**Article written by Nombuyiselo Mvelase, Candidate Attorney, checked by Jordan Dias, Associate and released by Maike Gohl, Partner at Schindlers Attorneys**

06 September 2021

**Introduction**

In an age where we are often required to share personal information such as our credit card numbers and identity numbers to make transactions online, it is important to remember that this information can be used by criminals to commit various crimes. This article defines identity theft, outlines the ways in which our personal information can be or is obtained and how individuals can protect themselves.

**The definition of identity theft**

Identity theft is commonly defined as the theft of someone’s personal information in order to impersonate that individual, with the intent to commit a crime. Although credit card fraud is the most common, there are various types of crimes that are linked to identity theft including organised crime, money laundering and human and drug trafficking. Despite the fact that South African law does not make specific provisions for identity theft as a crime, a perpetrator can still be held liable for the crimes he/she commits once identity theft has occurred. What this means is that it is not a crime to assume the identity of another, however, it is unlawful to use that identity to commit a crime such as fraud or forgery.

A perpetrator can fraudulently steal a victim’s identity by obtaining his or her personal information such as their identity document, credit card details, payslip and/or their address, and use it to do the following:

1. to hide their own identity in order to escape criminal liability:
2. to get employed;
3. in order to apply for a social grant;
4. to purchase products and services on credit;
5. to apply for a loan; or
6. to open retail or bank accounts in the name of the victim.

Victims of identity theft may lose job opportunities, become blacklisted, have their good name tarnished, or even face the threat of being arrested for crimes that they did not commit.

**How perpetrators obtain personal information and how to protect personal information**

There are various ways that a perpetrator can use to obtain an individual's personal information. These range from simple methods, such as digging through trash in search of bank statements, to more sophisticated methods, such as hacking emails.

Considering the above, it is important for individuals to know how to protect themselves, such as:

1. Registering with the Southern African Fraud Prevention Services ("SAFPS") database: SAFPS provides a free online platform where individuals may either safeguard themselves against any potential fraud attempts by registering on the website or register a stolen or misplaced identity book/card or passport on the website using the following link: https://www.safps.org.za/Home/OurServices_ApplyProtectiveRegistration.
2. Shred or burn confidential documents such as bank statements.
3. Be mindful of the information shared on social media.
4. Individuals should check their credit score regularly: this is essential as it gives individuals the opportunity of checking whether credit applications were made in their name and could help prevent potential blacklisting if a fraudster has not made a payment.
5. Activate the SMS notification function on your bank account to inform you of any account activity.
6. Never allowing a browser or websites to save or remember login details.
7. By thinking before clicking. One should carefully consider the source of one's emails before simply reacting to an alarming email from an unknown source requesting personal information or asking the reader to "click here".
8. Carefully considering the source of any phone calls received, in terms of which personal information is requested. If you are unsure that the caller is from the institution from which they allege they are, rather ask if you can call back on the service provider's official line to complete the transaction.

It is important to note that registering on the SAFPS website is, ideally, meant to alert credit providers who are members of the SAFPS, should a fraudster use someone's personal details. However, it is advisable to follow up with the credit provider should a fraudster still manage to do so.

Once an individual’s personal information has been stolen, he or she should contact their nearest police station, report the matter to SAFPS, contact his or her bank and lodge a query with his or her creditors.

It is especially important for all individuals to protect their personal information as he or she might not be reimbursed by his or her bank if they have been found to have been negligent with this information. However, once an account holder has reported a case of fraud or a lost or stolen card to his/her bank, the bank can be responsible to cover losses from fraudulent transactions that occur thereafter. Thus, banks have a responsibility to help victims of fraud mitigate their losses, by taking the necessary steps to deactivate the card or account as the case may be. It should be noted that not all institutions have the same responsibility, as such, it is incredibly important for the individual to take the necessary precautions.

**Conclusion**

Consequently, the crimes that result from identity theft have a serious impact on the victims. Thus, everyone has a responsibility to protect their personal information by taking precautionary measures and by acting quickly once they realise that their personal information has been stolen.

**Value**

This article provides the layperson with a definition of identity theft as well as a brief breakdown of how individuals can protect their personal information and the steps to be taken if a perpetrator uses this information to defraud them.

**Schindlers Attorneys**