, pyramid schemes, phishing schemes, and advance-fee (419) frauds.

2. Fraud against organisations

2.1 External Fraud

Examples of external fraud would be bid-rigging schemes, false invoices, bribery, and theft of intellectual property, security breaches, hacking, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.

2.2 Internal Fraud

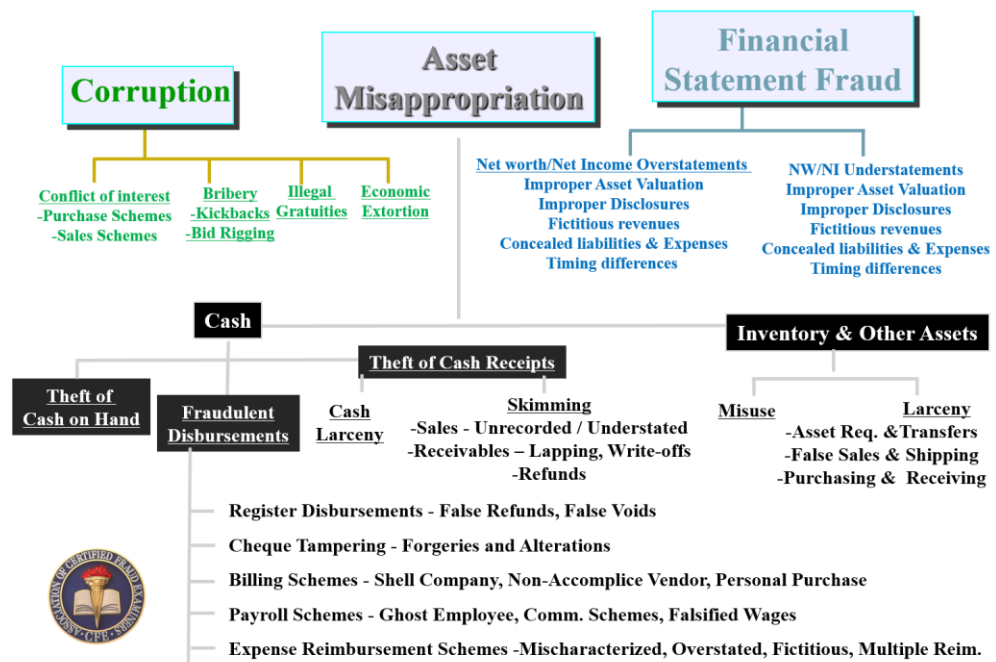
According to the Association of Certified Fraud Examiners (ACFE) , Internal fraud can be defined as: “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the organization’s resources or assets.” This type of fraud, also known as occupational fraud, happens when an employee, manager, or executive commits fraud against, or on behalf of, his or her employer.

Fraudsters are increasingly embracing technology (unlike many of their victims!) and therefore utilising new methods in committing and concealing their frauds. The basic methodologies used in the frauds, however, tend to fall into clear, time-tested categories. To identify and describe the schemes, the ACFE developed the Occupational Fraud and Abuse Classification System, also known as the Fraud Tree

The Fraud Tree has three major types of occupational fraud:

1. Corruption,
2. Asset Misappropriation, and
3. Financial Statement Frauds

Occupational Fraud & Abuse Tree



1. Corruption categories:

- 1.1 Conflicts of Interest** – where an employee has an undisclosed interest in a business transaction that adversely affect the employer when buying from or selling to the organisation. It's human nature to favour friends and family hence the requirement by most organisations for employees to disclose potential conflicts of interest.
- 1.2 Bribery** – there are two types of bribery schemes; kickbacks, where an employee colludes with a vendor to charge higher than market prices with the understanding that part of that excess will be “kicked back” to the employee and the other part to the vendor, and bid rigging, where the employee colludes with a vendor to ensure that that vendor is awarded the bid in the employer’s ‘competitive’ bidding process.
- 1.3 Illegal Gratuities** – offering or asking for illegal gifts – gifts that are not condoned under the organisation’s code of conduct.
- 1.4 Economic Extortion** – this is the same as bribery except the employee initiates the corrupt deal instead of the vendor. Basically, the employee tells the vendor, “pay me or you don’t get the order”.



2. Asset Misappropriation categories

2.1 Cash

2.1.1 Theft of cash on hand – where the perpetrator steals cash kept on hand at the victim organisation's premises.

2.1.2 Theft of cash receipts – here the perpetrator will steal cash receipts, either via cash larceny (stealing the cash after it has been recorded on the organisation's books) or via skimming (stealing the sales or receivables before they are recorded on the organisations books).

2.1.3 Fraudulent Disbursements – paying false invoices, paying ghost employees, paying false expense reimbursements, issuing fraudulent cheques, and fraudulent cash register disbursements.

2.2 Inventory

2.2.1 Misuse of inventory/assets

2.2.2 Theft of inventory/assets

3. Financial Statement Fraud

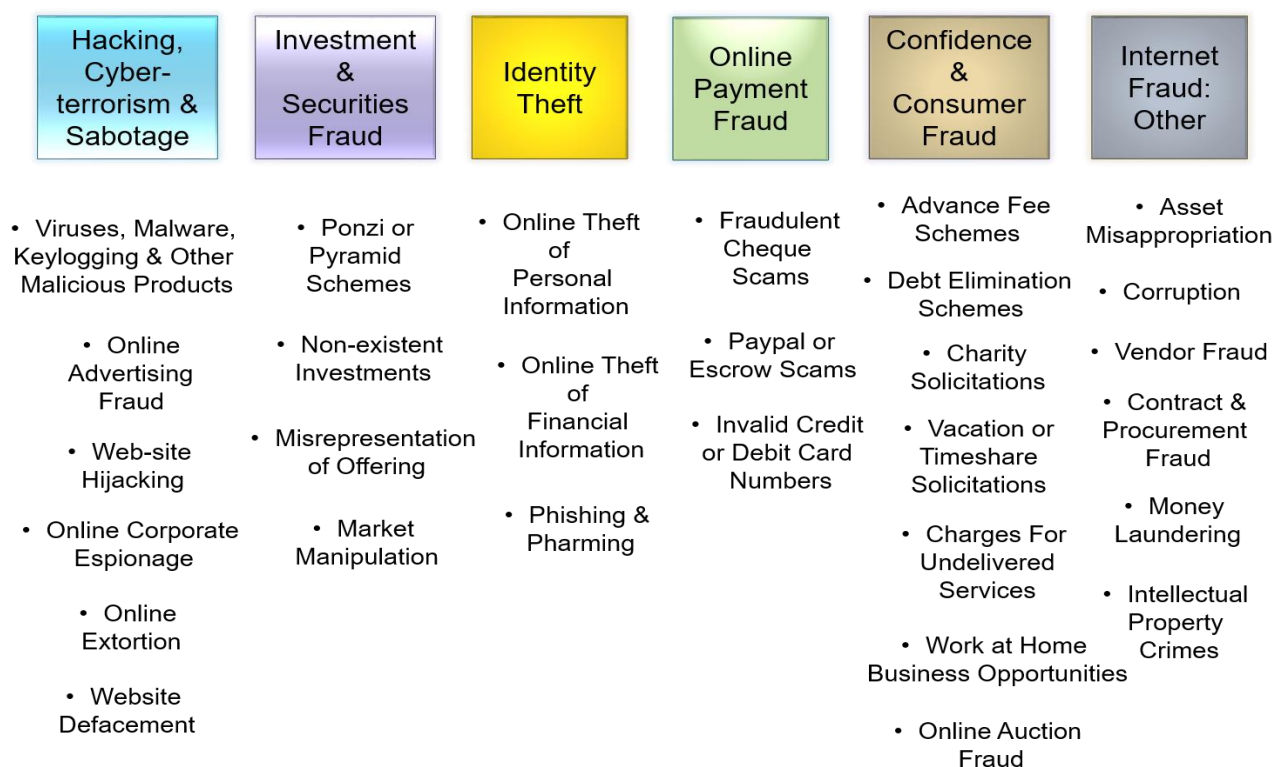
Net worth / Net Income Overstatements and Understatements. This type of fraud is perpetrated by the executives to either make their organisations performance look better or worse, depending on what their desired result is.

There are five schemes that are utilised to over or under-state assets and liabilities: a) improper asset valuations, b) improper disclosures, c) fictitious revenues, d) concealed/overstated liabilities & expenses, e) timing differences

Some of the highest impact frauds today occur in the cyber world and Joseph Wells, the founder of the ACFE, published a book called 'Internet Fraud Casebook: The World Wide Web of Deceit' . In it Wells describes the Internet Fraud Tree as follows:



Internet Fraud Tree



Hacking, Cyber-terrorism & Sabotage

- *Viruses, malware, keylogging & other malicious products* – these products are transferred to computers usually by an individual clicking on a link or downloading images or programs such as pornography or video player ‘updates’.
- *Online advertising fraud* – primarily ‘click fraud’ where advertisers are charged for clicks on their ads from thousands of fake people.
- *Web-site hijacking* – websites are either redirected or the content scraped
- *Online corporate espionage* – hackers for hire are paid to obtain the data that is not publicly available on a competitor or foreign country.



- *Online Extortion* – Websites, like Ashley Madison, are hacked and the members blackmailed. Alternatively, the latest threat is Ransomware where organisations are blackmailed after their data is encrypted.
- *Website defacement* – hackers gain administrator access to organisations websites and then proceed to deface them. Well over 100 000 South African websites have been defaced in the past few years.

Investment and Securities Fraud

- *Ponzi or pyramid schemes* – a Ponzi scheme is an investment scheme where investors are provided fake statements showing their investments have grown by huge percentages, which encourages them to invest more and tell friends and family. A pyramid scheme is a multi-level marketing scheme where the bulk of participants' earnings are dependent on recruiting with levels and stages emphasized and participants usually have to pay a joining fee and/or buy products. Non-existent investments, Misrepresentation of offering and Market manipulation are all variations of the Ponzi scheme.

Identity Theft

- *Online theft of personal information* – fraudsters gain personal information on individuals and then pose as these people in order to defraud, e.g. buy an expensive motor car
- *Online theft of financial information* – criminals obtain the list of customers of an organization and then send fraudulent faxes or emails from the supplier, informing the clients of a change of bank details. The clients usually don't phone to confirm and simply change the bank details and the next payment goes to the criminals. With BEC (Business Email Compromise) fraud, the fraudsters find out who the most senior person is and then send an email to a person in finance, allegedly from the CEO, informing them to make an urgent payment. In many organisations employees fear the CEO, who demands absolute obedience, so the request tends to be actioned.
- *Phishing and pharming* – Phishing is a fake link emailed to a victim while Pharming is where the victim is redirected to another fake site when surfing the net. Pharming can be done either by hacking the victim and changing the hosts file on the victim's computer or by hacking the DNS server software. DNS servers are computers that resolve Internet names into their real IP addresses.




Online Payment Fraud

- *Fraudulent cheque scams* – if you're selling something, the criminal buys the item but sends you a cheque for more than the selling amount and they ask you to refund the difference. The cheque is a stolen cheque that bounces.
- *PayPal or escrow scams* – There are many PayPal scams, one of which is the Shipping Address Scam where the scammer asks for the items to be shipped to an address and money is paid into your PayPal account. You send the item to the required address. The reality, however, is that the delivery address is invalid, and the shipping company cannot find the location to make the delivery. After several attempts they flag the item as undeliverable on their system. The scammer then contacts the delivery company giving them the new address where the parcel can be delivered to. The result is the scammer gets the item and files a complaint with PayPal that the item was not delivered. You have no proof that it was indeed delivered as the transaction detail shows the original address. PayPal Seller Protection only covers the shipping address that PayPal has on the system and therefore not only do you lose the item but also the money. Escrow is a legal concept in which a financial instrument or an asset is held by a third party on behalf of two other parties that are in the process of completing a transaction. There are legitimate companies, like Escrow.com and many fake ones too.
- *Invalid credit or debit card numbers* – there are many sites selling fake or skimmed credit and debit cards details, especially on the dark web.


Confidence and Consumer Fraud

- Advance fee schemes – the famous 419 scam where you must pay an upfront fee to get a huge amount of money under guise of a tall story.
- Debt elimination schemes - People who are in financial trouble can easily fall for an e-mail claiming to relieve their debt. This scam makes the false promise of collaborating with creditors to either consolidate or settle debts. All you need to do is pay an up-front fee for the services.
- Charity solicitations – there are many fake charity websites popping up, especially after a natural disaster but there are also legitimate-looking charities that do give to needy causes, but they keep 99% of the money and give just 1%!
- Vacation or timeshare solicitations – fraudsters are selling timeshare and holiday weeks of victims via online classifieds.

- 
- Charges for undelivered services – you receive an invoice out of the blue for tax services, for example or your company receives an invoice for an ad that was placed in a magazine – you even receive a copy of the ‘ad’ to convince you it was placed!
 - Work at home business opportunities – most of the work from home business opportunities are scams with the victims having to pay joining fees.
 - Online auction fraud – there are many types ways of perpetrating this fraud, some of which are; 1) Non-delivery. The seller places an item up for bid with no intention of delivering it, 2) Misrepresentation where the seller deceives the buyer as to the true value of an item, 3) Black-market goods. Illegal goods sold on online auction sites, 4) Fee stacking where the seller adds hidden charges to the item after the auction is over, 5) Triangulation, where stolen credit is used to buy from an online merchant and the item is resold at auction, and 6) Shill bidding, which is the intentional fake bidding by sellers to drive up the price of their items.

Internet Fraud

- *Asset Misappropriation, Corruption, Vendor Fraud and Contract & procurement Fraud* are some of the traditional Occupational Frauds that were discussed at the beginning of the article. The only difference is that these frauds are now perpetrated online, using computers. For example, fraudsters submit fraudulent purchase orders from government departments and the victims, who tend to not do due diligence, accept the order and deliver the merchandise to a fake address. When they don’t get paid after 30 days they approach the government department querying their payment only to be told that the orders were fake.
- *Money Laundering* – dirty money is now laundered through online businesses like casinos but also via ‘transaction laundering’, where legitimate merchant accounts are used to process unknown transactions for another business, for example, an ‘affiliate’ who sells on your behalf.
- *Intellectual Property Crimes* – includes individuals’ or business’s ideas, inventions, and creative expressions, which can be in the form of trade secrets, business plans, client lists, etc. A 2010 UK IP crime report found that 59% of employees ‘let go’ took IP when leaving while 25% of remaining employees collected IP ‘just in case’.



How Rife is Fraud?

We often get asked this question as many executives like to believe their employees are all honest but there is no denying the fact that the above frauds (occupational frauds and internet frauds) are affecting the majority of private and public sector organisations of all sizes, and the attacks are getting worse each year.

Fraud facts

- In the 2018 PWC Global Economic Crime Survey, South Africa was found to have the worst white-collar crime rate in the world.
- A similar study conducted by the Association of Certified Fraud Examiners in 2016 called the Report to the Nation, found that the typical organization loses 5% of its annual revenues to fraud. The study also found that once victimized, an organization was unlikely to ever recover the losses.
- “Fraud has become pandemic around the world and if fraud were a disease, political leaders of all our nations would have to declare a global health emergency!” - Jeffrey Robinson, international organized crime & fraud expert.

The current economic recession is fuelling the fire with previously ‘honest’ people now starting to lie, cheat and steal, and current fraudsters are being caught as organisations are now looking out for the cents as not just the Rands, thereby exposing the fraudsters who have been defrauding through the previous ‘good’ economic years. As Warren Buffet says, “Only when the tide goes out, do you see who’s been swimming naked”!

It is therefore crucial that organisations implement a best practice anti-fraud strategy to prevent, detect, investigate and remediate frauds. The components of a best practice anti-fraud strategy will be discussed in future papers.

References

- Association of Certified Fraud Examiners SA
 - <http://www.acfe.com/fraud-101.aspx>
 - <http://www.acfe.com/fraud-tree.aspx>
 - <http://www.acfe.com/InternetFraudCasebook/>
 - <http://www.acfe.com/rtn2016.aspx>
 - Price Waterhouse Coopers <https://www.pwc.co.za/en/press-room/reported-economic-crime-in-south-africa-hits-record-levels.html>