Western Cape Government

ISSUE 22 IMPACT

Evolution of Fraud

Just as times have changed and technology has evolved, so has the common law offence of fraud. Over the years, fraudsters have found more innovative ways to commit this offence.

Recap

The definition of fraud[1] is the unlawful and intentional making of a misrepresentation which causes actual harm to another or has the potential to cause harm. Given its definition, in order for fraud to be proven, the following elements must be present:

● **Making of a Misrepresentation** ● **Unlawfulness** ● **Intention** ● **Harm/Prejudice**

[1] *Criminal Law: CR Snyman - 2014*

So, how has fraud evolved over time?

300 BC

The earliest recorded attempt of fraud

Hegestratos, a Greek sea merchant, took out an insurance policy known as bottomry against his ship and its cargo, which allows the merchant to borrow money on the basis that when the ship and its cargo arrive at its destination, and the cargo is delivered, the loan is paid back with interest. If the loan is not repaid, the boat and its cargo or goods to the value of the loan plus interest are repossessed. Hegestratos, however planned to sell his cargo (corn) and sink his empty ship in order to keep the loan as the guaranteed security would no longer exist. Hegestratos was caught in the act of sinking his ship by his crew, was thrown overboard and drowned while trying to escape. Hegestratos made a misrepresentation by distorting the truth which brought potential prejudice to his lender.

193 AD

The year of the five emperors

The Praetorian Guard – a special group of soldiers supposedly loyal to the emperor Pertinax – assassinated Pertinax and held an auction to sell the Roman Empire to the highest bidder. A man called Julianus submitted an astronomical bid of 250 pieces of gold for every soldier in the army. The soldiers misrepresented that they had the rights to sell the Roman Empire.

1821

The imaginary prince

Gregor Mcgregor, a General in the Scottish army, boasted some impressive war achievements, but he also boasted that he had conquered a small island and became it's "Cazique" (prince). This small island, "Poyais", was however made up. This did not stop him from promising investors lavish homes and a life in paradise. Some even exchanged their Sterling for his own fabricated currency. His misrepresentations resulted in people buying houses which did not exist or exchanging their money for a non-existent currency, as a result, they suffered a loss.

1911

Louvre at first sight

Argentinian Eduardo de Valfierno was the mastermind behind the theft of the world-famous Mona Lisa painting. It is widely reported that Eduardo paid a Louvre employee to steal the painting which he had no real use for. He just needed people to know it was missing so that he could sell his replicas to underground collectors, misrepresenting it to them as the original painting.

1920

Ponzi

There have been countless Ponzi schemes over the years, but the original scheme was created in 1920. Italian-American, Charles Ponzi, discovered he could purchase postal vouchers in other countries, ship them abroad and make a modest 5% profit. He somewhat exaggerated this margin when selling to investors, promising them a 50% profit. Investors threw their money at him, with early investors being paid their "profit" from the money paid to Ponzi by his latest investors. His scheme ran for over a year, costing investors $20 million at that time. He was caught out and arrested in August 1920 and charged with 86 counts of mail fraud.

Source: https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/5-of-the-most-remarkable-instances-in-the-history-of-fraud/

1964

Identity theft

Long before the internet was around, fraudsters could steal your identity through "dumpster diving" (going through your trash) to find personal information on papers you had thrown out like statements and other documents. They could also use phone scams to obtain your personal information, e.g. a fraudster contacts you and tells you that you won a prize and that they need information like your date of birth or identity number to verify your identity. The fraudster then uses this information without your permission, to commit fraud – like applying for credit using your personal information (without your knowledge or permission) and incurring debt you become liable for. With the advent of the internet and other technology, identity fraud has become more common.

*Sources:
https://www.spamlaws.com/id-theft-history.html https://en.wikipedia.org/wiki/Identity_theft#:~:text=Identity%20theft%20occurs%20when%20someone,theft%20was%20coined%20in%201964*

The now

Cyber Fraud

Cyber Fraud is the fraud committed via an electronic device with the intent to steal and misuse an enterprise's or another individual's personal and financial information stored online.

Remote working has led to digital dependency, resulting to an increase in cyber fraud. According to an article titled "Beware of cyber fraud when working from home", there has been a sharp spike in the number of phishing attacks since the outbreak of the coronavirus with many of us working from home, exercising less vigilance. Information Security is a key function within the WCG and one of its main purposes is to ensure that information is protected against disclosure to unauthorised users and improper modifications. Various Microsoft product suites have been adopted as an enterprise standard to secure the workstations and servers on the WCG corporate network.

Phishing is a method of trying to steal personal information using deceptive e-mails and websites. Phishing scams continue to increase at alarming rates.

Source: https://www.sowetanlive.co.za/business/money/2020-06-04-beware-of-cyber-fraud-when-working-from-home/.

A couple of days before the monthly payroll is due to be finalised, an email with a subject line "Urgent" appears in a payroll officer's inbox. An "employee" is requesting a change of their bank details, they're working from home but cannot access their work emails and they know the cut-off date is looming. The sender's name in the email is familiar and the way it is written seems plausible. The payroll officer completes the necessary forms after the "employee" requests the update of the bank details. After the payroll run, the employee reports to the payroll officer that he/she did not receive their monthly salary. Upon further investigation it is established that the request received for the change of the banking details was from a fraudster who purported to be an employee, and the change in bank account details resulted in the salary being paid into the fraudster's bank account.

Requesting a change to employee information is an increasingly popular form of cyber fraud known as a "business email compromise" attack. It enables fraudsters to trick individuals to provide personal information to seemingly legitimate employees/colleagues, however, by providing the information the security might be compromised or personal information is leaked and can be used for various other crimes.

Source:https://www.peoplemanagement.co.uk/long-reads/articles/hr-cyber-criminals-latest-target#gref

Evolving Investigative techniques

The evolution of fraud has necessitated the evolution of investigation techniques in order to respond to the more sophisticated methods of committing fraud. Fraud detection and investigation now involve both human intervention and the use of tools/artificial intelligence. An integrated analytics driven approach, which relies on both human and artificial intelligence to eradicate fraud, will enable an organisation to proactively manage fraud risks, aiming at fraud prevention.

In fraud detection, for example, analytics tools such as IBM I2 Analyst's Notebook can be used to uncover hidden connections in sets of data and maps relationships between sets of data. E-Discovery tools such as Intella, allows forensic investigators to process, search and analyse data making it easier to find critical information within that data. Data analytics can be used to identify trends, exceptions or red flags in large sets of data, using a set of parameters, that could indicate fraud.

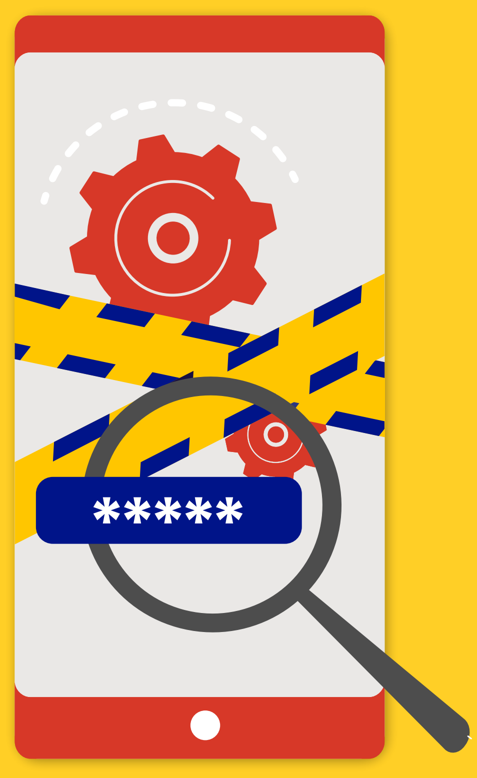
Eliminate the element of surprise - scrutinise!

The Department of the Premier's Centre for e-Innovation embarked on an Information Security Awareness campaign in June 2021, which, through short videos, provided insight into phishing scams and what you should be looking for when you are confronted with such scams. They provided the following pointers:

- Be cautious about all communications you receive. If it appears to be a phishing communication, do not respond. Delete it.
- Do not click on any links listed in the email message, and do not open any attachments contained in a suspicious email.
- Do not enter personal information in a pop-up screen. Legitimate companies will not ask for personal information via pop-up screens.

Interpol's African Cyber threat Assessment report 2021[2], provides a few more useful tips:

- Back up files regularly and securely online and offline
- Strengthen your home network
- Use strong passwords
- Keep your software updated
- Use two-factor authentication on your social media accounts
- Check privacy and security settings



[2] *African Cyber threat Assessment report, Interpol's key insight into cybercrime in Africa October 2021*

Join the fight and stop fraud in its tracks!

Tip-offs remain one of the most invaluable sources of information to detect fraud and the WCG encourages all employees and workers to speak up and blow the whistle responsibly when they suspect corruption, fraud and theft. (See the Whistle-blowing Policy here). Report any suspicions of fraud and corruption affecting the WCG to Provincial Forensic Services:
Post: PO Box 659, Cape Town, 8000. **Tel:** 021 483 0901 **E-mail:** Tip.Offs@westerncape.gov.za **Toll-free** to National Anti-corruption Hotline **(NACH):** 0800 701 701

Let us protect the integrity of our government.