SAFPS

SOUTHERN AFRICAN FRAUD PREVENTION SERVICE

2025 ANNUAL REPORT

COLLABORATIVE DATA-DRIVEN DEFENCE

The SAFPS is committed to protecting both businesses and consumers against the threat of fraud and financial crime.

CONTENTS

01

WHO WE ARE & OUR MANDATE

The Southern African Fraud Prevention Service (SAFPS) is a proudly South African not-for-profit organisation that was founded in 2001. The company is committed to combating fraud by providing: a shared database to Member organisations as a resource in fraud prevention, sharing fraud data and reporting, as well as access to a Member community that enables collaboration. The SAFPS is a registered credit bureau, fully funded by its Members spanning various sectors.

It also offers the South African public a means of protecting themselves against impersonation and identity theft through its services, including Protective Registration, victim fraud listings, and awareness initiatives. Yima, a product of the SAFPS, provides a scam prevention toolbox designed to empower consumers in the battle against fraud and scams. South Africans can report scams, scan websites to make sure they are safe, and expand their knowledge. All consumer services are free of charge.

OUR BUSINESS SERVICES

In collaboration with some of the largest and most trusted brands in South Africa, we combat fraud through delivering a centralised fraud-prevention function that spans various sectors.

The SAFPS maintains and provides an immensely powerful fraud database to assist our Members in detecting and preventing fraudulent activity.

OUR CONSUMER SERVICES

All South Africans have access to consumer products and services offered by the SAFPS at no cost. These include:

Fraud Victim Listings

The SAFPS provides victim support with our fraud victim listings on the SAFPS database. In the event of identity theft or impersonation, consumers can protect themselves from the associated financial implications. A Victim of Impersonation letter will be issued by the SAFPS that can be presented to organisations and credit providers in future to assist in the verification process.

Protective Registration

The SAFPS provides Protective Registration for all consumers who have experienced identity fraud, ID theft or have had their identity compromised, to prevent future fraud. Anyone can proactively register to protect themselves and add an extra layer of protection and peace of mind.

It is a FREE service that consumers can apply for, and it enables the SAFPS to alert its Members to take additional care when dealing with that individual's details.

Yima - Scam Prevention Toolbox

Yima, a product of the SAFPS, is a dedicated platform designed to empower consumers in the battle against fraud and scams. The Yima website hosts a scam prevention toolbox for South Africans to report scams and scan websites to make sure they are safe.

Users can also access a scam hotline to report an incident directly to their banks, retailers, insurance companies and the South African Police Service via a single number.

Additionally, consumers can expand their knowledge of how to identify a scam through useful articles and tips.

YIMA
Stop. Think. Don't get scammed!

02

OUR MISSION, VISION AND VALUES

Our Mission

- To protect both consumers and businesses against the threat of fraud and financial crime.
- To protect Southern Africa against the negative impacts of fraud and financial crime.
- To educate consumers, businesses, and markets on the most effective fraud prevention techniques and solutions.
- To actively collaborate with our Members and other stakeholders in the fight against fraud and financial crime.

Our Vision

To be a front runner in the fight against fraud by harnessing the power of collaboration and uniting the public sector, private sector, and consumers in the fight to combat financial crime.

The SAFPS is passionate about providing fraud prevention awareness relating to identity theft and impersonation, by publishing relevant and current information via multiple channels including social media.

Since 2001 we have prevented billions of rand worth of fraud losses within the South African economy for both our members and consumers at large.

Our Values

Commitment

The SAFPS is committed to providing effective and efficient service to consumers, our Members and other stakeholders through the application of leading practice principles in fraud prevention.

Continuous Improvement

Through drawing on trusted international and local sources, we maintain up-to-date awareness of the latest trends in fraud prevention, keep pace with industry-leading standards, and ensure that our methods reflect current technology in information transfer and systems.

Integrity

We deliver our services with integrity, always ensuring ethical conduct.

Communication

We aim to communicate effectively with all our stakeholders.

Dignity & Respect for the Community

We believe in treating everyone fairly, consistently, sensitively, honestly and with respect for their individual rights in compliance with all regulation and legislation.

Transparency

We accept accountability for our actions and decisions, and always act with honesty and openness.

03

CHAIRPERSON'S MESSAGE

CHRISTO OTTO

Fraud Is Evolving.

Data-Driven Defence Makes The Difference.

Fraud poses an enormous threat to the South African economy as it siphons billions of rands from organisations, the state, and the public. It erodes trust, diverts resources, and constrains economic growth as it continues to become more targeted, more organised and more complex.

The impact is significant, which means our work is never done. A collaborative, data-driven approach equips organisations with the intelligence needed to detect, prevent, and respond to financial crime - helping safeguard South Africa's economic future.

AI-enabled fraud and digital crime are escalating worldwide, and particularly in South Africa, as criminals use advanced technologies to make their attacks more sophisticated, scalable, and convincing. This trend is driven by a combination of economic hardship, widespread data breaches, and the growing accessibility of technologies such as generative AI, which enable cybercriminals to automate scams, create highly convincing fake content, and refine their methods with greater speed and precision.

Fraudsters target both organisations and consumers through increasingly sophisticated schemes that combine multiple techniques, channels, and platforms. This blended approach makes fraud harder to detect, more difficult to prevent, and increasingly challenging to respond to effectively.

Now more than ever, consumers feel vulnerable. It is increasingly difficult to know what, and who, to trust. As a fraud-fighting community, we have a shared responsibility to stand together, strengthen trust, and do everything we can to prevent fraud. It is an ambitious goal, but one we cannot afford to lose sight of. By remaining focused on our mission and working collaboratively, we can help protect consumers, strengthen organisations, and build a more trusted and resilient society.

The foundation of our work is the sharing of confirmed fraud data. Our Members play a vital role by following the appropriate due process and submitting verified fraud information to the shared SAFPS database. This trusted data enables our Member community to detect and prevent fraud more effectively while helping to protect consumers.

> **Thank you to the SAFPS Board for their ongoing commitment to fraud prevention. The collective knowledge and experience in the room enables the SAFPS to deliver superior service to its Members.**

I would like to extend my sincere thanks to our Members for their ongoing commitment to keeping the database accurate, current, and comprehensive. Every confirmed listing that is shared strengthens our collective ability to combat fraud. The more we share, the stronger our community becomes. I also encourage our Members to maintain this momentum, continue prioritising data sharing, and explore new and innovative ways to enhance the excellent work already being done. Together, through collaboration and shared intelligence, we can stay ahead of evolving fraud threats and deliver even greater value to the organisations and communities we serve.

Thank you to Manie Van Schalkwyk, his management team, and all the SAFPS employees for yet another wonderful year. It is their unyielding commitment to doing what is right that makes the SAFPS a long-standing, trusted partner in fraud prevention. I would also like to thank my fellow SAFPS Board members, all our SAFPS Members, key stakeholders, and industry partners for the ongoing support.

It remains my privilege to be a part of the SAFPS Board and to continue working with people who are passionate about making a real difference. The organisation may be small, but its impact is significant. This is reflected in the results, insights, and feedback shared throughout this report.

I would like to close with a message of hope. While the challenge before us is immense and constantly evolving, our collective efforts are making a meaningful difference. By remaining committed to collaboration, innovation, and our shared purpose, we will continue to strengthen our defences, protect consumers, and build a more trusted future.

Sincerely,

Christo Otto
Chairperson
Southern African Fraud Prevention Service (SAFPS)

04

CEO'S MESSAGE

MANIE VAN SCHALKWYK

Building Trust Through Collective Action

As we reflect on the past year, I am reminded that fraud remains one of the most significant threats to economic growth, financial inclusion, and consumer confidence in Southern Africa. Criminals continue to adapt their methods, exploiting new technologies and vulnerabilities with increasing sophistication. Yet, despite these challenges, the Southern African Fraud Prevention Service (SAFPS) remains steadfast in its mission to protect businesses and consumers through collaboration, intelligence sharing, and proactive fraud prevention.

This past year has once again demonstrated the power of collective action. Our Members continue to place their trust in the SAFPS as the custodian of shared fraud intelligence, enabling organisations across multiple sectors to identify and prevent fraud before losses occur. Every successful intervention represents not only a financial saving but also the protection of an individual's identity, reputation, and future opportunities.

The fight against fraud cannot be won by any single organisation acting alone. The strength of the SAFPS lies in our unique model of industry collaboration, where competitors become partners in protecting the integrity of the broader economic system. Through the sharing of confirmed fraud information, our Members contribute to a safer environment for consumers and businesses alike.

Over the past year, we have continued to enhance our systems, strengthen our partnerships, and improve the value we deliver to our Members. We have invested in technology, expanded stakeholder engagement, and increased awareness of the growing threat posed by fraud and scams. These efforts have further reinforced the SAFPS's position as a trusted leader in fraud prevention and it is visible in some of the following statistics.

IN 2025:

- The fraud database increased by 19%.
- The SAFPS saved our Members over R7 billion.
- The number of enquiries into the fraud database increased by 63% and totalled 131 million enquiries.
- The SAFPS Contact Centre handled over 68 066 calls and over 55 645 emails.
- The SAFPS Interactive Voice Response Self-Service (IVR), which is available 24/7, received 20 253 requests for letter re-issues from consumers.

IT ENABLEMENT & SECURITY

As custodians of sensitive consumer fraud data, our IT environment plays a critical role in enabling secure, efficient, and scalable services for our Members. We continue to invest in modern technologies, resilient infrastructure, and robust security controls to ensure that our systems are both high-performing and protected against evolving threats.

In 2025, our systems achieved an average response time of 250 milliseconds, while successfully processing 79 million of the total enquiries (131 million) through the API - demonstrating both the reliability and scalability of our infrastructure.

Skills: We have in-house expertise across various disciplines required to manage and maintain a secure and stable fraud data platform. As Member demand for our products and services continues to grow, we are expanding our technical capability to meet these evolving needs. Where specialised expertise is required, we also leverage long-standing partnerships with trusted external service providers to support skills development and ensure we continue to deliver a robust, secure, and future-ready platform.

System Availability and Reliability: Our Members rely on SAFPS systems every day to make timely, informed decisions in the fight against fraud. Maintaining a secure, resilient, and highly available platform is therefore a strategic priority.

Throughout the year, we remained focused on maximising system uptime, strengthening infrastructure resilience, and continuously improving the availability of our services. We also maintained robust disaster recovery capabilities to ensure business continuity and minimise operational risk in the event of an unforeseen disruption.

Cybersecurity: Protecting the integrity, confidentiality, and availability of our systems and data remains a top priority. We continuously strengthen our cybersecurity posture to safeguard our Members, and the data entrusted to us.

Our security programme includes continuous security monitoring, regular penetration testing, and proactive vulnerability management to identify and address potential risks before they can be exploited. We also invest in our people through ongoing cybersecurity awareness training, delivered by an independent specialist provider, ensuring that security remains a shared responsibility across the organisation.

Throughout the year, our security controls detected and blocked numerous unauthorised access attempts and other malicious activities originating from across the globe. While these threats are constant, our layered security approach, proactive monitoring, and rapid response capabilities helped protect our platform and maintain the integrity and availability of our services. We recorded thousands of attempts on a weekly basis, with **no successful breaches or access gained** during the reporting period. Most attempts originated from Russia and the United States, but we did note some more activity from Japan, South Korea and China.

Protection of Personal Information: We take the protection of personal information extremely seriously and remain fully committed to compliance with the Protection of Personal Information Act (POPIA). Safeguarding data privacy is embedded in our operational processes and governance frameworks.

Our approach is underpinned by strong data governance principles, robust access controls, and industry-standard encryption to ensure that sensitive information is protected at all stages of its lifecycle. Comprehensive audit trails provide transparency and accountability, while continuous privacy enhancements ensure that our controls evolve in line with emerging risks and regulatory expectations.

Member Service Improvements: In parallel with our security and compliance commitments, we continue to focus on improving Member experience. This includes faster processing and response times, enhanced user interfaces, and ongoing system optimisation to reduce downtime.

OUR PEOPLE

Our ability to deliver on our mission depends not only on strong systems and processes, but also on the culture of the organisation and the capability of our people. We continue to invest in developing the skills, expertise, and leadership capacity required to respond to an increasingly complex fraud and technology landscape.

In 2025, great strides were made in terms of our talent management strategy and governance, as well as employee engagement and wellbeing. This foundation will allow us to grow from strength to strength and ensure we remain well positioned to support our Members and consumers, while also creating a working environment that supports the growth and development of our people.

PREVENTING FRAUD THROUGH SHARED INTELLIGENCE – OUR NEW TAGLINE

In the same way that fraudsters deliberately target organisations and consumers, we need to be mindful and strategic in our efforts to frustrate their attempts. By working with our Members, strategic partners and regulators, we can extend our reach and amplify our impact. Adopting a data-driven approach proactively mitigates fraud risks and makes the financial landscape much less hospitable for fraudsters.

This approach is reflected in our new tagline,

"Preventing fraud through shared intelligence."

Many minds, one mission: united against fraud.

THANK YOU AND LOOKING AHEAD

I am particularly proud of the dedication and professionalism demonstrated by the SAFPS team. Their commitment to excellence, innovation, and service has enabled us to respond effectively to emerging threats while maintaining the highest standards of governance and operational integrity.

Our achievements would not have been possible without the continued support of our Members, Board of Directors, strategic partners, regulators, and industry associations. Your commitment to collaboration strengthens our collective ability to protect consumers and safeguard the integrity of our financial system.

Looking ahead, the fraud landscape will continue to evolve. Advances in artificial intelligence, digital identity technologies, and increasingly organised criminal networks present both opportunities and challenges. The SAFPS is committed to remaining at the forefront of these developments, ensuring that our Members have access to the intelligence, tools, and partnerships necessary to combat fraud effectively.

As we move forward, our focus remains clear: to strengthen collaboration, enhance fraud prevention capabilities, protect consumers, and contribute to a more secure and trusted economic environment throughout Southern Africa.

Together, we are making fraud more difficult, more costly, and less rewarding for criminals. Together, we are building a safer future.

Sincerely,

Manie van Schalkwyk
Chief Executive Officer
Southern African Fraud Prevention Service (SAFPS)

> **Thank you to our valued Members for the ongoing support. Through collaboration we are making a real difference.**

05

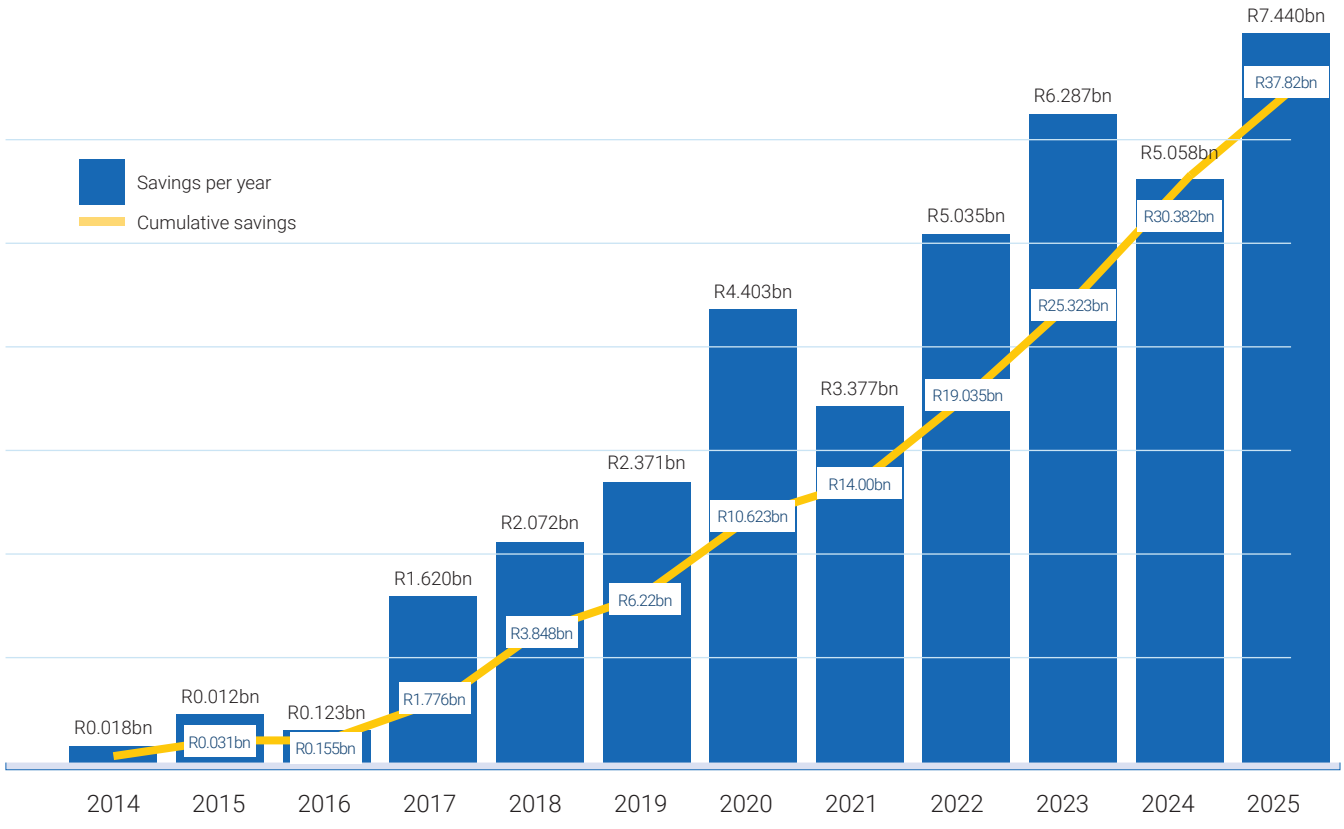
OUR VALUE ADD

SAVINGS

Due to fraud interventions, the SAFPS is saving our Members' money.

TOTAL SAVINGS IN 2025
R7.44 BN

INCREASE FROM 2024
47%



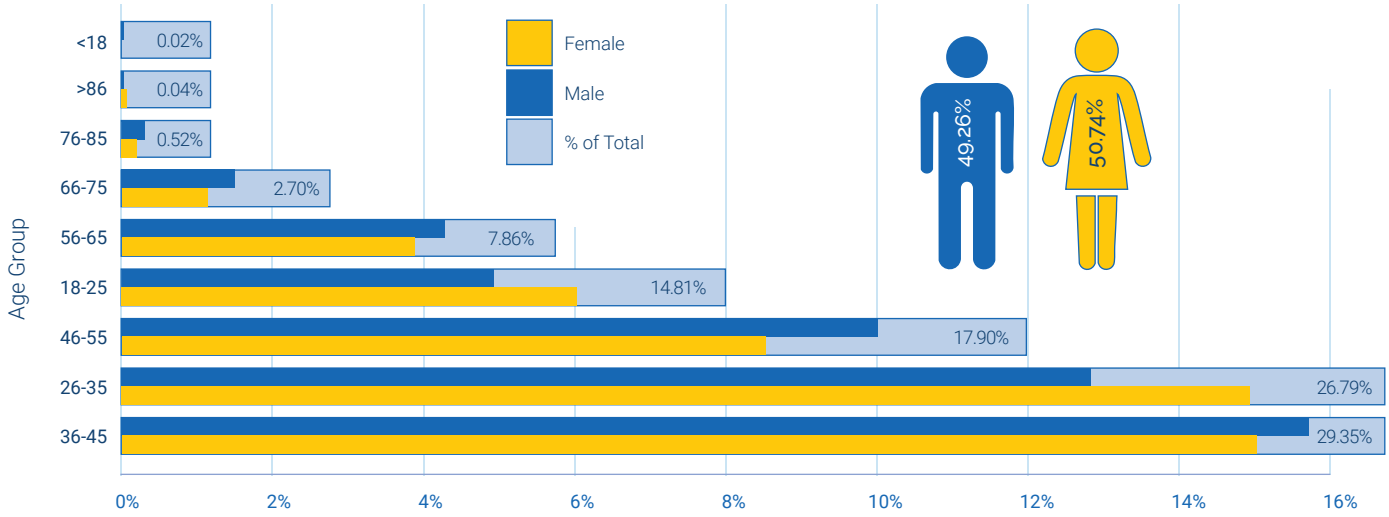
88%
of individuals who have Protective Registration are between the ages of 18 and 55.

36-45
is the top age category.

PROTECTIVE REGISTRATIONS

Due to the risks South Africans face, more and more people are turning towards the SAFPS's Protective Registration to give them an additional layer of protection on their identity. This is one of our most essential consumer services and is core to our offering.

DEMOGRAPHIC OF INDIVIDUALS WHO APPLIED FOR PROTECTIVE REGISTRATION IN 2025



06

2025 STATISTICS

OVERVIEW:

We have outlined key insights from the 2025 SAFPS statistics.

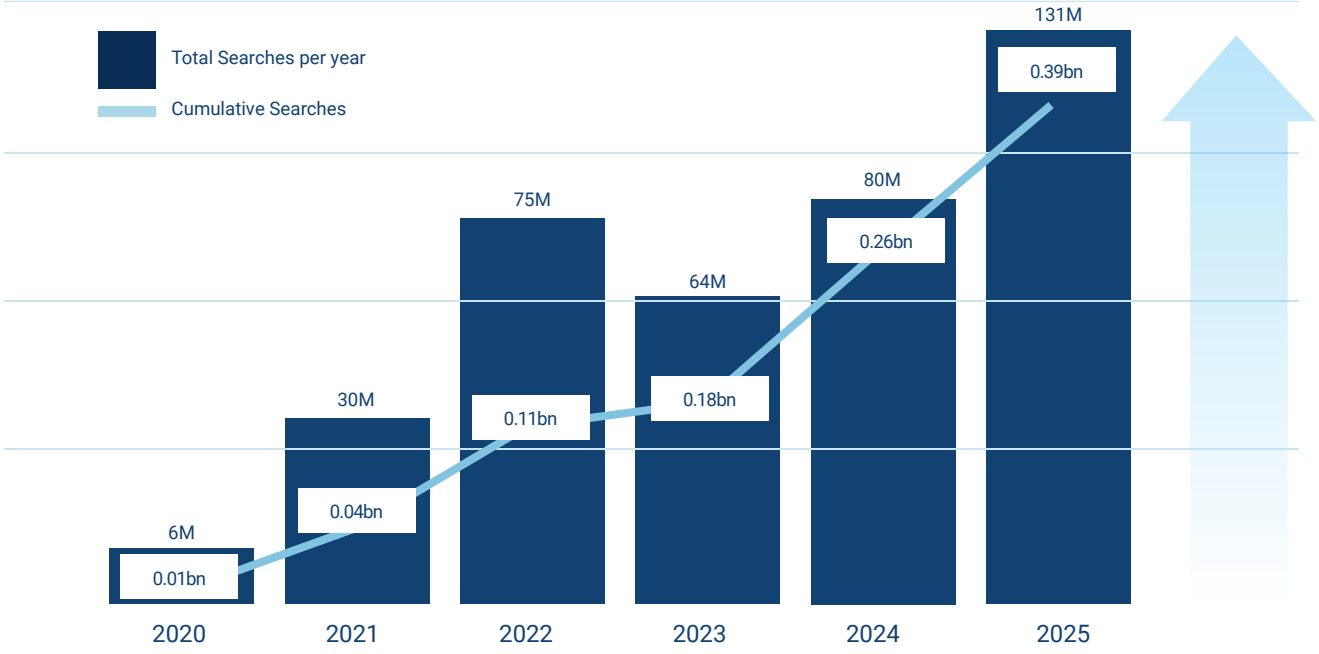
TOTAL ACTIVE FRAUD LISTINGS	TOTAL ACTIVE VICTIM LISTINGS	TOTAL ACTIVE PROTECTIVE REGISTRATIONS
INCREASED BY 19%	INCREASED BY 8%	INCREASED BY 5%

*Compared to the previous 12-month period (January 2024 to December 2024)

TOTAL SEARCHES:

In 2025, **131 million** searches were done by SAFPS Members, which is a **63%** increase when compared to 2024.

TOTAL SEARCHES: 2020 -2025



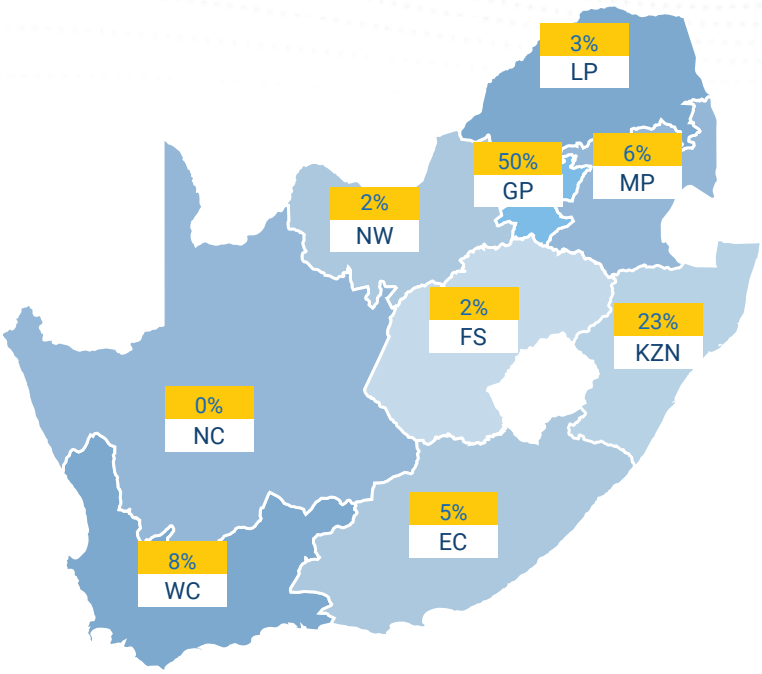
A CLOSER LOOK AT FRAUD INCIDENTS

Let us look at how fraud was perpetrated in 2025 based on the listings loaded to the SAFPS database by its Members.

FRAUD ANALYSIS PER REGION

Focusing on the fraud incidents per region, the Gauteng, KwaZulu-Natal and the Western Cape provinces remain the main centres for fraudulent activity.

PROVINCE	YTD % OF TOTAL
Gauteng	50%
Kwazulu-Natal	23%
Western Cape	8%
Mpumalanga	6%
Eastern Cape	5%
Limpopo	3%
North West	2%
Free State	2%
Northern Cape	0%
Total	**100%**



DOMINANT MODUS OPERANDI AND CRITICAL PATTERNS

LOOKING AT HOW FRAUD WAS PERPETRATED DURING 2025

Document fabrication and vishing scams constitute the predominant fraud mechanisms observed across the portfolio.

Document fabrication is the dominant enabler across insurance, funeral claims, and fraudulent document categories, manifesting as forged death certificates, falsified medical certifications, fabricated payslips, altered ID documents, and forged bank statements.

Vishing (voice phishing or phone-based scams) emerges as the leading attack vector within digital channels, accounting for 21.5% of money mule cases and 12.9% of digital fraud cases. Fraudsters use sophisticated social engineering techniques to deceive legitimate customers into disclosing one-time PINs (OTPs), banking credentials, and other sensitive information.

These two mechanisms converge in a dangerous pattern: vishing attacks compromise legitimate customers, whose accounts are used as mule accounts to receive and distribute the proceeds of other fraudulent activities.

Credential and qualification fraud is highly specialised, with 98.5% of employment fraud cases involving falsified academic qualifications. Organised professional collusion appears consistently; broker syndicates in insurance fraud, collusion involving medical practitioners and undertakers in funeral claims, and organised document fraud networks, particularly permanent residence and refugee fraud syndicates.

The systematic use of mule account networks across at least three major fraud categories indicates the existence of a coordinated money laundering ecosystem, in which mule accounts serve as the conduit for receiving and distributing illicit or stolen funds.

A significant number of mule-related cases across money mule, account misuse, and digital fraud categories show a consistent pattern: perpetrators use vishing or account takeover techniques to compromise legitimate customer accounts, before rapidly transferring or withdrawing the funds through pre-positioned mule accounts. These mule accounts are typically opened approximately one month before receiving the proceeds and are emptied within hours of the funds being deposited, significantly reducing detection and recovery.

Note on geographic insights. *The provincial findings presented in this report are based on the subset of fraud incidents for which geographic location information was available and recorded. Accordingly, provincial volumes and rankings should be interpreted as indicative of where reporting is concentrated, rather than a definitive measure or representation of the true geographic distribution of fraud.*

THE USE OF FRAUDULENT DOCUMENTS IS A SIGNIFICANT AND PERSISTENT CHALLENGE IN SOUTH AFRICA

Fraudulent documents constituted a significant proportion of the fraudulent activity reported to the SAFPS. This highlights the widespread use of falsified or altered documentation as a key enabler to various types of fraud.

These are not only used to impersonate legitimate consumers, but in many instances, consumers themselves are making use of fraudulent documents to obtain credit facilities or products and services with SAFPS Member organisations.

Document forgery was the most frequently recorded fraud type in the dataset and was geographically concentrated in Gauteng, which accounted for 37.7% of all reported fraudulent document listings. Absolute volume, however, is not the same as prevalence. When measured as a share of each province's recorded fraud, Mpumalanga exhibited the highest concentration, with approximately one in three (33%) of all fraud recorded involving a forged document. This indicates that, despite recording fewer cases overall, document forgery constitutes a disproportionately dominant fraud method within the province.

Although the **financial sector is the biggest target** for this type of fraud, the SAFPS data shows that the **clothing retail sector was the second most targeted sector** during 2025.

Top four contributors:

- Impersonation because of an altered ID document (34%)
- Fraudulent bank statements (33%)
- Multiple fraudulent documents (17%)
- Fraudulent payslips (11%)

IDENTITY THEFT FACILITATED THROUGH THE USE OF ALTERED OR FRAUDULENT IDENTITY DOCUMENTS

Criminals use altered or fraudulent identity documents to impersonate legitimate or deceased individuals, enabling them to open accounts and apply for credit fraudulently. The sector largely impacted by this was the clothing retail sector.

KEY FINDINGS:

- Identity theft via an altered ID document made up the bulk of these listings, accounting for 53%.
- Beyond forged and altered documents, identity misuse was also heavily concentrated in Gauteng. The province accounted for 48.6% of identity misuse listings and recorded the highest concentration among the major economies, with approximately 11% of the province's recorded fraud involving identity misuse. Identity misuse was therefore predominantly a Gauteng phenomenon, followed by the Eastern Cape (24.9%), KwaZulu-Natal (8.3%) and Mpumalanga (6.1%).
- Permanent residence/refugee fraud accounted for 19% of these listings. This is where applicants with permanent residence status or refugee documentation present additional fabricated documents.
- Deceased individual impersonation fraud, which is where the perpetrator applies for credit claiming to be a deceased person or includes a fraudulent Letter of Executorship to access estate funds, accounted for 21% of these listings.
- Vehicle finance application fraud accounted for 8.8%.

BANK STATEMENTS ARE THE MOST FREQUENTLY FORGED SUPPORTING DOCUMENTS

Fabricated statements are used to demonstrate false income, assets, or business performance. This includes falsified transaction records with inflated balances and statements created to show false income sources or business turnover. It is also combined with forged ID documents and payslips for multi-document fraud schemes. The sector largely impacted by this was the banking sector, with 60% of the listings reported by them.

KEY FINDINGS:

- This type of fraud is often linked to vehicle finance and credit card applications.
- Bank statement fraud is a specific form of document forgery and was most prevalent in KwaZulu-Natal, which accounted for 33.8% of all reported listings. However, the pattern differs when viewed in relative terms. Measured as a share of each province's recorded fraud, the Free State exhibited the highest local concentration, with approximately 10% of the fraud recorded involving bank statement manipulation.

SUBMITTING MULTIPLE FRAUDULENT DOCUMENTS

In cases involving multiple fraudulent documents, criminals submit complete sets of supporting documentation to create the appearance of legitimacy.

This includes forged payslips and bank statements submitted together, false power of attorney documents for fraudulent fund access or property transfers, fraudulent confirmation of drawings from non-existent businesses, forged letters of earnings combined with fake financials for business loans, false financial statements, balance sheets, and management accounts from shell companies, as well as fraudulent executor documents targeting estate funds and investments.

KEY FINDINGS:

- Coordinated payslip and bank statement fraud accounted for 51.5% of these listings. By submitting these together, it creates the appearance of financial stability.
- 24.8% of these listings were in relation to vehicle finance and 11.3% in relation to personal loans.

FRAUDULENT PAYSLIPS USED TO MISREPRESENT INCOME AND EMPLOYMENT

Forged payslips are primarily used to substantiate employment and income in applications for vehicle finance and home loans. Criminals frequently target recognised employers by replicating their documentation or fabricate entirely fictitious companies.

This includes self-generated or fabricated payslips exhibiting alignment, spacing, and formatting irregularities detectable through forensic analysis; fictitious employer entities registered at residential rather than business addresses; fraudulent employment confirmation letters containing fabricated company logos and contact details; salary increase confirmation letters dated prior to the commencement of employment; and instances of collusion with dishonest company employees to validate fraudulent employment and income information.

KEY FINDINGS:

- Majority of these listings are linked to employment verification (47.1%) and vehicle finance (45.6%).
- Vehicle finance was the dominant target of fraudsters in terms of fraudulent documents, as this makes up 20 - 46% of these listings.
- Fraudulent payslips were most frequently reported in Gauteng, which accounted for 35.4% of all recorded payslip fraud listings. However, the pattern changes when assessed in relative terms. Measured as a share of each province's recorded fraud, the Free State exhibited the highest local concentration, with approximately 21% of fraud listings involving fraudulent payslips. This notably high proportion suggests that income document fabrication is a particularly prominent fraud method within the province, despite its lower absolute number of cases.

MISUSE OF ACCOUNTS THROUGH MONEY MULE ACTIVITY

Money mule schemes involve the use of bank accounts to receive stolen or fraudulently obtained funds and transfer them to other accounts, often located overseas.

These schemes serve two primary purposes:

1. **Layering**: Conceals the criminal origin of funds by moving money through multiple accounts and transactions, making it more difficult for authorities to trace.
2. **Identity distancing:** Allows criminals to avoid handling the stolen funds directly, reducing their risk of detection and prosecution.

TYPES OF MONEY MULES

Willing mules - Individuals who knowingly allow their bank accounts to be used to receive and transfer illicit funds, typically in exchange for financial gain, a commission, or a share of the proceeds.

Unwitting (victim) mules - Individuals whose accounts are misused without their knowledge or consent. Their accounts may be compromised through scams, hacking, or other forms of unauthorised access.

Account takeover - Occurs when a criminal obtains a legitimate account holder's credentials and gains unauthorised access to the account, using it to receive and transfer fraudulent proceeds.

Money mule accounts are a key component of organised fraud networks, enabling criminals to move illicit funds while distancing themselves from the underlying criminal activity. These networks often exploit both willing participants and unsuspecting victims.

KEY FINDINGS:

- Vishing (voice phishing or phone-based scams) was the leading fraud method associated with mule accounts, accounting for 21.5% of reported listings. Its prevalence is largely driven by scalability, as a single fraudster can use social engineering techniques over the phone to deceive multiple victims and gain unauthorised access to their accounts within a matter of hours.
- Money mule activity was heavily concentrated in two of South Africa's largest economic hubs, Gauteng and KwaZulu-Natal, which together, accounted for 70.9% of all reported money mule activity listings. Gauteng also recorded the highest local concentration, with approximately 11% of the province's fraud involving money mule accounts. Vishing displayed a similar geographic pattern, with Gauteng accounting for 51.8% of all identified vishing listings.
- These two methods were closely linked operationally in terms of the fraud chain. Approximately 70% of vishing incidents also involved a money mule account - indicating that vishing typically served as the social engineering mechanism used to deceive victims, while the money mule account facilitated the movement and withdrawal of funds.

TRANSACTION PATTERNS

Pattern	% of Total	Interpretation
Single Transaction Mule Accounts	34.5%	The account is opened specifically for one fraudulent deposit, then abandoned/closed.
High Value Transfers	2.9%	R30k - R170k+ per transaction; indicating coordinated organised fraud.
Multiple Transaction Accounts	2.2%	The account is reused for 2 - 10+ fraudulent transfers, indicating higher sophistication.
Rapid Turnover	1.0%	Funds are deposited and immediately transferred out; the mule account is used as a pass-through mechanism.
Account Withdrawn (Physical Cash)	1.9%	Funds are withdrawn via ATM/ branch, indicating coordinated cash pickup operation.
Funds Transferred to Other Accounts	1.3%	Second-layer transfer; obfuscates the money trail.

MISREPRESENTATION OF INFORMATION DURING THE EMPLOYMENT APPLICATION PROCESS

Unlike organised money mule schemes or coordinated document fraud, employment fraud is typically driven by individual opportunism rather than organised criminal networks. Perpetrators generally act independently, exploiting recruitment processes, falsifying employment credentials, or misrepresenting their qualifications to obtain financial or employment-related benefits.

Many applicants perceive credential fraud as a low-risk, high-reward strategy to improve their employment prospects.

Employment fraud occurs when applicants misrepresent qualifications to:

- Secure employment: Falsifying qualifications, experience, or credentials to meet job requirements and obtain employment.
- Obtain credit: Using fraudulent qualifications or employment credentials as proof of employment or income when applying for loans or other forms of credit.
- Increase compensation: Misrepresenting qualifications to negotiate higher salaries.
- Pass the compliance threshold: Presenting false credentials to satisfy regulatory/professional requirements for restricted or specialised roles.

KEY FINDINGS:

- **98.5%** of these listings involved **falsified academic credentials** rather than payslip or employment information fraud.
- Employment fraud is concentrated within the core working-age population, with individuals aged 26–35 accounting for 44% of reported listings and those aged 36–45 contributing a further 37%. Together, these two age groups represent just over four-fifths of all listings. The category also exhibits a male majority, with men accounting for 59%.
- **Misrepresentation in the employment application process** accounts for 96% of all listings and therefore mirrors the overall demographic profile, with a 60% male majority and a clear concentration in the 26–35 age group. **Employee fraudulent conduct** is a distant second, representing around 3% of listings, but displays a contrasting demographic pattern. This subtype has a female majority (55%) and is even more concentrated among younger adults, with the 26–35 age group accounting for just over half of the listings.
- The age profile is consistent with the findings that these listings consist almost entirely of falsified qualifications submitted during the job application process. As such, the observed demographic pattern largely reflects the profile of the economically active, job-seeking population rather than a distinct age-specific fraud trend.

FUNERAL CLAIMS FRAUD - THE MAIN CONTRIBUTOR TO LONG-TERM INSURANCE FRAUD

Funeral claims fraud is a significant form of insurance fraud in the long-term insurance sector in South Africa. It involves the intentional submission of false or misleading information to obtain funeral policy benefits to which the claimant is not entitled. Because funeral policies typically provide rapid payouts and require relatively modest sums insured, they are particularly vulnerable to fraudulent claims and involve sophisticated document forgery schemes.

Funeral benefit insurance covers death-related expenses such as burial costs, cremation, funeral services, grave/plot maintenance etc. Claims are triggered by a death notification and require death certification documentation.

Common schemes include:

- **Paper child fraud:** Submitting a death benefit claim for a fictitious child or an individual who either never existed or died long before the policy was issued.
- **False death claims:** Claiming insurance benefits by falsely reporting someone as deceased or submitting claims for deaths that occurred before the policy became effective.
- **Document forgery:** Creating or altering supporting documentation, including death certificates, doctor certificates, undertaker documents, and identity documents, to substantiate fraudulent insurance claims.

Funeral claims fraud is a high-volume, moderate-value form of insurance fraud that targets vulnerable populations, particularly bereaved families seeking financial assistance during their time of loss. Detecting this type of fraud is challenging because records are fragmented across multiple government bodies and private entities, which can delay verification.

KEY FINDINGS:

- Fabricated documents dominated, accounting for **73.9%** of these listings.
    - Paper child fraud is significant with **22.3%** of these listings.
    - False death claims represent **22.1%** of these listings.
- ID document fraud was common, as 45.5% mentioned ID document related issues.
- Doctor, undertaker, and government body verification were the primary detection methods.
- KwaZulu-Natal emerged as the dominant hotspot for funeral and long-term insurance claim fraud, accounting for 74.5% of reported listings - a level of concentration that far exceeded any other province. The province also exhibited the highest local intensity of this type of fraud, with nearly 10% of the reported listings relating to funeral claims.

Fraud Type	Description & Examples
Fabricated Documents	Forged death certificates, doctor certifications, undertaker docs, ID documents
False Death Claims	Claiming deceased never died, person still alive, or death predates policy
Paper Child Fraud	Claiming death benefit for non-existent person (never born, or died years prior)

FALSE SHORT-TERM INSURANCE CLAIMS

Personal insurance claims fraud involves submitting claims for incidents that never occurred or deliberately inflating the extent of the loss to get a higher insurance payout.

KEY FINDINGS:

- **52%** of these listings related to **falsified documentation**, including invoices, receipts and damage reports.
- **Motor vehicle fraud** accounted for **27%** of these listings. These varied from staging accidents to multiple parties being involved, such as family members.
- The third highest modus operandi was claims for **property damage** at **26%**. The reports identified false claims on home invasions, geyser theft, and false repair claims.
- Trends identified included forged receipts and damage reports dated months after the incident occurred.
- Short-term insurance fraud exhibited a distinctly different geographic profile from long-term insurance fraud. While long-term (funeral and life) insurance fraud was overwhelmingly concentrated in KwaZulu-Natal, short-term insurance fraud was more broadly distributed across South Africa's three major urban economies. Gauteng accounted for the largest share with 39.8%, followed by the Western Cape (21.8%) and KwaZulu-Natal (21.1%). This suggests that short-term insurance fraud is more closely associated with the country's major economic and metropolitan centres than its long-term counterpart.

FRAUD THROUGH DIGITAL CHANNELS

Fraud committed through online or digital channels refers to the use of electronic platforms, online services, and digital technologies to deceive individuals or organisations for financial gain or other unlawful benefits.

Platforms and methods used include online banking channels, email, messaging platforms, phishing attacks, as well as vishing (voice phishing or phone-based scams).

Perpetrators use these channels to:

- Compromise legitimate customer accounts: To trick customers into revealing login credentials or OTP (One-Time PIN) codes.
- Open fraudulent accounts: Using stolen ID documents or legitimate identities to open mule accounts to receive funds.
- Execute unauthorised transfers: Once accounts are compromised, fraudsters transfer the victim's funds to mule accounts.
- Facilitate money laundering: Mule accounts are used to receive and transfer stolen or fraudulently obtained funds, helping to obscure the origin of the money and conceal the identity of the individuals behind the criminal activity.

FRAUD TYPES & MECHANISMS

Fraud Through Digital Channels	% of Total	Description & Mechanism
Mule Account (Receives Proceeds)	49.0%	Account is opened/ compromised to receive stolen funds, and funds are rapidly transferred or withdrawn.
Vishing Scam	12.2%	Voice phishing attack tricks customer into revealing credentials; attacker opens an account or compromises the existing account.
Online Banking Fraud	9.9%	Unauthorised transfers via compromised online banking; phishing emails redirect to fake banking sites.

KEY FINDINGS:

Many cases combined two vectors: Vishing attack and mule account fraud. Let us look at an example of the sequence:

1. It starts with a targeted vishing attack. The fraudster phones the customer pretending to be from their bank claiming there is an issue with their account or that some type of immediate action is required.
2. The customer is manipulated into revealing an OTP (One-Time PIN) or their credentials.
3. The fraudster transfers the customer's funds from their account to a mule account.
4. The funds are quickly withdrawn from an ATM machine, or transferred to an offshore account, or goes into crypto or online gambling.

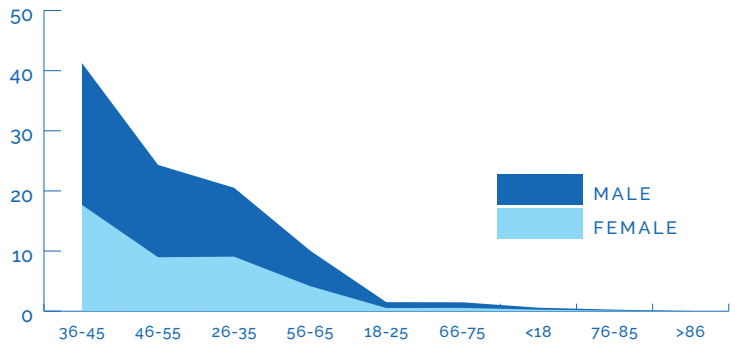
Vishing attacks are prevalent and represent a critical vulnerability. Consumers are targeted with a high success rate because these attacks are inherently difficult to detect and disrupt in real time.

Fraud perpetrated through digital channels is high-volume, executed in real time, and inherently difficult to trace, as it frequently spans multiple institutions and jurisdictions.

VICTIM ANALYSIS

Let us take a closer look at the victims of fraud:

Victims – Age and Gender Distribution



-24%
YOY % Change

4 008
CY

5 263
CY-1

VICTIMS OF IMPERSONATION

A victim of impersonation listings is loaded to the SAFPS database when it has been confirmed that someone's personal information has been used fraudulently.

It makes up **15%** of the listings we get from our Members.

The Gauteng and Kwa-Zulu Natal provinces had the most reported cases with 45% and 18% respectively.

SCAMS IN SOUTH AFRICA

While fraud is typically perpetrated without the victim's knowledge or consent, scams rely on manipulating victims into voluntarily transferring funds or disclosing personal and confidential information. In South Africa, scams are becoming increasingly sophisticated, with fraudsters continually adapting their tactics to exploit consumer trust and emerging digital channels.

At the end of 2024, the SAFPS introduced a new category allowing SAFPS Members to report scam-related incidents under dedicated sub-categories such as advance fee scams, ancestry scams, cyber scams, phishing, vishing, romance scams etc. This supports improved trend analysis and addresses specific scam typologies more effectively.

KEY FINDINGS:

Vishing scams accounted for 21% of these listings.

In these scams, fraudsters impersonate representatives of trusted organisations over the phone to manipulate victims into taking specific actions, disclosing personal or confidential information, or transferring funds under false pretences.

Change of banking details accounted for 12% of these listings.

In these scams, the victim is led to believe that they are being legitimately requested to update their details, usernames and passwords.

Advance fee delivery scams accounted for 11% of these listings.

Advance fee delivery scams involve fraudsters sending fraudulent messages claiming that the recipient has an undelivered parcel or package. Victims are instructed to pay an upfront fee, supposedly for taxes, release fees or customs. Once the payment is made, the scammers either disappear or continue to demand additional payments under various pretexts.

- 70% of the perpetrators were male, of this, 41% were between the ages of 18 and 25.
- In total, 40% of the fraudsters (both male and female) were between the ages of 18 and 25, and 37% were between the ages of 26 and 35.
- 62% of these listings were reported within Gauteng.
- Items used to entice victims varied greatly from animals to vehicles and related services (parts, engines etc) as well as building material.

“JUST SAY GOODBYE” CAMPAIGN

Fighting back against vishing scams

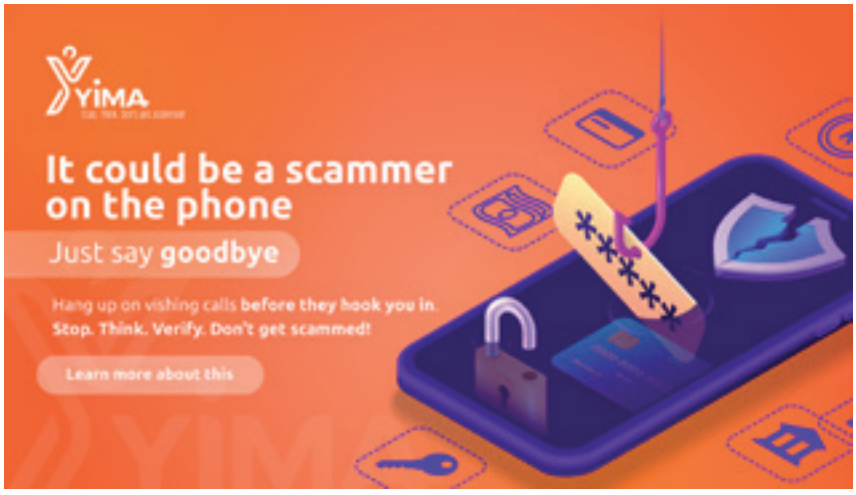
You are going about your day when you receive an unexpected call from your “bank” claiming there is fraud on your account. The caller tries to pressure you into taking action, but something does not feel right. So, what do you do? **“Just Say Goodbye”.**

In 2025, the SAFPS launched the “**Just Say Goodbye**” awareness campaign aimed at helping South Africans recognise and respond to increasingly sophisticated phone-based scams. These scams, known as vishing, involve fraudsters phoning victims impersonating representatives from banks, financial institutions, cellular companies, insurers, law enforcement or government agencies to manipulate victims into revealing sensitive information or transferring funds.

In South Africa, this scam tactic has become a preferred method for syndicates targeting both individuals and corporate employees, especially those with access to financial systems or customer data. The consequences range from drained bank accounts to compromised internal networks. Understanding how this scam works is the first step in building resilience, as awareness is the frontline defence in fraud prevention.

To empower consumers, the campaign unpacked three critical elements; how it works (modus operandi), red flags to look out for, and how to protect yourself.

Consumers should know they have power and that there are tools available to protect them.
Stop, think, and just say goodbye.



Website Banner

Mailer Banner

Social Media Carousels

Social Media Carousels

Social Media Carousels

07

SAFPS BOARD MEMBERS 2025


Christo Otto - Chairperson


Pero Roux - Deputy Chairperson


Manie van Schalkwyk - CEO


Sibusiso Buthelezi


Verusha Christmas


Louis Hennings


Kevin Maartens


Ulrich Janse van Rensburg


Athaly Khan


Wendy Knowler


Hlamalani Mashaba


Charl van der Walt

08

SAFPS MEMBERS

The SAFPS is a not-for-profit organisation, that is fully funded by its valued Members.

42
NEW SAFPS MEMBERS ONBOARDED SINCE 2021

Subscribing Members

Affiliate Members

BANKS
ABSA
Access Bank of South Africa
African Bank
Albaraka Bank
Amber Financial Technologies
Bidvest Bank
Capitec Bank
Discovery Bank
FNB, a division of FirstRand Bank Limited
Investec Bank Ltd
Nedbank Ltd
Standard Bank
Tyme Bank Ltd
Tyme Bank Ltd - Retail Capital

INVESTMENT
Discovery Life Investment
FNZ SA Holdings (Pty) Ltd
Sasfin Securities (Pty) Ltd

FINTECH
Apollo Access (Pty) Ltd
Pay Just Now (Pty) Ltd

ASSET FINANCE
BMW Financial Services
Daimler Truck Financial Services
Mercedes Benz Financial Services
MFC
MQ Finance (Pty) Ltd t/a Marquis Finance
SA Home Loans
SA Taxi Development Finance
Wesbank, a division of FirstRand Bank Limited

CASH-IN-TRANSIT
Fidelity Security Group
SBV Services (Pty) Ltd

CLOTHING RETAIL
Home Choice (Pty) Ltd
Mr Price Group
RCS Cards
The Foschini Retail Group (Pty) Ltd
Truworths Limited
Woolworths Financial Services (Pty) Ltd

PUBLIC SECTOR
National Lotteries Commission

TELECOMS PROVIDERS
Cell C
Lesake Merchant Solutions (Pty) Ltd
Mobile Telephone Networks Proprietary Limited t/a MTN
Telkom SOC Limited

FURNITURE RETAIL
Pepkor Lifestyle
Lewis Group

HEALTHCARE
Discovery Health (Pty) Ltd
Discovery Vitality (Pty) Ltd

MICRO FINANCE
Bayport Financial Services
Direct Axis
Evolution Finance
Finchoice
iMas Finance Co-operative Ltd
Old Mutual Finance (Pty) Ltd
Thuthukani Housing Finance (Pty) Ltd

INSURANCE

- 1 Life
- ABSA Life Division
- Capitec Life Limited
- Discovery Central Services
- Discovery Life - Employee Benefits
- Discovery Insure Limited
- Discovery Life Limited
- Dotsure
- FirstRand Life Assurance Limited
- Hollard Assurance Company Ltd
- MiWay Insurance Ltd
- Nedbank Group Insurance Holdings Ltd
- Santam Ltd
- Standard Bank Insurance Division
- Telesure Investment Holdings (Pty) Ltd

PUBLIC SECTOR

- Department of Home Affairs
- Financial Intelligence Centre
- South African Reserve Bank
- South African Revenue Service

AFFILIATE MEMBERS

- Experian Credit Bureau
- TransUnion Credit Bureau
- XDS Credit Bureau

GLOBAL FINANCIAL CRIME PREVENTION NETWORK

- AFCX - Australian Financial Crime Exc.
- Cifas - UK counterpart to SAFPS
- Insurance Crime Bureau
- SABRIC

RESELLERS

- Contactable (Pty) Ltd
  - Assupol Insure
  - Avbob Mutual Asurance Society
  - Ayo Intermediaries
  - Boland Motor Group (Pty) Ltd
  - Europcar SA
  - F & I Management Solutions
  - FAIMS Motus Dealership
  - HeyCarter Dealerships (Pty) Ltd
  - Melon Mobile
  - Metro Fibre
  - Motus Corporation
  - Seriti Solutions
  - Shoprite Checkers
  - Sileo Vehicle Rentals (Pty) Ltd
  - Tsogo Sun
  - We Buy Cars
- Secure Citizen
  - BidorBuy
  - EFT Corp Technologies (Pty) Ltd
  - Privately Property
  - The Good People Data Company Ltd
  - Trustlink (Pty) Ltd

RESELLERS

- Akiba Digital
- Consumer Profile Bureau (CPB)
- Cred-IT-Data
- Dots Africa
- Experian
- ICFP
- iPulse Systems (Pty) Ltd
- Lemonaide (Pty) Ltd
- LexisNexis Risk Management
- MAB Bureau (Pty) Ltd
- Maris IT Development (Pty) Ltd
- Metagrated (Pty) Ltd
- MIE (Pty) Ltd
- National Validation Services
- Octagon Business Solutions (Pty) Ltd
- Orocorp (Pty) Ltd
- Profitshare Partners (Pty) Ltd
- Supplierrate (Pty) Ltd
- TransUnion
- Vericred Credit Bureau (Pty) Ltd
- Xpert Decision Systems (Pty) Ltd

OUR PURPOSE IS CLEAR - TO PREVENT FRAUD THROUGH SHARED INTELLIGENCE.

09 IN CLOSING

Collaborative, data-driven defence drives impactful change.

We hope that you enjoyed reading the 2025 SAFPS Annual Report and found the information shared insightful. Fraud continues to remain a threat to organisations, the South African economy, and consumers.

As the SAFPS, our purpose is clear – to prevent fraud through shared intelligence. We are committed to continue working with our Members and fraud prevention partners to enhance and develop solutions that will ultimately reduce the impact of fraud and financial crime.

We would like to once again thank our valued SAFPS Members, strategic partners and stakeholders, as well as our Board members for the support that makes this all possible. May we continue to work together to create freedom from fraud.

Sincerely,
The SAFPS Team

10 DISCLAIMER

While every effort has been made to ensure the accuracy and reliability of the aggregated data, the original data was provided by Members and external sources. Consequently, the organisation cannot guarantee the completeness or accuracy of the data at its origin.

The statistics and analyses contained in this report are based on the aggregated data and are intended for informational purposes only. They should not be construed as definitive indicators of trends or as a substitute for professional advice or detailed investigation.

Additionally, the interpretations and conclusions drawn from the data are those of the organisation and do not necessarily reflect the views of all stakeholders. Readers are encouraged to consider the data in the context of the broader environment and other available information.

The organisation disclaims any liability for decisions made based on the information presented in this report. Users of this report are advised to conduct their own due diligence and verify the information before making any business or financial decisions.

For further information or clarification regarding the data and analyses presented in this report, please contact our team via the SAFPS Contact Centre.

11

GLOSSARY

YoY – Year-on-Year
CY – Calendar Year
CY-1 – Previous Calendar Year
YTD – Year-to-Date

Digital Fraud

This category is used in situations where illegal online or electronic fraudulent activities have led to financial, data or reputational losses by using a computer or other electronic devices. Sub-categories include ATM crime, card cloning, data breaches, internet fraud, and mobile device fraud.

Employment Fraud

This is when an employee, prospective employee, or employer has been involved in any corrupt, criminal and/or fraudulent related practices. This includes instances when an employee, person, firm, organisation, or company has aided, abetted, assisted, and/or conspired through the solicitation of a bribe, to fraudulently or otherwise dishonestly obtain credit, hire facilities or other products or services (commonly known as an accomplice). This is done through supplying false ID/personnel/ employer particulars, staff dishonesty, using false information or qualifications on an application form, etc.

Fraudulent Documents

This category will be used most often, but not exclusively, with application fraud where the applicant supplies false documents about him or herself to deceive the organisation. This is when documents provided by individuals are forged or falsified. For example, payslips, bank statements, or ID documents, etc.

Impersonation Because of an Altered ID Document
When the subject provides a name and/ or ID number that either does not correspond to official records, or the information does not exist.

Insurance: Long-Term
This category relates to when fraud was perpetrated in long-term insurance policies i.e., life changing events like death, retirement or disability.

Insurance: Short-Term
This category relates to fraud perpetrated in insurance policies that includes all types of insurance, excluding long-term or life insurance cover.

Misuse of Accounts Through Fraudulent Conduct
When an individual tries to evade financial liability by guile, trickery or illegitimate presentation of the individual's financial position, this category should be used.

- **Money mule** - When a bank account owner allows the movement of funds that are the proceeds of crime via their bank account, on behalf of another individual.

Scams
This category relates to fraud perpetrated by scammers who deliberately attempted to gain a benefit from fraudulent or deceptive operations.

- **Advance Fee: Delivery Scam** - Payments are requested for the delivery of a fictitious package.
- **Change of Banking Details** - The victim is led to believe that they are being legitimately requested to update their details, usernames and passwords.
- **Vishing: OTP/ Remote Access Scams** - Victims are contacted telephonically under the guise of a government, financial or reputable institution and requested to provide or confirm personal information or passwords.
- **Vishing: Personal & Security Information** - Victims' information is phished via a call from the scammer impersonating an institution's employee, a person of authority, a family member, etc.

Victims of Impersonation
This is when there is confirmed evidence that the person to be listed has become the Victim of Impersonation due to their personal information having been used fraudulently.

SAFPS
SOUTHERN AFRICAN
FRAUD PREVENTION
SERVICE

safps@safps.org.za
www.safps.org.za
+27 (0)11 867 2234

YIMA

info@yima.org.za
www.yima.org.za
+27 (0)11 867 2234