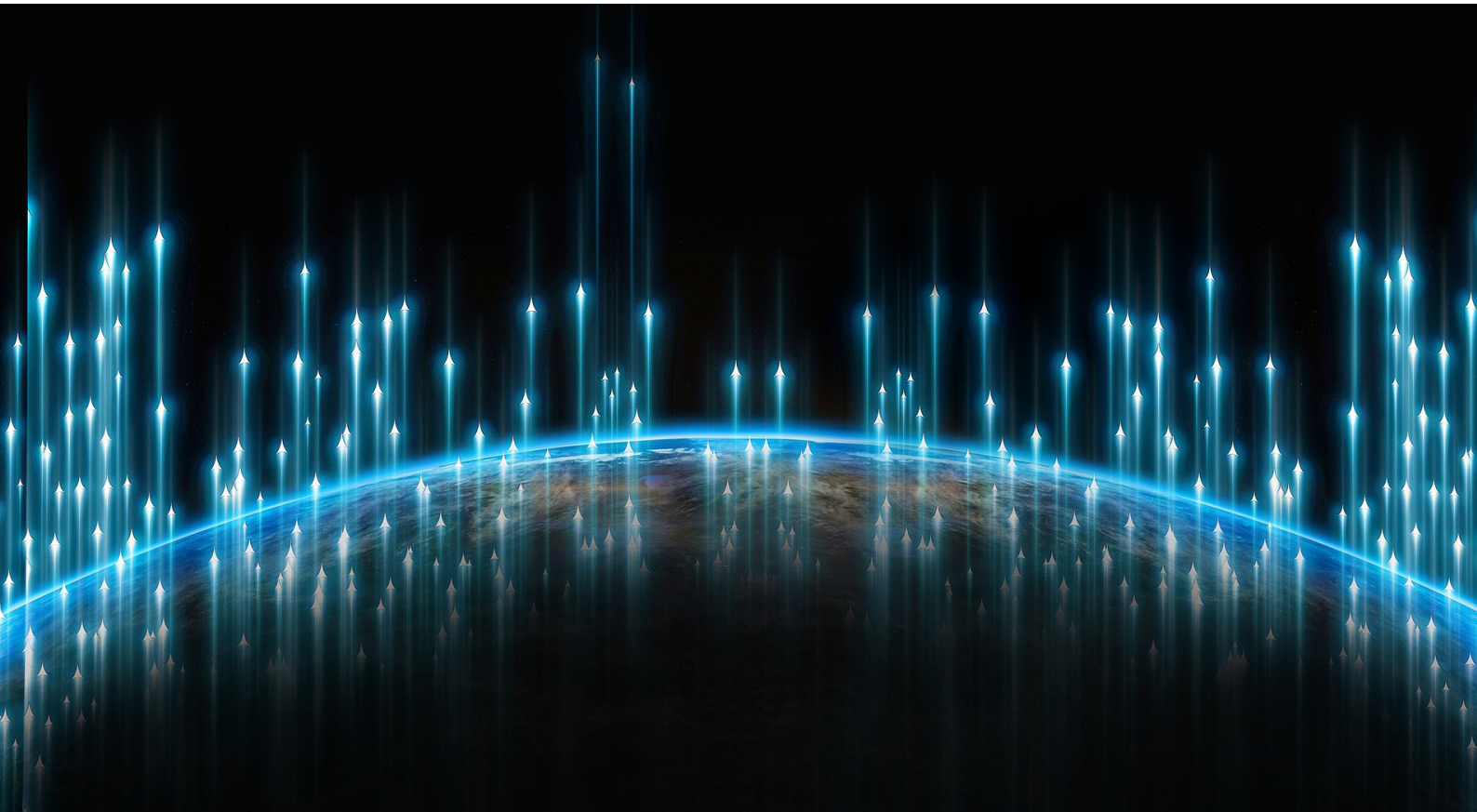
# IDENTITY THEFT:

## HOW MODERN IDENTITY THEFT OPERATES AND IMPACTS THE BUSINESS

May 2022 Newsletter

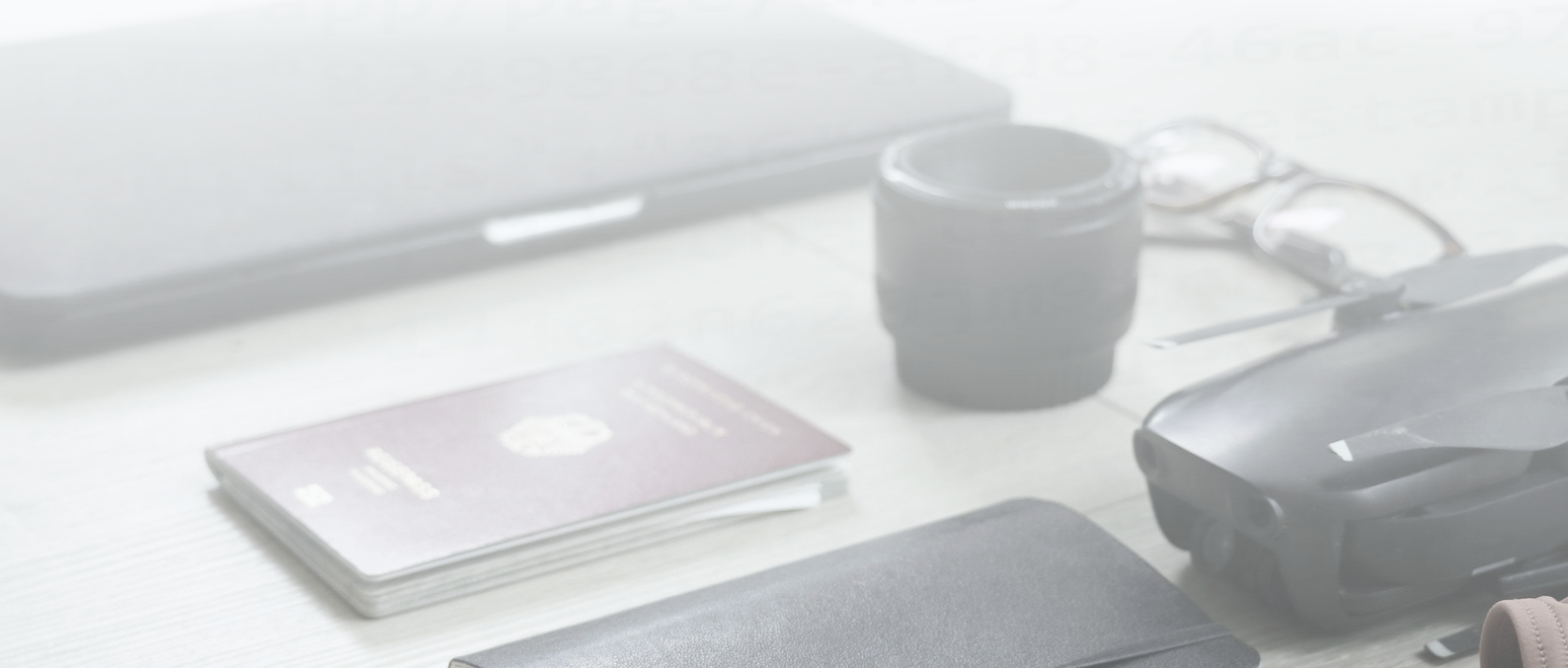
18th Edition

RMG



# TABLE OF CONTENTS





## FOREWORD

Identity theft takes on many forms and is an ever-evolving form of commercial crime. What constitutes a commercial crime is not always clear-cut, and it is important to know that simplistic events can occur throughout the business if management is not vigilant during their evaluation of internal controls.

With the implementation of the **Protection of Personal Information Act 4 of 2013 ("POPIA")** employers must fulfil the requirements of the act before being able to be compliant enough to store the information entrusted to them by employees who at times do not even know what POPIA entails. Even for ground-level employees, it is essential that training on all forms of commercial crime is given to lay the foundation for an ethical and effective corporate culture that radiates throughout all tiers of the business hierarchy.

## WHAT IS IDENTITY THEFT?

We live in an age where digital platforms are becoming the norm throughout the digital revolution. Currently, as throughout history, the protection of personal information is of paramount importance within many facets of the industry and life. Go Legal has reported that often private information gets shared and used in ways that the sender has never known to have agreed to. This includes impersonation, creating debt, and other nefarious criminal activities.

**Cybercrime** is the most prevalent factor in the commercial crime spectrum in terms of personal information, however, there are several ways that Identity Theft can occur, not only overstepping internal controls resulting in disciplinary proceedings but may incur legislative and reputational repercussions due to unwittingly agreeing to terms and conditions. Unethical businesses will often make their terms and conditions hard to comprehend and use language that is deliberately difficult to understand to confuse the consumer. Employers can encourage employees to do regular personal credit checks through companies such as One Identity, TransUnion, or Legal and Tax to check for any anomalous activities

**Physical identity theft** can occur through actions demonstrated like the theft of documents or account statements, stealing postal packages, and telephonic impersonation to disclose or update information. However, in the new age, cybercrime and identity theft have merged, resulting in victimisation without the physical presence of a perpetrator or physical theft.

## THE HIDDEN LEAK

Often information is obtained from individuals without their knowledge of any crime taking place. Higher-level information can be obtained by organised criminal syndicates that facilitate these crimes through digital impersonation or to create "fake identities". Apart from the obvious financial exploitation that is the trump throughout the identity theft playing field, there are many other uses that criminals can use the identity of another for example:

- Escape criminal prosecution
- Obtaining employment as a foreign citizen
- Claim social grants and apply for other "person-specific" benefits
- Claim medical benefits and access pension funds

These large-scale information grabs can come from even the lowest of employees, as criminal organisations do not just target the digital information that is stored online but would target workers who would not be suspected to be accessible. This can be mitigated by having internal security of information controls in place that only restricts information access to very few individuals. The most prevalent was personal information is obtained through Internet of Things ("IoT") methods are:

**Phishing** reported by Terranova security as a cybercrime that uses digital communication to steal confidential and corporate information. Victims are tricked into giving up personal information such as financial information, mailing addresses, and organisational information.

**Pharming** reported by Kaspersky as an instance of phishing where a website traffic flow is manipulated, and large quantities of confidential information is stolen. It is in essence the act of producing a fake website and then redirecting users to it

This information can be obtained by cybercriminals if management is not diligent with security training. Reported by BusinessTech.com, TransUnion suffered a cyberattack early in 2020 by the group N4aughtysecTU that allegedly gained access to the personal records totalling 4 terabytes of data. It is essential to understand that the commercial crime

platform does not have mercy and does not discriminate, criminals will attack mega moguls as easily as mom- and pop-owned organisations.

The theft of personal information can occur even in the "greatest" and "most secure" organisations. Reported by currentware, a sub-lieutenant in the Canadian navy was passing through confidential military information and personal information of military employees to the Russian embassy in exchange to elevate his dire financial circumstances. This was done using a floppy drive as the device was seen as redundant, the desperate employee used personal technology to export the files to a USB drive.

## REAL LIFE SCENARIOS

Through diligent investigations, RMG has noted trends in relation to identity theft. As outlined above, identity theft can target either an individual or an organisation. **One example** of personal identity theft is that of a newly appointed director of a leading producer and supplier within African and global markets, referred to as Mr. L. In recent months, Mr. L received an SMS requesting a payment be made on his account which had fallen into arrears. Mr. L immediately became suspicious as he did not have an account at the specific retail outlet. Upon contracting RMG offices, it became evident that multiple accounts had been opened using Mr. L's details which could easily be found in the public domain such as CIPC. Had this criminal element been left undetected, debt of hundreds of thousands of rands could have been racked up in Mr. L's name without his knowledge. While it is important to be cautious of the information available in the public domain, it is

furthermore vitally imperative to regularly conduct credit due diligence on yourself to ensure accounts allocated to your name or identity number are true and correct.

Identity theft perpetrated against an organisation, can be done with the assistance of criminally-aligned employees, or with the absence of internal controls – or worse, the presence of ineffective internal controls. Identity theft illustrates the importance of performing accurate and thorough due diligence before entering into contractual business agreements.

**A second real-life example** of organisational identity theft is that of a leading international supplier with their head office in South Africa. RMG's client was approached by a criminal syndicate impersonating a wholesale and retail group. An improper due diligence was conducted, and an account and credit facility opened for the criminal syndicate purporting to be legitimate traders during the first 3 transactions in an amount of R480k. These transactions were legitimate and paid for in full leaving the client to believe that the bona fides of the respected relationship is intact and honoured. The suspects engaged in the third transactions in the amount of approximately R1,5 M worth of stock and transportation fees with no intention to honour this transaction. Had an impartial and objective due diligence been performed at the onset, it would have come to light that our client was not dealing with the genuine wholesale and retail group. Furthermore, had stricter internal governance and verification and financial controls

been in place regarding accounts, the criminal syndicate would not have been able to entice the client sales department that was commission driven and had no knowledge of proactive and preventative risk management principles that should have been the primary decisive factor to continue with transactions with the bogus entity.



**A third real-life example** is an act of organisational identity theft perpetrated by an employee. Our client, a merchant-based system service provider, was alerted by their customer that they did not receive a settlement of their account, however it had been paid from our client's side. Further investigation revealed that the account details had been changed using fraudulent documentation. A list of fraudulent transactions was identified, indicating the theft of more than R500 000 over a period of 3 months. The criminally motivated employee had created fraudulent documentation using their customers' details but with her own elected bank details. The suspect was identified via the accounts that the fraudulent deposits

were made into and led to a successful prosecution of the accused. Unfortunately, in instances such as these, due to the time lapses during the investigation, the possibility to recover stolen funds are in most cases slim to none.

## CONCLUSION

It is thus not only the responsibility of the employee to hoist the yolk of security of information but shared alongside the responsibility of the employer to ensure that these security protocols are performed without question and followed to the letter to ensure a tighter grip on securing and hosting information. Having POPIA and the GDPR in place mitigates risks but can never completely erase the threats looming in the shadow; ever evolving to take on more terrifying forms. Is it not man's greatest fear to have his face, identity or name stolen and be incriminated falsely?

## BIBLIOGRAPHY


Go legal

Legal and tax

Law for all

Kapersky pharming

Terranova secutiry

BusinessTech

CurrentWare