Fraud within the payment industry in South Africa

As the payment space evolves to keep up with the needs of citizens, there has been a marked uptick in the creation and use of digital solutions.

However, this presents new risks. As the way money is handled changes, so too do the methods criminals use. This white paper delves into payment fraud in South Africa, and what this means for the changing landscape of the country's payment industry.

OZOW

Contents

OZOW

Executive Summary

When the world was brought to a standstill in 2020, global economies saw a rapid acceleration and uptake of digital services.

The Covid-19 pandemic caused an explosion in eCommerce. A lockdown-fuelled online shopping boom lifted South Africa's eCommerce sales by 66% in 2020 to more than R30 billion, from reaching R14.1 billion in 2018[1]. It is also 50% higher than the total forecast for 2020, when online retail in South Africa was expected to reach R20 billion.

According to a report released by Deloitte, approximately 22 million consumers in South Africa shopped online in 2020[2]. More importantly, this number is expected to grow by 44% to 32 million users by 2024.

The payments industry has completely changed. Gone are the days when you had to write out a cheque or scramble for the right amount of cash to pay for something. The explosion of digital tech has provided consumers with faster and more convenient ways to pay.

Unfortunately, where the money flows, criminals follow.

[1] http://www.worldwideworx.com/online-retail-in-sa-2021/

[2] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/strategy/za-Digital-Commerce-Acceleration-2021-Digital.pdf

With the evolution of the payment's ecosystem, there has been an increase in malicious attempts by those trying to take advantage of the payment process to fraudulently benefit themselves. According to a global report published by Transunion[3], digital fraud attempts in financial services increased by a staggering 187% in the first four months of 2021, when compared to the same period in 2020.

This has been supported by the South African Banking Risk Information Centre (SABRIC), which saw a spike in digital banking fraud. It noted that, as customers turned to online shopping and settling payments in apps, criminals enhanced their efforts to phish customers to steal their personal data and defraud them on these platforms[4].

When it comes to digital payment fraud in 2021, there is a common misconception that the biggest threat to consumers is the use of third-party payment providers offering instant/automated EFT solutions.

However, recent stats released by SABRIC and data from some of South Africa's leading payment providers show that this isn't the case. In fact, the modus operandi for criminals to steal sensitive information has remained largely unchanged, with a strong focus on targeting traditional payment methods.

Regardless of the source of risk, traditional banking institutions, financial technology (fintech) companies and other third-party payment providers have been working to ensure their systems are protected against cyber-attacks. More importantly, their efforts are focused on guarding the sensitive information and data used by consumers and businesses during the payment process.

[3] https://newsroom.transunion.co.za/suspected-financial-services-digital-fraud-attempts-from-south-africa-rise-187-as-prevalence-of-digital-transactions-increase/

[4] As customers turned to online shopping and settling payments in apps, criminals enhanced their efforts to "phish" customers to steal their personal data to defraud them on digital and online platforms.

A change in payments

Technology is changing payments

Technology is transforming the world around us at an accelerated rate. The evolution is allowing people and economies to become more and more interconnected. In Africa, technology has been recognised as one of the most powerful drivers of growth – to revitalise industries, create employment, and bridge the divides between the rich and the poor.

Both the World Bank and the International Monetary Fund have indicated that technology will act as a catalyst for building the economies of developing nations. A central part of this includes reinventing the financial services sector to better serve the needs of the people.

Banks in South Africa currently hold R4.2 trillion in deposits, and process R110 trillion in payments annually. Financial inclusion in South Africa is high with 80% of adult South Africans holding a bank account in 2018. However, this inclusion is shallow, with almost 40% of these accounts underutilised.

More importantly, there is a serious need to improve banking and financial access for the 49 million bank account holders in South Africa, as well as the remaining 10.5 million who don't have one.

Traditional banking has typically relied heavily on scale and infrastructure build-out, including brick-and-mortar branches and ATM machines. The need for widespread branch infrastructure created extensive capital requirements.

Technology will act as a catalyst for building the economies of developing nations.

Developments in technology have meant that banks are increasingly able to enter new markets and territories and expand without physical infrastructure. This is particularly true since digitalisation has enabled “branchless banking” through internet and mobile banking, as well as through digital terminals. In South Africa, there have historically been instances of branchless retail banking by banks (typically targeting the affluent market) such as Investec or Sasfin.

Unfortunately, most banks’ lack of agility often prevents them from innovating quickly enough to meet the ever-changing needs of consumers.

This is where fintech companies are perfectly positioned to act as valuable allies of innovation. They can develop consumer-facing payment solutions to support these types of banking initiatives.

Rather than replacing what the banks offer, fintech solutions act as a support service to improve the uptake of banking in the digital age.

The International Finance Corporation (IFC) believes that mobile money solutions and open banking are essential. In a report[5], they stated that open banking can offer affordable, instant, and reliable transactions, savings, credit, and even insurance opportunities in rural villages and urban neighbourhoods where no bank had ever established a branch.

This is where the Covid-19 pandemic put a spotlight on the greater need to serve the underbanked and underserved in the country. This has become increasingly important with the rapid shift to a contactless ecosystem that is helping accelerate the de-cashing of the economy.

[5] https://www.ifc.org/wps/wcm/connect/067d6a0c-f1b5-4457-97aa-2982a7dfda69/EMCompass+Note+42+DFS+Challenges+updated.pdf?MOD=AJPERES&CVID=ITM-26u

The rise of eCommerce in SA

A lockdown-fuelled online shopping boom lifted South Africa's eCommerce sales by 66% in 2020 to more than R30 billion, according to a World Wide Worx research report published last month. This is thanks to consumers becoming more accustomed to buying goods and services online.

This surge saw online sales in South Africa more than double in two years to R30.2 billion. This is thanks to consumers becoming more accustomed to buying goods and services online, particularly after the country was put into lockdown.

"The most astonishing aspect of this total is that it is more than double the R14.1 billion reached in 2018, in just two years," said World Wide Worx MD Arthur Goldstuck, principal analyst on the research project, in a statement at the time.

The rise of eCommerce isn't slowing down. The increased usage of online retail platforms has transformed the way that people pay.

Online sales in South Africa more than double in two years to R30.2 billion.

Shifting payment behaviour

There has been a permanent change in the way that people shop and, in turn, the way that businesses have to operate. In the absence of brick-and-mortar stores being open during nationwide lockdowns, online and digital applications exploded.

Unlike developed nations, the majority of Africa's SME and informal economy has become heavily reliant on mobile payment solutions to drive growth and market penetration.

Over the last year, consumers have adapted to using digital, and importantly, contactless payment channels such as tap-to-pay, eCommerce and e-wallets.

In fact, mobile payments and digital wallets were two of the most popular payment types, eclipsing cash transactions globally in 2020[6].

Global research by Mastercard found that **88% of South Africans view contactless payment as a cleaner and safer way to pay.** This is supported by the increased usage of QR codes, e-wallets and other contactless payment options, like ApplePay, which has gained serious traction in the country over the last 12 months.

88% of South Africans view contactless payment as a cleaner and safer way to pay.

[6] https://www.paymentsdive.com/news/payment-trends-2021/597764/

The introduction of e-wallets and invisible payments, like those used by Uber and Amazon Go, are providing people with a way to pay for goods and services without having to take any action. Traditionally, these often required a credit card on file. However, this is being eliminated with the introduction of e-wallets and direct payment links to bank accounts through digital overlay services developed by fintechs.

The shift to a contactless ecosystem is also accelerating the de-cashing of the economy and has primarily been led through mobile.

The efforts to create a contactless and cashless society are helping drive financial inclusion and close the digital divides. Unfortunately, the shift has also meant that there has been an increase in fraudulent activity.

Payment Fraud

Understanding payment fraud

eCommerce forever changed the way people transact. There are so many benefits to the rise of online payment gateways. But alongside the good that digital transactions bring, there are some dangers as well. One of the biggest threats today is payment fraud.

Payment fraud is any type of false or illegal transaction completed by a criminal. The perpetrator deprives the victim of funds, personal property, interest, or sensitive information via the internet.

Payment fraud is any type of false or illegal transaction completed by a criminal.

The most common ways they do this is through phishing scams or by installing malware onto a victim's computer to steal personal information and banking details. Criminals will use data breaches or any alternative method to try steal consumers' information and identities.

These practices have been used extensively within the financial services sector by criminals to commit fraud. In 2020, 75% of companies around the world experienced some form of fraudulent scam or phishing attack on their systems.

Common types of fraud include

- **Phishing scams:** a type of fraud where someone's personal information is gained through emails or websites that act like legitimate sources.
- **Vishing scams:** the fraudulent practice of making phone calls or leaving voice messages claiming to be from reputable companies to encourage individuals to reveal personal information, such as bank details and credit card numbers.
- **Account takeovers:** this occurs when a thief gains access to someone else's online account to order goods or sell the account data elsewhere.
- **Credit card fraud:** this commonly known type of fraud refers to a transaction made with stolen payment information — someone else's credit card or other banking information.
- **Spoof websites:** a fake website that seems to show the correct URL in the browser window, but tricks users by using characters that closely resemble the legitimate domain name.
- **Social media fraud:** when attackers use social networking sites like Facebook, Twitter, and Instagram to obtain victims' sensitive data or lure them into clicking on malicious links.
- **Merchant identity fraud:** this involves criminals setting up a merchant account on behalf of a seemingly legitimate business and charging stolen credit cards.

Payment Fraud

Breaking down payment fraud in SA

Within the banking and payments sectors, fraud affects several payment services, the most notable being card fraud. But other payment methods are also being targeted, as criminals seek out new avenues to target unsuspecting consumers.

Card fraud

Card fraud can take place in a variety of ways, including counterfeit cards, card not present (CNP), lost cards, stolen cards and account takeovers, among others.

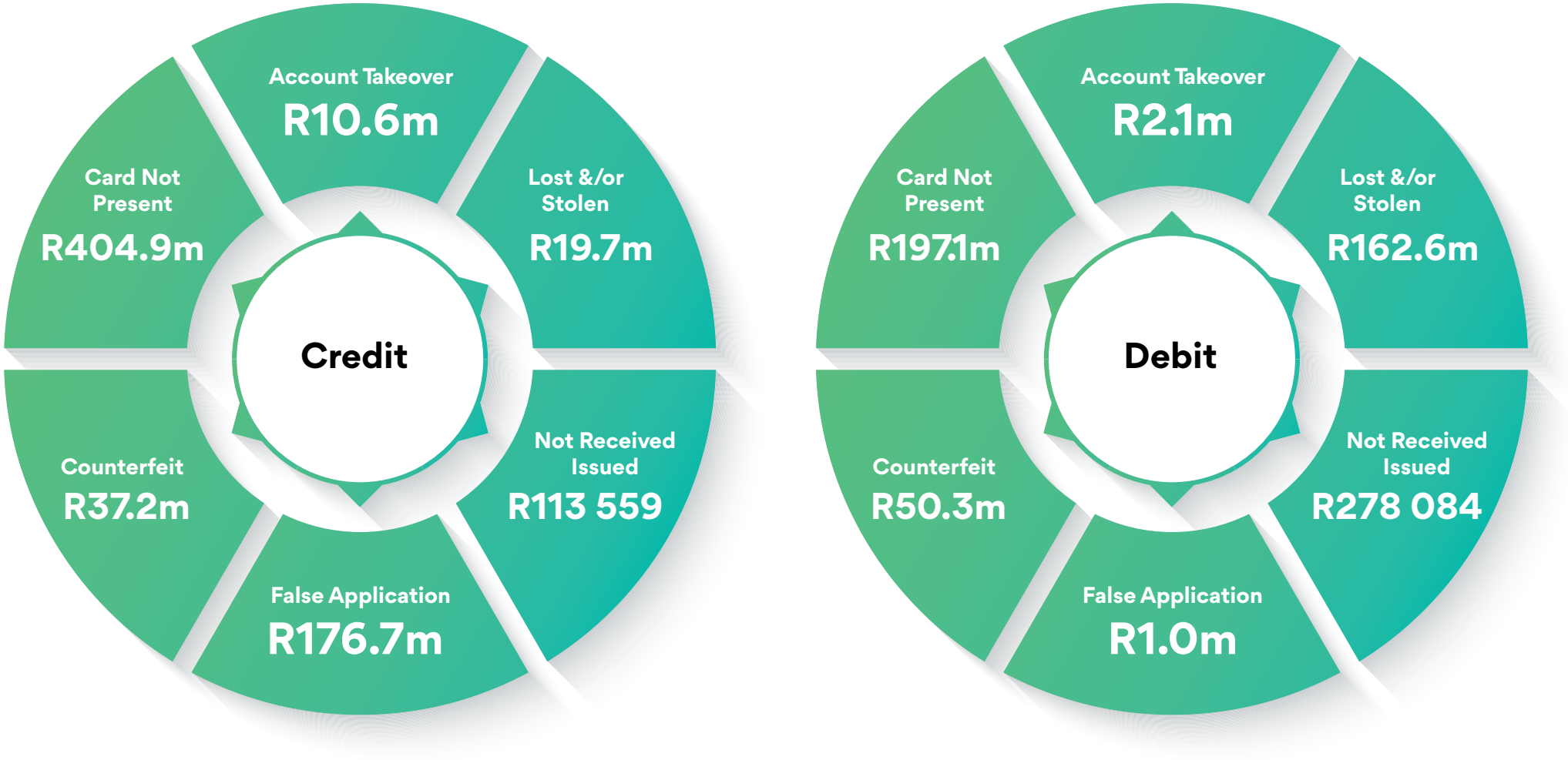
According to SABRIC, credit card fraud decreased by 27% from 2019 to 2020, whereas debit card fraud increased by 22% for the same period.

Financial uncertainty prompted people to use debit cards as opposed to buying on credit, as they were more comfortable spending money they already had. This, in conjunction with increased eCommerce activity, created more opportunities for criminals.

Credit card fraud down 27% from 2019 to 2020

Debit card fraud up 22% from 2019 to 2020

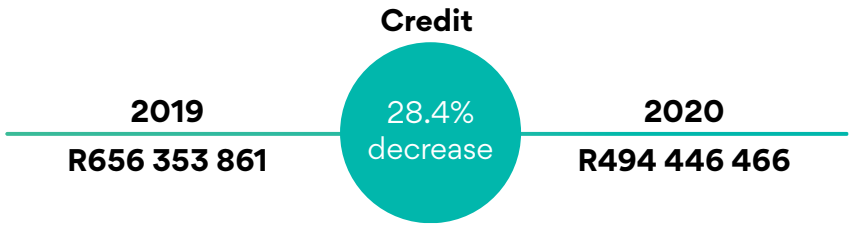
Fraud Value by Card Type

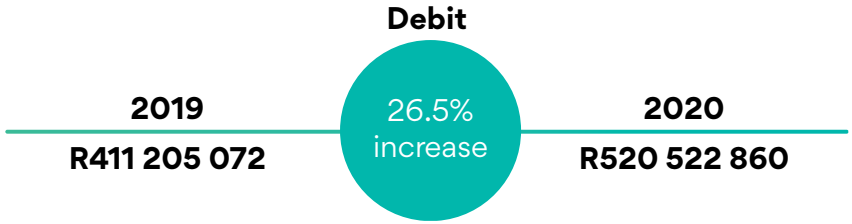


Annual Crime Statistics 2020, SABRIC

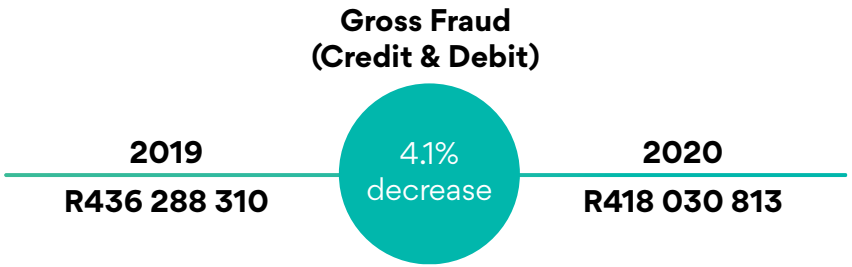
Debit and credit card fraud: SA issued cards

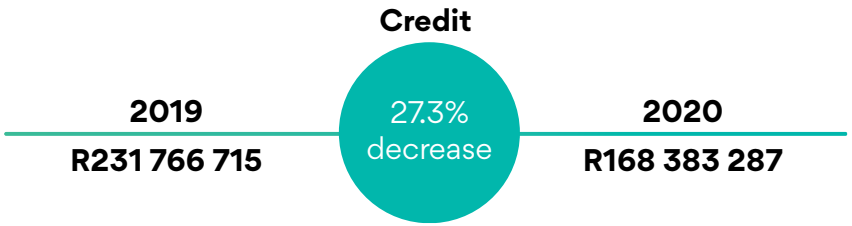
SA Debit & Credit Card Fraud Losses:

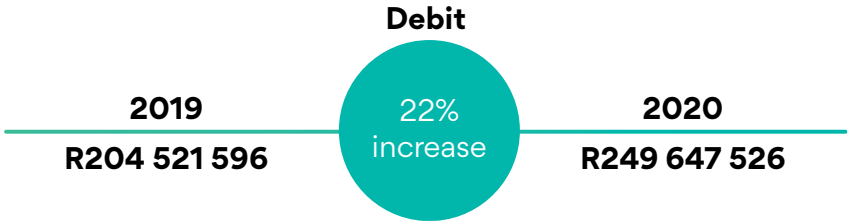




During the Covid-19 lockdown restrictions, consumer buyer behaviour shifted to online platforms. In addition, debit cards were enabled for online purchases, creating new opportunities for scammers to steal card information from bank customers. Reports received from the banking industry indicated increases in various phishing and OTP vishing scams where fraudsters used social engineering to obtain customer bank detail information.







Fraudsters were limited in their ability to harvest credit card details nationally and internationally as a result of travel restrictions due to Covid-19, for a number of months in 2020.

Annual Crime Statistics 2020, SABRIC

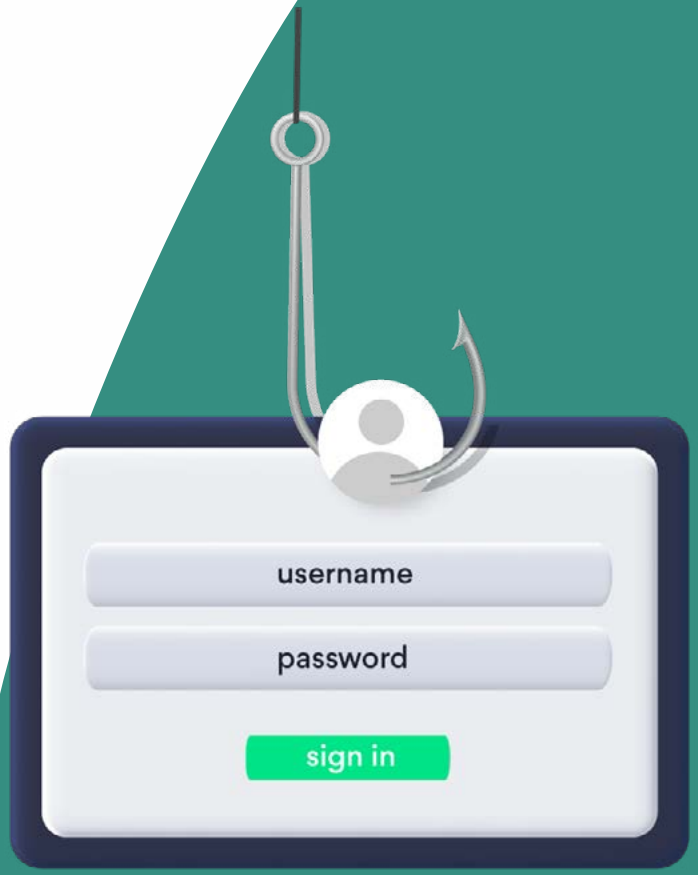
Digital Banking Fraud

Social engineering (phishing, vishing and smishing) continue to be the primary methods employed by criminals when targeting victims across the digital channels.

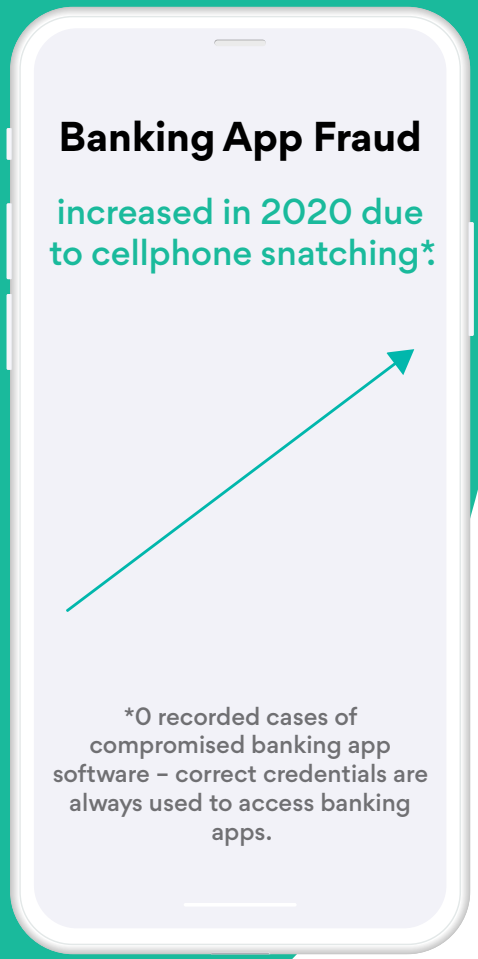
These methods can be used in combination with one another, or as one component within a broader scheme. Although the Covid-19 pandemic did not have a significant and direct, long-term effect on digital banking fraud reported to SABRIC[7], it did affect the landscape in various ways.

The large-scale move to remote working lead to unprecedented technical vulnerabilities related to network security and the uptake of online collaboration platforms. Social vulnerabilities resulting from fear and confusion caused by the pandemic and adjusting to lockdowns were also exploited by criminals.

The Covid-19 lockdown resulted in an increased uptake and use of the digital banking channels by the public as they were limited in their ability to visit a physical branch.



[7] Annual Crime Statistics 2020, SABRIC



Banking App

Despite the overall decrease in reported incidents on the channel, during 2020 a significant increase in banking app fraud as a result of cell phone snatching was recorded. It is important to note that there have been no reports where the banking app software was compromised to commit the fraud. Although there are various methods and techniques used in the cell phone snatching MO, the correct credentials are used to access the app.

These credentials may have been previously compromised through social engineering methods, such as shoulder surfing or phishing. However, in many cases, the credentials were exposed through vulnerabilities in the management of such information.

For example, the credentials were saved elsewhere on the device, or the same username and password were used across multiple apps.

An increase in the number of incidents involving SIM swops was reported in 2020 with 26.11% (2 684) as compared to 8% (855) in 2019.

2019: 855 Cases - 8% of Banking app fraud incidents

2020: 2684 cases - 26.11% of banking app fraud incidents

Mobile Banking

According to the digital banking crime incidents reported to SABRIC in 2020, mobile banking fraud accounted for 59.7% of digital crime incidents, but only 14.8% of the gross losses. Fraud on the mobile banking channel is characterised by a high volume of lower value transactions.

SIM swops were reported in 92.7% (19 537) of mobile banking fraud incidents reported in 2020 and is the most commonly used MO for committing crime on this channel. The increased ability of criminals to carry out SIM swops may account for the significant increase in incidents (67.6%) and gross losses (62.1%).

Known-party or “friendly” fraud was also a commonly reported MO on the mobile banking channel during 2020. In this type of fraud, an individual known to the victim (such as family member or colleague) and is in close proximity to them and/or their device, is able to access the device and conduct transactions without the victim’s knowledge.

The cash out method of this MO usually consists of purchasing airtime or electricity and instant cash sending facilities.

Online Banking

Online fraud makes up the smallest portion digital banking crime incidents, accounting for 11.1% of reported incidents. However, it accounts for the highest portion (45.1%) of gross losses. This may be indicative of multiple transactions occurring in one instance of fraud, as well as the higher value of the fraudulent transactions.

Social engineering, specifically phishing and vishing, remains the most common method of obtaining banking login credentials.

In some cases, vishing is used once the criminals have access to the victims account as an additional step to deceive the victim into providing the verification token (OTP or RVN) required to complete a transaction.

Covid-19 did not directly lead to a significantly higher number of social engineering attacks, as reported by the banking industry. However, the content used within these methods shifted drastically towards the virus, associated lockdowns, remote working, personal protective equipment, and vaccinations, to name a few. The shift in content and taking advantage of the vulnerabilities related to the unprecedented time may have led to higher success rates of such attacks.

Payment Gateways

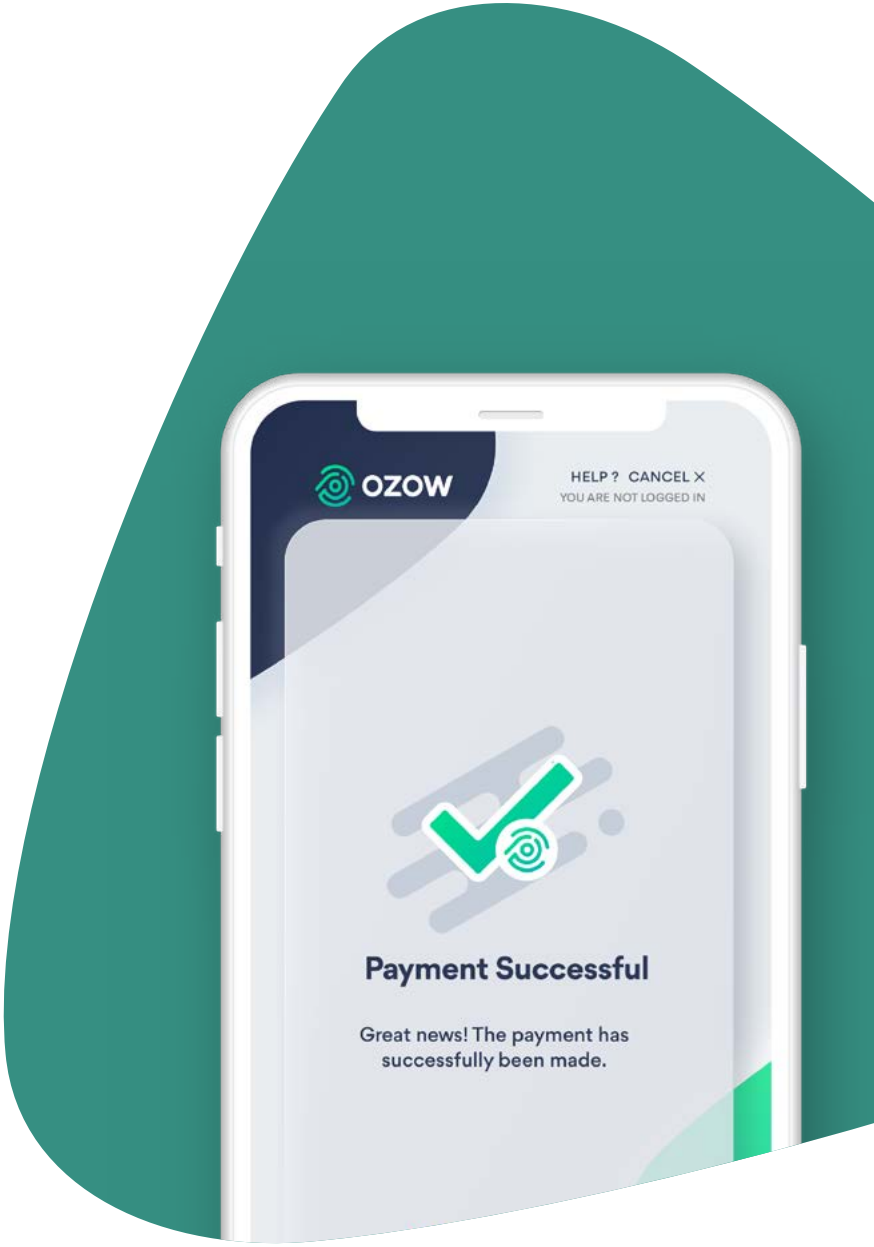
Digital overlays services, like screen scraping, collect screen display data or payment information from one application and translate it so that another application can display it. This is normally done to capture data from a legacy application and display the information using a more modern user interface.

This technology helps consumers access financial and payment solutions easily, conveniently, and quickly. Recognised and trusted third-party payment solution providers use digital overlay services on the existing and legacy South African payment system infrastructure.

Unfortunately, these ancillary payment services have been framed as unsafe and unsecure. However, payment solution providers using these services often have the lowest incidences of fraud via their payment systems.

As one of the leading payment solution providers in South Africa, Ozow has only experienced fraud on 0.02% of all transactions processed on a monthly basis.

Ozow has only experienced fraud on 0.02% of all transactions processed on a monthly basis.



Payment Fraud

Fraud types and the impact on industries

The changes in payment behaviour and the rise of fraud have affected various industries. Most notably, gambling and financial services have been ranked as the two sectors most impacted by fraud.

TransUnion analysed a range of industries for a change in the percentage of suspected digital fraud attempts against them, comparing the 2019/2020 period to 2020/2021.

Industry	Suspected fraud change coming from South Africa	Global suspected fraud change for industry	Type of fraud globally
Gambling	239.87%	54.81%	Policy/license agreement violations
Financial Services	114.68%	57.49%	Identity theft
Retail	86.32%	38.71%	Promotion abuse
Telecommunications	46.26%	57.52%	Credit card fraud
Logistics	30.63%	4.87%	Shipping fraud
Gaming	-4.96%	48.40%	Gold farming
Communities (online dating, forums etc.)	-15.71%	-11.10%	Profile misrepresentation
Travel & Leisure	-35.09%	26.68%	Credit card fraud

https://newsroom.transunion.co.za/one-year-after-covid-19-transunion-research-shows-digital-fraud-attempts-in-south-africa-have-increased-exponentially/

Payment Fraud

Challenging the narrative

One of the biggest challenges the payments sector faces, especially for those who operate within the open banking space, is unbalanced narratives that have been created around safety and security.

The practice is known as the illusory truth effect, which is the tendency to believe false information to be correct after repeated exposure. When truth is assessed, people rely on whether the information is in line with their understanding or if it feels familiar. Repetition makes statements easier to process relative to new, unrepeated statements, leading people to believe the repeated conclusion is more truthful.

This is exactly what is happening when it comes to the safety and security of fintech companies.

Banks have deliberately targeted third-party payment providers and payment gateways that use digital overlay/screen scraping solutions to create accessible payment products for the market.

This ultimately deters consumers and businesses from accessing and using alternative payment solutions. This, in turn, prevents greater financial inclusion in South Africa.

Mitigating Fraud

Reducing the risks

Banks and fintechs, like Ozow, need to counter the increase in fraud and ensure consumers and merchants are protected against cyber and data risks. To do this, they are continually implementing system security, data integrity, and business continuity processes.

To ensure consumers and merchants are protected, there has been an increase in processes and security by the banks to protect their clients against fraudulent and suspicious activity. This includes processes that trigger an alert for any suspicious activity, as well as data encryption, and Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA).

Recognised third-party payment providers and fintech companies comply with the highest safety and security measures to ensure customer data is protected. This includes:

- Performing regular reverse-image and unique phrase searches to identify any potential rogue website clones.
- Educating consumers about how to spot phishing sites, since web crawling can be insufficient as phishing sites aren't generally linked from public pages.
- Having a unique SLL certificate to identify the legitimacy of their pages and assure users that their data is encrypted and secure between themselves and the third-party payment providers.
- Securing access to platforms via VPN, strong password authentication, and 2FA/MFA.
- Segregating testing environments from production environments, reviewing any access to systems and components regularly, and logging and auditing actions by users.
- Implementing DMARC on their domains to detect, report and avoid email spoofing in the office environment.
- Using data theft protection solutions to detect and prevent confidential and personal information being leaked.
- Putting mobile device management solutions in place, enforcing encryption and providing remote wiping and monitoring capabilities.

Mitigating Fraud

The safety and security of fintech

Digital overlay services (also sometimes referred to as screen scraping) have undoubtedly delivered a valuable service to millions of consumers. This is especially true when acting as an alternative payment solution technology when an API with a bank is not available. For many, these services allow millions to transact in the formal banking sector for the first time, all while empowering them to be part of the Fourth Industrial Revolution by closing the digital divide.

Not only do fintech payment solutions help drive greater access compared to other payment methods, but they also provide a very low risk of fraud.

The prospective availability of these digital overlay service solutions to customers could rival cash as an attractive medium of exchange.

For consumers, this means being able to execute a payment instantly, at any time of the day with the confidence and knowledge that it has been safely received by the recipient[8].

Licensed systems operators and third-party payments providers with the Payment Association of South Africa (PASA) are deliberate about building safe and secure systems to protect their merchants and consumer bases.

Remaining compliant with all applicable laws is also important. This includes developing risk-based compliance plans to monitor and assess the effectiveness of the controls implemented to manage and mitigate the regulatory risks to the business.

[8] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/za-The-future-of-payments-in-South-Africa.pdf

These companies also abide by PCI-DSS Level 1 processes and security standards, and encrypt consumer, merchant, and transaction data end-to-end.

Companies like Ozow have also applied the relevant recommendations of King IV. This is to achieve good performance and effective control to ensure legitimacy and good ethical practices. Additionally, there is a strong focus in ensuring that they also comply with all applicable laws, including the Protection of Personal Information Act (POPIA), as amended from time to time.

Fintech companies will always opt to use Application Programming Interface (APIs) with the banks, where available. Currently, digital payment overlays are often used if the banks do not make any direct APIs publicly available. In some cases, both APIs and overlays will be used in conjunction, with overlays used as a backup to maintain its service should the APIs encounter any problems.

Improving access and usage

Driving financial inclusion

In a report published by the World Bank, it found that less than a quarter of adults in Africa have an account with a formal financial institution, and that many adults in Africa use informal methods to save and borrow. The study also found that most small, micro and medium-sized enterprises (SMMEs) in Africa are unbanked and access to finance is a major obstacle.

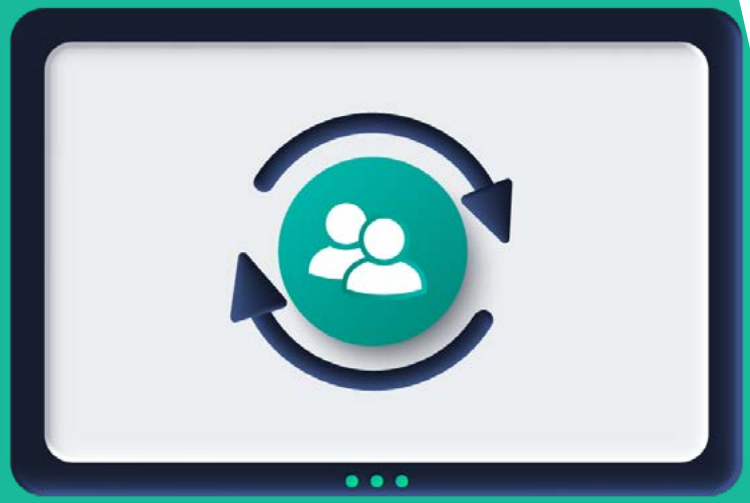
Compared with other developing economies, high-growth SMMEs and informal businesses in Africa are less likely to use formal financing, which suggests formal financial systems are not serving their needs. With more than 70% of the Sub-Saharan population employed in these sectors, the lack of financial access contributes to persistent income inequality and slower economic growth.

Addressing this challenge is imperative. One way of doing this is through open banking, which can act as the gateway to traditional banking systems for the more than 370 million unbanked adults in Sub-Saharan Africa.

Open banking allows third-party financial services companies to access users' banking data. The primary goal of open banking is to put power back into the hands of customers, enabling them to securely use third-party financial products and services that rely on banking data or functionality.

This can assist with online and mobile payment transactions, as well as to help aggregate data from multiple financial institutions, letting consumers analyse their spending and earnings, and budget better for the future.

More importantly, by leveraging off some of the latest digital technologies, coupled with enabling policies and regulations, open banking creates greater financial inclusion. This in turn acts as a catalyst for equitable development and inclusive economic growth, which is vital for Africa's growth.



Collaboration is vital

Understanding the unique challenges throughout the region, fintech companies continue to develop alternative payment solutions, such as payment gateways and mobile payment infrastructures for businesses. These help to drive greater financial inclusion and access in Africa.

Rather than replacing what the banks offer, fintech solutions act as a support service to improve the uptake of banking in the digital age. Banks are the experts in understanding risk management, while fintech has proven its worth in attracting new customers at scale.

Greater collaboration between the banks and fintech companies also help to foster an environment that allows the banks to broaden their reach, deepen their relationships with their customers and accelerate innovation.

Traditional banking systems can leverage the technological innovations that the fintech industry offers. This will enable them to transform their frameworks to be quicker, more malleable, and respond to the changing needs of consumers.

Seeing fintech companies as collaborators instead of competitors is ultimately a win-win situation – for the industry and for consumers.