OFFICE OF THE
TAX OMBUD

Ensuring fairness

Draft report on the investigation in terms of
Section 16(1)(b) of the Tax Administration Act 28 of 2011 into

Alleged eFiling Profile Hijacking

1 October 2025

Table of contents

1 EXECUTIVE SUMMARY 4

1.1 PURPOSE 4

1.2 BACKGROUND 4

1.3 WHAT IS A SYSTEMIC INVESTIGATION? 4

1.4 THE TITLE OF THE REPORT: *"eFILING PROFILE HIJACKING"* 5

1.5 METHODOLOGY FOLLOWED DURING INVESTIGATION 5

1.6 EXPANDED SCOPE OF THE OTO KEY FINDINGS AND RECOMMENDATIONS ON THE DRAFT REPORT 6

1.7 SUMMARY OF KEY FINDINGS 8

1.8 SUMMARY OF RECOMMENDATIONS 10

2 INTRODUCTION 20

2.1 BACKGROUND TO THE INVESTIGATION 20

2.2 INVESTIGATION FOCUS 22

2.3 UNDERSTANDING SARS EFILING AND PROFILE REGISTRATION PROCESS 23

2.4 SYSTEMIC INVESTIGATION AND ANALYTICAL FRAMEWORK 27

3 METHODOLOGY 30

3.1 INVESTIGATIVE AND RESEARCH PROCESS 30

3.2 CONCLUSION 34

4 UNDERSTANDING EFILING PROFILE HIJACKING 35

4.1 WHAT IS EFILING PROFILE HIJACKING? 35

4.2 HOW EFILING PROFILE HIJACKING OCCURS? 35

4.3 TYPES OF EFILING PROFILE HIJACKING 36

4.4 TAXPAYER VULNERABILITIES 36

4.5 HOW CAN TAXPAYERS PROTECT THEMSELVES FROM EFILING PROFILE HIJACKING? 38

4.6 CONCLUSION 40

5 CASE STUDIES 41

5.1 CASE STUDY 1: FRAUDULENT COMPROMISE OF TAXPAYER'S EFILING PROFILE 42

5.2 CASE STUDY 2: FRAUDULENT MODIFICATION OF TAXPAYER REPRESENTATION AND VAT REFUND MISAPPROPRIATION 45
5.3 CASE STUDY 3: DIGITAL FRAUD INVESTIGATION ON TAXPAYER'S EFILING PROFILE 49
5.4 CASE STUDY 4: FRAUDULENT UPDATE OF TAXPAYER'S REGISTERED PARTICULARS ON EFILING 51
5.5 CASE STUDY 5: FRAUDULENT EFILING REGISTRATION AND UNAUTHORISED TAX RETURNS 54
5.6 CASE STUDY 6: UNAUTHORISED ONE-TIME PIN (OTP) AND EFILING PROFILE FRAUD 58
5.7 CASE STUDY 7: FRAUD AND SIMULATED STOPPER 60
5.8 KEY FINDINGS FROM CASE STUDIES 63
6 SARS INTERNAL SYSTEMS AND INVESTIGATION CONTROLS 65
6.1 INTERNAL OPERATIONAL CHALLENGES WITHIN SARS 65
6.2 CONCLUSION 73
7 SARS DIGITAL IMPROVEMENTS POST THE COMMENCEMENT OF OTO INVESTIGATION 75
7.1 IMPLEMENTATION OF THE TAXPAYER VERIFICATION AND EDNA SYSTEM AT SARS BRANCHES 75
7.2 ENHANCEMENTS TO TWO-FACTOR AUTHENTICATION AND EFILING PASSWORD SECURITY 76
7.3 CONCLUSION 78
8 RELEVANT INFORMATION SHARING-ARRANGEMENTS BETWEEN SARS AND VARIOUS INSTITUTIONS 79
8.1 INFORMATION SHARING BETWEEN SARS AND CIPC 79
8.2 INFORMATION SHARING BETWEEN SARS, SAPS AND NPA 80
8.3 INFORMATION SHARING BETWEEN SARS AND SARB 81
8.4 INFORMATION SHARING BETWEEN SARS AND FIC 81
8.5 INFORMATION SHARING BETWEEN SARS and DHA 82
8.6 INFORMATION SHARING BETWEEN SARS AND BANKS 82
8.7 CONCLUSION 83
9 KEY FINDINGS AND RECOMMENDATIONS 84
9.1 KEY FINDINGS 84

9.2 RECOMMENDATIONS 93
10 CONCLUDING REMARKS 103
11 ABBREVIATIONS 105

1 EXECUTIVE SUMMARY

1.1 PURPOSE

The purpose of the report is to assess the scope and impact of eFiling profile hijacking, identify factors that make taxpayers vulnerable to eFiling profile hijacking, evaluate SARS's response mechanisms to taxpayers who report eFiling profile hijacking and suggest areas for improvement.

1.2 BACKGROUND

The integrity of SARS eFiling system is critical for efficient tax administration and taxpayer compliance. The rapid increase in e-filing profile hijacking has presented significant challenges for South African taxpayers and tax practitioners and has raised concerns regarding the security of the SARS eFiling system.

Fraudsters have exploited vulnerabilities of the SARS system to gain unauthorised access to taxpayer accounts, modify banking details and redirect tax refunds for fraudulent gain.

1.3 WHAT IS A SYSTEMIC INVESTIGATION?

Generally, section 16(1)(b) of the Tax Administration Act, 28 of 2011(TAA) makes provision for the Office of the Tax Ombud (OTO) to review at the request of the Minister or at the initiative of the OTO with the approval of the Minister, any systemic and emerging issue related to a service matter or the application of the provisions of the TAA, or procedural or administrative provisions of a tax Act.

The OTO has been receiving complaints and queries from taxpayers and industry bodies. Following a public workshop held with SARS, taxpayers and industry bodies on 13 June 2024 the OTO sought and obtained approval from the Minister of Finance on 12 August 2024, to conduct a review of possible systemic and emerging issues related to alleged SARS's service failures in

assisting taxpayers with eFiling profile hijacking timeously in terms of section 16(1)(b) of the TAA.

In simple terms, a systemic investigation refers to an examination of underlying problems that affect or may affect multiple taxpayers within a tax system. These issues often pertain to how specific SARS systems operate, how policies, practices or procedures are formulated and implemented or how tax provisions are applied or disregarded by SARS. Even if the sample from which these issues are identified is small, what matters is the potential impact of the systemic issues raised.

1.4 THE TITLE OF THE REPORT: *"eFILING PROFILE HIJACKING"*

The OTO has chosen the title "eFiling profile hijacking" for this report because it aptly reflects the nature and scope of the systemic investigation undertaken by the OTO. The rationale behind this title is that eFiling profile hijacking refers to situations where a taxpayer's or tax practitioner's SARS eFiling profile is unlawfully accessed, taken over or manipulated by unauthorised persons. In such instances, the taxpayer or tax practitioner loses access to the SARS e-Filing profile.

These unauthorised activities often lead to significant fraudulent conduct, such as the redirection of tax refunds to bank accounts controlled by the fraudsters. Victims of such hijackings suffer not only financial loss but also compromised personal and tax information as well as administrative challenges in regaining control over their tax affairs.

1.5 METHODOLOGY FOLLOWED DURING INVESTIGATION

The investigation into alleged eFiling profile hijacking followed a structured, triangulated research methodology. This approach included:

- **Data collection through survey:** Gathering data from affected taxpayers and tax practitioners.

- **Case Study Analysis:** Case studies were selected from a broader pool of fraud related complaints received by the OTO; and
- **Stakeholder engagements:** Engagements were held with taxpayers, tax practitioners, Recognised Controlling Bodies (RCBs), South African Tax Practitioners United (SATPU), the South African Revenue Service (SARS), the Companies and Intellectual Property Commission (CIPC), Banking Association South Africa (BASA), Southern African Fraud Prevention Service (SAFPS).

Given the complexity of these fraud cases, the investigation prioritised identifying root causes, systemic vulnerabilities and institutional response mechanisms. This comprehensive and multifaceted approach ensured a thorough analysis, leading to key findings and actionable recommendations, aimed at improving taxpayer protection and the integrity of the South African tax system.

1.6 EXPANDED SCOPE OF THE OTO KEY FINDINGS AND RECOMMENDATIONS ON THE DRAFT REPORT

While the OTO conducted its investigation into the alleged SARS eFiling profile hijacking, it is important to note that the OTO's authority extends beyond merely reporting on SARS's conduct. In line with its mandate, the OTO has issued key findings and recommendations not only to SARS, but also to taxpayers, tax practitioners and other affected institutions.

- **Key findings and recommendations to tax practitioners and banks**

The OTO is legally empowered to make recommendations to SARS and taxpayers in matters falling within the OTO mandate.

In turn section 151 of the TAA defines a *"taxpayer"* as including:

- A person who is or may be chargeable to tax or with a tax offence
- A representative taxpayer
- A withholding agent
- A responsible third party

- A person who is subject of a request to provide assistance under an international tax agreement.

Based on the above-mentioned definition, persons such as tax practitioners and banks, which may act as withholding agent or responsible third parties, fall within the scope of the definition of *"taxpayer".*

- **Key findings and recommendations to broader stakeholders**

Whilst institutions such as the National Treasury, the South African Reserve Bank (SARB), the Companies and Intellectual Property Commission (CIPC) and the South African Police Service (SAPS) fall outside the formal jurisdiction of the OTO, they are often indirectly implicated in cases of profile hijacking. This includes:

- **SAPS**: As SARS require taxpayers to report and obtain the case number for profile hijacking cases from SAPS in order to conduct criminal investigation fraud or identity theft in this regard.
- **CIPC**: As changes to directors of companies are made at CIPC.
- **SARB**: Where financial regulatory oversight is conducted.
- **National Treasury**: Where tax policy changes are made.
- **Banks**: Where fraudulent changes to baking details are made on taxpayer profiles.

Although these entities fall outside the direct mandate of the OTO, the interconnected nature of SARS eFiling profile hijacking necessitates cooperation and responsiveness from these institutions in line with the OTO's recommendations.

The multi-stakeholder nature of eFiling profile hijacking cases demands collaborative stakeholder response. Such an integrated approach is essential to protect taxpayers, prevent profile hijacking and restore trust in the South African tax system.

1.7 SUMMARY OF KEY FINDINGS

1.7.1 Highest Prevalence of eFiling profile hijacking in tax practitioners followed by individual taxpayers.

1.7.2 Incidents of eFiling profile hijacking are common with Personal Income Tax (PIT) followed by Value Added Tax (VAT).

1.7.3 Estimated value of fraud in most eFiling profile hijacking cases is below R10 000, but a considerable number also fall within R10 000 to R100 000.

1.7.4 Challenges on the authentication systems and security measures have created vulnerabilities that fraudsters exploit.

1.7.5 Challenges with fraud detection and slow response mechanisms allow hijackers to access and misuse eFiling profiles undetected.

1.7.6 Taxpayers and tax practitioners encounter ineffective communications channels and limited support from SARS when trying to resolve eFiling profile hijacking cases.

1.7.7 Syndicated tax fraud begins with unauthorised or fraudulent changes to the information of directors of companies at the CIPC.

1.7.8 Victims of eFiling profile hijacking report that SAPS stations are often unable to categorise or escalate cases of tax profile hijacking.

1.7.9 Fraudsters continue to open fraudulent bank accounts, particularly with digital banks, and redirect fraudulent tax refunds from SARS into these bank accounts.

1.7.10 Alleged internal fraud and insider involvement

1.7.11 Taxpayers lack digital security awareness.

1.8 SUMMARY OF RECOMMENDATIONS

1.8.1 Recommendations to SARS

1.8.1.1 Strengthen authentication & access controls

- Compulsory Two Factor Authentication (2FA) for all users.
    - With effect from 22 November 2024, SARS made 2FA compulsory for individual taxpayers and tax practitioners. SARS should implement graded 2FA policies based on activity risk level.
    - According to the information from SARS, with effect from March 2025, SARS introduced One-Time Pin (OTP) on eFiling registration detail function for all bank detail changes. SARS should continue monitoring the effectiveness of the OTP implementation to ensure that it adequately addresses the underlying risks.
    - SARS also advised the OTO that they have implemented alert emails being sent to the taxpayer's security contact detail addresses for any changes to a taxpayer's registered details, including updates to security contact details. SARS should continue enhancing its security measures to ensure that its online platforms remain trusted, secure and user friendly for all taxpayers.
- Strengthen known 2FA challenges
    - SARS should continue monitoring the implementation of notifications to taxpayers and tax practitioners when:
        - high risks changes are made to their profiles, for example, passwords resets, banking detail changes, changes to the director/s of company, new access grants.
        - Login attempts are made from unusual devices or unusual locations.

- SARS should consider introducing additional measures such as:
    - Enable OTP location/device verification with alerts (e.g., “OTP requested from a new device/IP”).
    - Add optional authenticator app support (e.g., Google Authenticator, Microsoft Authenticator) rather than relying solely on vulnerable SMS OTPs.
    - 2FA reset protocols requiring full identity re-verification, especially when suspicious activity is detected.

1.8.1.2 Enhance biometric security across all profiles

- Current biometric application is limited
    - Biometric authentication implemented in August 2024 is currently only used for new eFiling registrations.
    - SARS must retrofit biometric re-verification for:
        - All existing taxpayer profiles (individual and business).
        - Key changes to existing taxpayer profiles (banking details, tax representative changes).
    - SARS should create a biometric check-in schedule for dormant profiles (e.g., if no activity for 6–12 months, biometric re-authentication is triggered before allowing access).

1.8.1.3 Strengthen fraud detection while enhancing service efficiency

- Currently SARS is restricting tax practitioners from updating security details on behalf of clients, even when a valid Power of Attorney (POA) is provided. While this control is aimed at reducing fraud, SARS should enhance it to strike a balance between fraud prevention and service accessibility. The current approach inadvertently hinders efficient service delivery to taxpayers.

1.8.1.4 *Enhancement of security and prevention of fraud*

- SARS should allow taxpayers to view a detailed login history (IP address, device, location) from within their profile.
- During the risk period of SARS tax filing season, SARS should consider introducing a profile lock option that allows taxpayers to voluntarily freeze changes to their banking details by those taxpayers who do not expect to make changes in this regard. This measure would help prevent unauthorised updates and reduce the risk of eFiling profile hijacking during times of increased fraudulent activity.

1.8.1.5 *Improve refund verification*

- SARS should hold refunds for additional verification when banking details are changed shortly before a refund is claimed.
- SARS should increase pre-refund verification steps for all VAT refunds above certain thresholds.
- SARS should ensure that stoppers (not simulate stoppers) are implemented immediately on taxpayer accounts as soon as the taxpayer or tax-practitioner reports the incident of eFiling Profile Hijacking.
- SARS should adjust its refund audit triggers to not only flag high value claims but also:
    - Unusual refund patterns.
    - New or recently modified new bank details, company directors' profiles, tax practitioner profiles.
    - Frequent/similar amounts refund requests from the same entities.
- Implement automated alerts for refunds processed after hours or within days of bank account creation or change in banking details.

1.8.1.6 *Improve SARS end to end digital fraud process*

- SARS should ensure that they provide timely responses and regular updates to fraud victims, thereby preventing gaps in communication.

- SARS should ensure that the SARS digital fraud hotline is up to standard.
- SARS should clearly communicate the steps taxpayers need to take if their profile is hijacked.
- SARS should ensure that they fast-track account recovery so that tax practitioners do not wait for too long before their profile is updated as this renders them unable to work or provide services to their clients.
- SARS should ensure that eFiling profile hijacking cases are concluded within a reasonable time frame of 150 days to prevent prolonged taxpayer uncertainty. This should be clearly communicated to taxpayers in the service charter.

1.8.1.7 Strengthen internal controls and processes

- SARS should conduct periodic independent audits on SARS eFiling systems and Mobi APP.
- To reduce the risk of internal fraud and insider involvement, SARS should initiate or continually improve on:
    - regular audits on system log ins, employee access history and refunds processed after hours or within days of bank account creation or change in banking details.

1.8.1.8 Communication and education

- SARS should improve nationwide taxpayer awareness campaigns targeting:
    - Digital security, phishing scams and best practices.
    - Taxpayers to monitor eFiling access and refund activity.
    - Provision of step-by-step guidelines on how to report eFiling profile hijacking.
- SARS should provide targeted services for vulnerable groups, for example:
    - Mobile support units or community service desks in low-income earners to assist with reporting, education and follow up on unresolved complaints.

1.8.2 Recommendations to Tax Practitioners

1.8.2.1 Strengthen third-party access controls.

1.8.2.1.1 Tax practitioners should work with SARS to:

- Strengthen two factor authentication for all tax practitioner logins to eFiling profiles.
- Implement a specific user ID and password for each individual user in a practice, rather than using shared credentials.
- Implement automatic real time email/SMS notifications to taxpayers when:
  - Tax practitioners request access to taxpayers' profiles.
  - High risk changes are made to taxpayer profiles such as:
    - changing banking details
    - updating tax practitioner details
    - changing directors of company information.

1.8.2.2 Tax practitioners should submit taxpayer details when they are registering to act on behalf of a taxpayer. This assists to create a direct association between the tax practitioner and the taxpayer themselves.

1.8.2.3 SARS should provide taxpayers with a login history visibility where they can:

- View all active tax practitioners linked to their profile.
- Monitor recent activity on their account.

1.8.2.4 SARS should require additional verification if tax practitioners make high risk changes to taxpayer profiles such as:

- changing banking details
- updating tax practitioner details
- changing directors of company information.

1.8.2.5 Improve Code of conduct between tax practitioners & SARS

- Tax practitioners should engage with SARS to improve the current code of conduct in relation to digital security.

1.8.3 Recommendations to Taxpayers

1.8.3.1 Use strong, unique passwords

- Taxpayers should create complex passwords using a mix of letters, numbers, symbols.

1.8.3.2 Use Two Factor Authentication System

- Taxpayers should use the recently introduced two factor authentication on individual SARS eFiling profile to add an extra layer of security.
- Taxpayers should use the recently introduced Biometrics on individual SARS eFiling profile to add an extra layer of security.
- Taxpayers should use a trusted authenticator app or SMS verification.

1.8.3.3 Beware of phishing scams

- Taxpayers should never click on suspicious links or open attachments from unknown sources.
- Taxpayers should verify emails or SMS claiming to be from SARS via the official SARS website, SARS call centre or OTO call centre.

1.8.3.4 Keep login credentials private

- Taxpayers should not share their SARS eFiling login details with anyone, including tax accountants, without secure arrangements.

1.8.3.5 Secure e-mail account

- Taxpayers should use strong passwords and two factor authentication on their email accounts as; these are linked to their SARS profiles.
- Taxpayers should regularly monitor their emails for unauthorised access.

1.8.3.6 Avoid using public Wi-Fi for tax transactions

- Taxpayers should perform SARS related tasks on secure, private networks only.

1.8.3.7 Update software regularly

- Taxpayers should ensure that their operating system, browser and antivirus software are up to date to avoid malware risks.

1.8.3.8 Monitor SARS profile activity

- Taxpayers should regularly log into their SARS eFiling account to check for unusual activity or unauthorised changes.

1.8.3.9 Use trusted devices

- Taxpayers should avoid logging in from shared or public computers where keyloggers may be installed.

1.8.3.10 Report suspicious activity immediately

- If taxpayers suspect that their profiles have been hijacked, they should contact SARS immediately to secure their accounts.

1.8.4 Recommendations to National Treasury

1.8.4.1 Proposed changes to the TAA

It is proposed that the following changes should be made to:

- insert a provision that expressly provides that in instances where a taxpayer's profile has been unlawfully accessed and hijacked, resulting in a refund being fraudulently redirected to a third-party bank account, SARS shall remain obligated to pay the legitimate refund to the affected taxpayer, after the investigation is done and there is no evidence of taxpayer involvement , notwithstanding the prior payment of a refund to the fraudulent bank account.

- insert a provision that expressly prohibits SARS from initiating or continuing recovery actions against a taxpayer, until the investigation is done and there is no evidence of taxpayer involvement, in instances where the taxpayer's profile has been hijacked and false deductions, such as fictitious expenses, have been claimed by fraudsters in the taxpayer's tax return in order to generate artificial refunds subsequently paid into fraudulent accounts.

1.8.4.2 Establishment of an Inspector General as recommended by the Nugent Commission of Inquiry

One of the recommendations of the Nugent Commission of Inquiry into SARS was the establishment of an Inspector General. If established, the Inspector General would amongst other things, be responsible for:

- Conducting proactive investigations into high-risk areas where internal fraud or collusion is most likely to occur.
- Implementing continuous risk assessments and internal control evaluations to identify and address vulnerabilities in SARS systems and processes.
- Monitoring and evaluating the effectiveness of SARS internal anti-fraud measures and making recommendations for improvements.
- Providing a secure and independent reporting system accessible to all SARS employees. This system would allow employees to report, without fear or favour, colleagues suspected of internal fraud and/or insider involvement in profile hijacking.
- Ensuring timely follow up on those reports with independent oversight.
- Publishing periodic reports on the nature and resolution of internal fraud cases, to promote transparency and organisational accountability.

1.8.5 Recommendations to the South African Reserve Bank

- It is recommended that the incidents that the OTO have identified with the specific banks should be reported to the Prudential Authority of the South African Reserve Bank for their consideration.

1.8.6 Recommendations to SARS and Banks

- It is recommended that SARS should collaborate with banks to:
    - flag new accounts receiving refunds tied to new bank accounts (created within the last 90 days and/or with no transaction history), recently changed CIPC entities, large VAT refunds amounts, unusual VAT refunds amounts (for example similar amount in month 1 and month 2).
    - Flag bank accounts previously used in VAT fraud schemes and blocks or delays refund to those accounts pending investigation.
    - Strengthen the real time pre-refund validation with all banks.
    - Revise its MOU with the banking sector to include:
        - Sector wide minimum compliance standards for bank detail validation.
        - Turnaround time guarantees for verification requests.
        - Joint escalation pathway for fraud investigation.

1.8.7 Recommendations to SARS and CIPC

- It is recommended that:
    - CIPC must notify SARS immediately and automatically of any changes to directors or company ownership information and SARS should use this notification to temporary freeze payment of VAT refunds until the new information is verified.
    - Any changes to the directors of company information submitted to CIPC should be pre-validated by SARS.
    - SARS and CIPC should establish a joint vetting process of high-risk changes aimed at flagging frequent changes to directors of

companies, changes to directors of companies closely followed by large VAT refunds.

- CIPC should maintain a publicly accessible audit trail of historical changes to directors of companies for transparency and due diligence.
- SARS and CIPC should encourage business owners to regularly check CIPC status and company director records.

1.8.8 Recommendations to SARS and SAPS

- It is recommended that SARS in collaboration with SAPS should:
  - develop and provide standardised training modules to SAPS station level personnel covering the following: what is tax profile hijacking, how to identify digital tax fraud, how to escalate these matters to National Prosecuting Authority.
  - develop a national Standard Operating Procedure for reporting and handling tax profile hijacking.

2 INTRODUCTION

2.1 BACKGROUND TO THE INVESTIGATION

The OTO initiated this investigation in response to widespread concerns from taxpayers and tax practitioners regarding the alarming increase in unauthorised access to eFiling profiles. Reports indicated that fraudsters were systematically exploiting security weaknesses to gain control over taxpayer and tax practitioner accounts. These unauthorised intrusions primarily involved altering security details, manipulating banking information, and submitting fraudulent tax returns to redirect refunds to fraudulent bank accounts.

The urgency of the investigation was heightened by the frustration expressed by tax practitioners, who found themselves unable to assist clients whose eFiling profiles had been hijacked. This has been a long standing issue, and the previous Tax Ombud, Judge Ngoepe, alluded to it during the meeting on ***7 June 2022***, with the Parliamentary Standing Committee on Finance, wherein he stated the following: "*Also, there had been a number of complaints to Parliament about SARS's conduct, such as not paying refunds on time and matters relating to identity theft. The OTO had raised some of these issues with SARS, and believed SARS was working on resolving its systematic issues".*

Also, when the new Tax Ombud, Miss Yanga Mputa, joined the OTO on ***1 July 2023***, both taxpayers and tax practitioners continue to raise their frustrations regarding eFiling Profile hijacking. As such, a meeting was held between the OTO and the South African Tax Practitioners United (SAPTU) on ***8 April 2024***, where concerns about escalating fraud were brought to the forefront. Subsequent engagements on ***18 April 2024***, involving the OTO, the South African Revenue Service (SARS), and Recognised Controlling Bodies (RCBs), confirmed the severity of the problem. SARS acknowledged the growing threat but unauthorised the need for RCB members to utilise its online reporting system to escalate cases.

Recognising the systemic nature of the issue, the OTO expanded its enquiry by hosting a public engagement on ***13 June 2024***. This platform allowed taxpayers

and tax practitioners to share their direct experiences with eFiling hijackings, providing critical insights into the fraudulent methodologies used. The engagement attracted 305 participants, reinforcing the need for intervention at a systemic level.

During the session, SARS officials assured attendees that the revenue service itself had not been hacked, but rather that individual taxpayer profiles were being compromised through techniques such as phishing, social engineering, and credential manipulation. SARS outlined its existing fraud mitigation strategies, which included:

- Blocking multiple profiles suspected of fraudulent activity.
- Enhancing the online query resolution system.
- Collaborating with banks and key stakeholders.
- Establishing a digital fraud reporting portal to streamline fraud case submissions.

Despite these measures, participants expressed dissatisfaction with SARS's handling of reported cases, particularly regarding delayed responses, lack of case updates, and undefined resolution timelines. Tax practitioners lamented the absence of clear turnaround times for SARS investigations, leaving affected taxpayers vulnerable without recourse.

In concluding the public engagement, the OTO identified immediate reforms SARS could implement, including:

- Improved acknowledgment of fraud queries.
- Issuance of tax clearance certificates to prevent disruptions.
- Suspension of payments linked to suspicious transactions.
- Enhanced communication and case tracking mechanisms.

Given the continued concerns, the OTO submitted a request to the Minister of Finance to conduct a review of possible systemic and emerging issues related to alleged SARS's service failures in assisting taxpayers with eFiling profile hijacking timeously in terms of section 16(1)(b) of the TAA. The findings from this investigation are intended to drive meaningful system level and policy reforms, prevent similar occurrences and restore public trust in the tax administration system.

2.2 INVESTIGATION FOCUS

The primary objectives of this investigation are to assess the scope, patterns, and effectiveness of SARS's response to eFiling profile hijacking.

Specifically, the investigation seeks to identify factors that make taxpayers vulnerable to hijackings, suggests some precautionary steps to taxpayers, identify any improvements to SARS processes to reduce risks, analyse procedural effectiveness of SARS assistance to taxpayers who raise any suspicions that their profile was hijacked, any potential tax policy matters to be considered by National Treasury and any other matters or findings that are incidental to this investigation. To achieve these objectives, the investigation focused on the following key areas:

- **Evaluate Service Failures:** Determine whether systemic inefficiencies within SARS contributed to taxpayers' inability to reclaim hijacked profiles and prevent fraudulent tax filings.
- **Identify Fraud Mechanisms:** Analyse how fraudsters manipulate eFiling security protocols to hijack profiles, change banking details, and illicitly claim tax refunds.
- **Assess SARS's Response**: Review the adequacy of SARS's fraud detection and resolution mechanisms, including case turnaround times and taxpayer communication efforts.
- **Analyse Financial Impact**: Measure the monetary consequences of fraudulently filed tax returns, unauthorised banking detail modifications, and delayed interventions.

- **Investigate Regulatory Gaps:** Identify legislative or procedural shortcomings that enable profile hijackings to persist undetected or unresolved.
- **Strengthen Prevention Strategies:** Develop recommendations for improving fraud detection, taxpayer education, and fraud resolution protocols within SARS.

Additionally, SARS's prolonged investigation periods pose severe financial implications, as taxpayers who lose access to their profiles struggle to file returns and correct fraudulent transactions.

Given the widespread nature and growing financial consequences of eFiling profile hijacking, the OTO deemed it necessary to conduct a systemic review, engaging SARS, industry bodies, and affected taxpayers to develop recommendations for improving fraud resolution efficiency and strengthening taxpayer protection mechanisms.

2.3 UNDERSTANDING SARS EFILING AND PROFILE REGISTRATION PROCESS

2.3.1 What is SARS eFiling?

SARS eFiling is an online platform provided by the SARS that enables taxpayers, tax practitioners, and businesses to interact with SARS in a secure and convenient digital environment. Through eFiling, users can:

- Register for various tax types (e.g., Income Tax, VAT, Pay As You Earn (PAYE).
- Submit tax returns and declarations.
- Make payments to SARS.
- Receive correspondence from SARS.
- Lodge disputes or request tax directives.
- Update taxpayer details.

The platform is a central digital point of access for SARS services, designed to promote efficient tax compliance, reduce the need for in-person visits, and enhance record-keeping.

2.3.2 What is SARS eFiling profile?

A SARS eFiling profile is the user account or digital identity created by a taxpayer or a tax practitioner on the SARS eFiling portal. It serves as the main interface for managing tax affairs online and consists of key elements:

- Username and password: Credentials used to log in.
- Linked tax reference numbers: Income Tax, VAT, PAYE, etc.
- User roles: e.g., individual taxpayer, registered representative, or tax practitioner.
- Security settings: Including email, mobile number, and two-factor authentication.
- User access rights: Permissions that allow users to submit returns, view correspondence, or make changes.

eFiling profiles can be created by individuals or legal entities and can include multiple users depending on the nature of the account (e.g., a company may have several authorized users).

2.3.3 How to obtain or register for SARS eFiling profile

To register for a SARS eFiling profile, taxpayers can visit the official SARS eFiling website at https://www.sarsefiling.co.za and Register. Taxpayers need to complete a registration form with their full name, ID or passport number, tax reference number (if available), contact details, and both physical and postal addresses. After setting up a username and password, SARS will send a OTP to their registered mobile number or email for identity verification. Once verified, the taxpayers will gain access to the eFiling dashboard where they can link tax products like Income Tax, VAT, or PAYE. Tax practitioners must include their registration number and can manage multiple client profiles through the “Manage Tax Types” feature. In some cases, SARS may require the taxpayer

to visit a branch for an in-person verification or to submit supporting documents, especially due to heightened fraud prevention measures.

2.3.4 SARS security and access controls

To prevent unauthorised access, SARS has implemented several measures:

- **2FA:** Required for login and profile updates.
- **EDNA system:** Used at SARS branches for biometric and identity verification.
- **Notification alerts:** Users receive alerts via SMS/email for profile changes.

However, as identified in this investigation, these measures have had varying degrees of effectiveness, especially where insider fraud, poor password practices, or phishing attacks occur.

2.3.5 Importance of eFiling profile integrity

The integrity of an eFiling profile is essential to protect taxpayer information and prevent:

- Unauthorised submission of returns.
- Fraudulent refunds.
- Misuse of sensitive personal and business information.
- Financial loss to both the taxpayer and the fiscus.

Understanding how eFiling profiles work is crucial for taxpayers, SARS, and the OTO to effectively identify weaknesses, improve systemic safeguards, and respond to fraud incidents.

2.3.6 Conclusion

eFiling is a vital part of the modern tax system. It enhances accessibility, improves efficiency and supports auto-assessments. These features befit both the fiscus and the taxpayer by streamlining tax compliance and reducing manual effort. For taxpayers, understanding how eFiling works is essential. It

not only helps ensure accurate and timely tax return submissions to SARS but also supports the integrity and security of the entire tax system.

2.4 SYSTEMIC INVESTIGATION AND ANALYTICAL FRAMEWORK

2.4.1 What is a systemic investigation?

Generally, section 16(1)(b) of the Tax Administration Act, 28 of 2011(TAA) makes provision for the Office of the Tax Ombud (OTO) to review at the request of the Minister or at the initiative of the OTO with the approval of the Minister, any systemic and emerging issue related to a service matter or the application of the provisions of the TAA, or procedural or administrative provisions of a tax Act.

The OTO has been receiving complaints and queries from taxpayers and industry bodies. Following a public workshop held with SARS, taxpayers and industry bodies on 13 June 2024 the OTO sought and obtained approval from the Minister of Finance on 12 August 2024, to conduct a review of possible systemic and emerging issues related to alleged SARS's service failures in assisting taxpayers with eFiling profile hijacking timeously in terms of section 16(1)(b) of the TAA.

In simple terms, a systemic investigation refers to an examination of underlying problems that affect or may affect multiple taxpayers within a tax system. These issues often pertain to how specific SARS systems operate, how policies, practices or procedures are formulated and implemented or how tax provisions are applied or disregarded by SARS. Even if the sample from which these issues are identified is small, what matters is the potential impact of the systemic issues raised.

2.4.2 Systemic investigations versus system investigations

The terms systemic investigation and system investigation are sometimes mistakenly used interchangeably, but they differ in scope and purpose:

Feature	Systemic Investigation	Systems Investigation
Definition	Investigates patterns or recurring issues affecting groups of taxpayers	Examines technical, IT, or administrative systems for security flaws or inefficiencies.
Focus	Root causes of repeated complaints, often linked to service, procedural, or administrative issues in application of a Tax act administered by SARS.	Technology infrastructure, digital controls, authentication systems, and IT operations.
Example in eFiling Hijacking	Repeated taxpayer inability to resolve hijacking incidents due to lack of clear SOPs.	Two-factor authentication flaws or poor password reset protocols in the eFiling system.
Responsibility	Tax Ombud (within its mandate, e.g. fairness, delay, poor communication)	Inspector-General or Auditor-General (technical/procedural enforcement, systems audits).

In this report, the OTO conducted a systemic investigation because the nature of complaints indicated structural vulnerabilities in eFiling profile registration, verification, and communication processes, rather than an isolated failure of the eFiling IT system.

2.4.3 How materiality informs systemic investigations

Materiality threshold plays a key role in assisting the OTO systemic investigation. It helps to determine whether a tax issue is serious or widespread enough to justify broader and formal inquiry. In this OTO investigation, the OTO determined that materiality threshold was met based on the following:

- A significant number of complaints from taxpayers and tax practitioners indicated a recurring problem.
- Reports of unauthorised changes to banking details and fraudulent refund claims pointed to systemic vulnerabilities in SARS eFiling system.
- Discussions with taxpayers, tax practitioners revealed widespread concerns regarding the ease with which security protocols could be bypassed, thereby eroding public trust in the SARS eFiling system.
- The estimated financial losses, even if small per incident but the cumulative effect was significant. For example, the OTO found that while many eFiling hijacking cases involved amounts below R10,000, the frequency and administrative burden they imposed met both the quantitative and qualitative materiality standards.

2.4.4 Conclusion

Materiality served as the foundation for initiating this OTO investigation, as it established that the problem was not isolated, but systemic in nature. It involved recurring patterns of fraud, service delivery failure by SARS and financial loss to the taxpayers who are victims of eFiling profile hijacking. Despite SARS implementing digital improvements during the course of the investigation, the continued occurrence of eFiling profile hijacking cases confirms that this issue remains materially significant.

3 METHODOLOGY

3.1 INVESTIGATIVE AND RESEARCH PROCESS

The investigation process into eFiling profile hijacking followed a structured, multi-method approach incorporating stakeholder engagements, empirical data collection, and systemic evaluation. Given the complexity of these fraud cases, the process prioritised understanding the root causes, systemic vulnerabilities, and institutional response mechanisms, ensuring a comprehensive analysis leading to actionable recommendations.

3.1.1 Triangulated investigation methodology

The investigation into alleged eFiling profile hijacking followed a structured, triangulated research methodology. This approach included:

- **Data collection through survey:** Gathering data from affected taxpayers and tax practitioners.
- **Case Study Analysis:** Case studies were selected from a broader pool of fraud related complaints received by the OTO; and
- **Stakeholder engagements:** Engagements were held with taxpayers, tax practitioners, Recognised Controlling Bodies (RCBs), South African Tax Practitioners United (SATPU), the South African Revenue Service (SARS), the Companies and Intellectual Property Commission (CIPC), Banking Association South Africa (BASA), Southern African Fraud Prevention Service (SAFPS).

3.1.2 Survey data analysis

The eFiling Profile Hijacking Survey, conducted by the OTO, aimed to assess the prevalence, impact, and resolution challenges faced by taxpayers experiencing fraud.

- **Survey Period:** Open between 3 February 2025 and 5 March 2025.
- **Responses:** 393 taxpayers participated.

- **Target Groups:** Individual taxpayers, corporate taxpayers, registered tax practitioners.

The survey instrument consisted of both closed and open-ended questions to extract quantitative trends and qualitative insights.

- **Closed-ended questions:** These questions provided measurable data on hijacking incidents, taxpayer awareness, and reporting trends.
- **Open-ended questions:** These questions uncovered deeper themes, including taxpayer frustrations, systemic weaknesses, and fraud enablers.

3.1.3 Case study analysis

Specific eFilling profile hijacking cases were selected from OTO cases to reflect a cross-section of taxpayer categories (individuals, practitioners, VAT vendors), types of compromise (OTP theft, banking updates, unauthorised refund claims), and complexity levels.

To substantiate the investigation, the report incorporated an analysis of real hijacking cases. The case study method was employed to illustrate:

- The modus operandi of fraudsters gaining unauthorised access to eFiling accounts.
- The sequence of fraudulent banking detail modifications leading to redirected taxpayer refunds.
- The effectiveness (or lack thereof) of SARS's intervention in individual cases.

Each case study was reviewed to extract patterns of fraudulent activity and identify where SARS's service and fraud mitigation strategies failed.

3.1.4 Stakeholder engagements

Qualitative Data was obtained through various stakeholder engagements. Targeted interviews and workshops with key stakeholders (e.g., tax

practitioners, SARS officials, digital security experts) assisted validate the emerging themes from the data.

The OTO conducted the following engagements with different stakeholders to obtain insights on this issue:

- Meeting with SATPU on 08 April 2024
    - The meeting was convened to discuss incidents of profile hijackings affecting several Tax Practitioners, as detailed by SATPU. It was alleged that these hijackings occurred over the 2024 Easter long weekend.
- Meeting with the RCBs on 18 April 2024
    - During the SARS and RCB National Operations meeting, SARS and OTO discussed the increase in eFiling profile hijacking cases.
- Public Engagement session on 13 June 2024
    - A public engagement session with about 305 participants provided additional insights into:
        - Taxpayer frustrations with SARS's delayed fraud resolution efforts.
        - Deficiencies in SARS's fraud detection mechanisms.
        - Poor communication practices, leaving victims without timely case updates.
- Meeting with SARS on 20 September 2024
    - The meeting served as an initial engagement to discuss the scope and gather information regarding the factual circumstances surrounding profile hijackings and how SARS addresses these cases.
- SARS / OTO executive leadership meeting on 09 October 2024
    - A quarterly meeting was held between SARS and OTO executive leadership to discuss various issues, including the hijacking of eFiling profiles.

- Meeting with Australian Tax Ombud on 02 December 2024
    - A meeting was held between South African Tax Ombud, Miss Yanga Mputa and Australian Tax Ombud, Ms Ruth Owen to gain insight and share best practices on the eFiling profile hijacking.
- Meeting with the BASA on 14 February 2025
    - A meeting was convened to discuss various issues related to eFiling profile hijacking and digital fraud.
- Meeting with the SAFPS on 26 February 2025
    - A meeting was held between OTO and SAFPS to discuss how taxpayers can protect themselves against digital fraud. The following was discussed:
        - Role of SAFPS in Fraud Prevention.
        - Consumer Protection Services.
        - Collaboration with SARS.
        - Consumer Awareness and Education.
- Public engagement for eFiling Profile Hijacking Survey feedback held on 28 May 2025.
    - A public engagement session with about 170 participants to share the results on the eFiling profile hijacking survey.

3.1.5 Investigation tools and data analysis techniques

The investigation employed a combination of qualitative and quantitative analysis:

- Descriptive Statistics were used to summarise hijacking trends and taxpayer experiences.
- Thematic Coding was applied to open-ended survey responses to identify recurring fraud patterns and taxpayer concerns.
- Comparative Case Study Analysis helped validate key themes identified in survey data.

Additionally, the investigation evaluated SARS's digital fraud reporting systems, identifying:

- Reliance on manual tracking via spreadsheets, leading to inefficiencies.
- Absence of a centralised case management system, exacerbating case resolution delays.
- Limited cross-divisional collaboration in fraud investigations.

The multi-layered investigation approach provided a comprehensive understanding of eFiling hijacking trends, taxpayer vulnerabilities, and SARS's systemic challenges. The findings emphasised the urgent need for operational reforms to improve fraud detection, case resolution, and taxpayer support mechanisms.

3.2 CONCLUSION

Given the complexity of these fraud cases, the investigation prioritised identifying root causes, systemic vulnerabilities and institutional response mechanisms. This comprehensive and multifaceted approach ensured a thorough analysis, leading to key findings and actionable recommendations, aimed at improving taxpayer protection and the integrity of the South African tax system.

4 UNDERSTANDING EFILING PROFILE HIJACKING

4.1 WHAT IS EFILING PROFILE HIJACKING?

eFiling profile hijacking refers to a scenario where a taxpayer's SARS eFiling profile is unlawfully accessed, taken over or manipulated by unauthorised persons. These unauthorised persons exploit weaknesses in the SARS eFiling system. This fraudulent activity often leads to significant financial losses, compromised personal data and administrative difficulties for the victims.

The simple example of eFiling profile hijacking is when fraudsters gain access to a taxpayer's SARS eFiling profile, once inside the profile, they change the taxpayer's personal details, change the taxpayer banking details to a bank account they control. After that, the fraudsters file a fraudulent tax return or wait for SARS to issue a refund. When SARS processes the refund, it is paid into the fraudster bank account not the real taxpayer's bank account. The real problem is that the taxpayer often doesn't know that this has happened until it is too late. In turn, SARS may hold the taxpayer liable for filing fraudulent tax return. As a result, it results into financial loss to the taxpayer, thereby breakdown of trust in the SARS eFiling system.

4.2 HOW EFILING PROFILE HIJACKING OCCURS?

Personal information can be stolen in various ways, including:

- **Physical theft**: Criminals may steal wallets, documents, or mail containing sensitive data.
- **Dumpster diving**: Fraudsters search through discarded documents to obtain valuable personal details.
- **Cybercrime**: The rise of digital technology has significantly increased identity fraud risks. Fraudsters use internet-based techniques, including phishing emails, spoofed websites, and malicious software, to extract confidential information.
- **Social engineering**: Scammers manipulate individuals into revealing sensitive details through social media interactions, fake customer service calls, or fraudulent SMS messages.

4.3 TYPES OF EFILING PROFILE HIJACKING

- **Phishing Scams**: Fraudsters send emails or messages impersonating legitimate organisations, urging victims to click on fraudulent links and enter personal information. These scams often mimic government agencies or banks to appear credible. SARS will never ask for taxpayers' eFiling details, passwords, or credit/debit card information via email or phone.
- **Tax Refund Scams**: Criminals use stolen identities to file fraudulent tax returns, claiming refunds they are not entitled to. Additionally, they may alter banking details on eFiling profiles to redirect legitimate refunds into fraudulent accounts.
- **Identity Theft for Financial Gain**: Fraudsters impersonate victims by using their personal details to access financial accounts, apply for loans, or conduct transactions under their names. Victims may be left responsible for debts they did not incur.
- **Fake SARS Officials**: Scammers pose as SARS officials, falsely claiming that the victim is due a refund or under investigation. They may send fraudulent letters or contact businesses pretending to be auditors, pressuring them into providing confidential financial information.

4.4 TAXPAYER VULNERABILITIES

Taxpayers face several vulnerabilities that increase the risk of eFiling profile hijacking. These weaknesses stem from systemic challenges, security gaps, and taxpayer behaviour. Key factors contributing to their susceptibility include:

4.4.1 Weak authentication measures

Many taxpayers rely on basic login credentials without two-factor authentication, making it easier for fraudsters to gain unauthorised access. The lack of biometric verification or additional authentication steps creates opportunities for criminals to exploit stolen credentials.

4.4.2 *Phishing and social engineering attacks*

Fraudsters commonly trick taxpayers into revealing login details through phishing emails, SMS scams, or fake SARS websites. Taxpayers often unknowingly provide personal information or OTPs (One-Time Pins) to cybercriminals, allowing unauthorised profile access.

4.4.3 *Reuse of weak passwords*

Many taxpayers use predictable passwords or reuse passwords across multiple platforms, making it easier for hackers to compromise accounts, especially after a data breach from another service.

4.4.4 *Limited awareness of digital security threats*

Despite growing incidents of identity fraud, many taxpayers remain unaware of best practices for securing their eFiling accounts. A lack of regular password updates, failure to check for unauthorised transactions and insufficient monitoring of suspicious activity leave profiles vulnerable.

4.4.5 *Insider threats and third-party access*

Some taxpayers share login details with tax practitioners, family members, or fraudsters posing as SARS officials. If these credentials fall into the wrong hands, profile hijacking becomes easy, with criminals able to manipulate banking details and file fraudulent tax returns.

4.4.6 *Inadequate banking verification controls*

Fraudsters exploit loopholes in SARS and banking security measures, such as weak verification processes for new bank account registrations. Without stringent identity validation, criminals can replace legitimate taxpayer banking details with fraudulent accounts.

4.4.7 *Data breaches and dark web exposure*

A significant number of taxpayers do not use official SARS channels to access their eFiling profiles, opting instead for insecure platforms. Additionally,

widespread data breaches at various organisations expose private information on the dark web. Many individuals reuse passwords across multiple platforms, meaning that a breach in one system can compromise accounts elsewhere. Clicking on phishing links in emails, SMS messages, or WhatsApp messages further increases fraud risks.

4.4.8 Poor device and network security

Many taxpayers fail to secure their devices, lacking firewalls, antivirus software, or regular system updates. Public Wi-Fi use further increases risk, making taxpayer login credentials more susceptible to interception.

4.5 HOW CAN TAXPAYERS PROTECT THEMSELVES FROM EFILING PROFILE HIJACKING?

eFilling profile hijacking can have serious consequences, including fraudulent tax filings and financial loss. To safeguard taxpayers' personal information and prevent unauthorised access to taxpayers' tax profile, it is essential to adopt secure practices and remain vigilant against potential threats.

4.5.1 Recognising and avoiding phishing scams

Fraudsters often attempt to steal personal information by impersonating legitimate institutions like the SARS. It is crucial to recognize that SARS will never request banking details, credit card information, or personal financial data via post, email, or SMS. Additionally, SARS will never send hyperlinks directing taxpayers to other websites. If you receive any unsolicited requests for sensitive data, do not respond or click on any links—these may be phishing attempts aimed at harvesting taxpayer credentials.

4.5.2 Ensuring secure online transactions

When interacting online, always verify that you are using a legitimate and secure website. A secure connection will have a URL that starts with HTTPS, where the "S" denotes security encryption. Look for the lock icon in the address bar and click on it to verify security details. Fraudsters can create fake websites

that mimic legitimate ones, so it is important to test the lock icon and confirm the website's authenticity before entering any information.

4.5.3 Safeguarding personal information

Taxpayers' identity documents, including taxpayers' ID Books, Passports and bank statements should be kept in a secure location. When disposing of financial or personal records, always shred them to prevent unauthorised access. Criminals can use discarded documents to impersonate individuals and commit fraud.

4.5.4 Strengthening device security

Taxpayers' computer and mobile devices should be protected by firewalls, anti-virus software, and regular security updates. Ensure that all security patches are installed promptly to mitigate potential vulnerabilities. Additionally, using screen locks and biometric authentication (such as fingerprint or facial recognition) can prevent unauthorised access when devices are unattended.

4.5.5 Using strong passwords and enhancing digital security

Passwords play a critical role in securing taxpayers accounts. Use strong, complex passwords that include a combination of letters, numbers, and symbols. Avoid using easily guessed passwords or reusing passwords across multiple accounts. Additionally, it is recommended to change taxpayers' passwords monthly and enable multi-factor authentication wherever possible.

4.5.6 Securing social media profiles

Social networking platforms can be exploited by criminals seeking personal information. It is advisable to tighten taxpayers' privacy settings to restrict access to taxpayers' profile and personal details. Be cautious about sharing sensitive information on public forums, as fraudsters can use these details to impersonate you.

4.5.7 Monitoring credit records and fraud alerts

Checking taxpayers credit record annually helps identify unauthorised accounts or transactions. If you suspect fraudulent activity, register with the SAFPS to prevent further abuse of taxpayers' identity. If taxpayers' ID or passport has been stolen, this registration can serve as an additional safeguard.

4.5.8 Reporting suspicious activity

If a taxpayer encounters potential fraud or phishing scams, the taxpayer must report to the SARS Fraud and Anti-Corruption Hotline (0800 00 2870) or email phishing@sars.gov.za. Timely reporting of suspicious activity can help prevent further fraud and assist authorities in tracking down criminals. By taking proactive security measures, taxpayers can significantly reduce their risk of falling victim to profile hijacking. Vigilance, strong password management, and secure online practices are essential to safeguarding personal financial information and preventing identity fraud.

4.6 CONCLUSION

In conclusion, eFiling profile hijacking involves criminals using stolen personal information to fraudulently submit tax returns and claim tax refund from SARS. It is crucial for taxpayers to be aware of the threat of eFiling profile hijacking, as it can lead to financial loss, compromised personal data and significant administrative burdens. To mitigate these risks, taxpayers are encouraged to protect their personal data, use secure authentication methods and to be vigilant during the risk period of the SARS tax filing season and file their tax returns on time to reduce exposure to potential fraud.

5 CASE STUDIES

This report examines seven carefully selected cases from the broader pool of fraud-related complaints received by the OTO. These cases were chosen due to their direct relevance to eFiling Profile hijacking, a growing concern in digital tax administration. The selection process prioritised cases that exemplify systemic vulnerabilities, recurring fraud patterns, and the direct impact on taxpayer trust and financial security.

The significance of these cases lies in their ability to illustrate critical weaknesses in authentication protocols, fraud detection mechanisms, and SARS's response strategies. By focusing on a subset of six cases, this investigation aims to provide a detailed and manageable analysis, ensuring that key insights are thoroughly explored without being diluted by an overwhelming volume of data.

eFiling profile hijacking poses severe risks to taxpayer security, allowing fraudsters to manipulate taxpayer details, redirect refunds, and engage in unauthorised transactions. The analysis of these cases forms a crucial part of the investigative methodology, helping to identify recurring fraud tactics, assess SARS's response effectiveness, and formulate recommendations for stronger fraud prevention measures. Through this focused examination, the report seeks to contribute to policy discussions on enhancing digital security controls and improving taxpayer protection against digital fraud.

5.1 CASE STUDY 1: FRAUDULENT COMPROMISE OF TAXPAYER'S EFILING PROFILE

5.1.1 Background

In August 2023, a taxpayer's eFiling profile was unlawfully accessed and compromised. On 17 August 2023, fraudulent income tax returns for the 1999 and 2023 assessment years were submitted to the SARS, reflecting fraudulent new banking details. The fraudulent assessment resulted in a refund amounting to R23,576.10.

5.1.2 Initial SARS intervention

Upon identifying discrepancies, SARS initiated a bank account exception case, requesting that the taxpayer verify their banking details. However, this case was cancelled on the same day, with an internal note stating, "New Bank Details Verifications Received", despite no new bank details or supporting documentation being provided to substantiate the fraudulent bank account information.

5.1.3 Subsequent banking detail verification attempts

On 21 August 2023, SARS opened a second bank account exception case, again requesting banking detail verification. The taxpayer updated their banking information to a correct banking account and submitted substantiating proof to SARS on 23 August 2023. However, the taxpayer did not provide an image of themselves holding their proof of identity, as required by SARS. Despite this, on 24 August 2023, the bank account exception case was cancelled, with the notation "New Bank Details Received". As a result:

- The correct banking details were not updated in SARS's system.
- The unverified bank account remained linked to the taxpayer's profile.
- On 29 August 2023, SARS processed the refund of R23,576.10 into the fraudulent bank account.

5.1.4 *Reporting of fraud case to SARS and investigation*

The taxpayer reported suspicious activity on their eFiling profile to the SARS Digital Crime Investigation Unit on 08 July 2024. While SARS acknowledged the report and initiated an investigation, it only placed a stopper on the taxpayer's account on 11 December 2024—five months after the fraudulent activity had been reported. This delay contributed to prolonged financial uncertainty for the taxpayer.

5.1.5 *Escalation to the OTO*

On 17 July 2024, frustrated by the lack of resolution, the taxpayer lodged a complaint with the SARS Complaints Management Office (CMO), highlighting concerns over unauthorised banking detail modifications and misallocated refunds. Due to persistent delays and lack of response from the CMO, the taxpayer escalated the issue to the OTO.

5.1.6 *Case resolution*

Following a review, the OTO accepted the complaint and recommended to SARS the following:

- Address the fraudulent activities impacting the taxpayer's eFiling profile.
- Provide a resolution regarding the unauthorised refund transaction.

The SARS Digital Crime Investigation Unit concluded its investigation on 04 February 2025, confirming that fraud had occurred. As a result, the taxpayer's SARS account was reimbursed to correct the fraudulent payment transaction.

5.1.7 *OTO's observations*

On 07 February 2025, the misappropriated refund of R23,576.10 was reimbursed to the taxpayer's legitimate bank account. However, throughout the investigation:

- The taxpayer received no formal updates or estimated timeframes regarding case progress.
- Despite repeated follow-ups, SARS failed to provide status reports, exacerbating frustration.
- The investigation spanned approximately seven months (approximately 213 days) before reaching a final resolution.

The OTO recognises the critical role of comprehensive investigations while emphasising the taxpayer's entitlement to procedural fairness, transparency, and prompt updates. The extended resolution timeframe underscores the pressing need for improved fraud case management protocols and more effective engagement strategies within SARS.

5.1.8 Conclusion

This case illustrates significant inefficiencies within SARS's fraud prevention and resolution mechanisms. Delays in fraud response, inadequate banking verification, poor communication, and manual case tracking contribute to systemic failures in taxpayer protection.

5.2 CASE STUDY 2: FRAUDULENT MODIFICATION OF TAXPAYER REPRESENTATION AND VAT REFUND MISAPPROPRIATION

5.2.1 Background

On 20 April 2023, the sole director of a company was fraudulently changed at the CIPC. Subsequently, on 15 June 2023, the registered taxpayer representative was illegitimately updated at SARS, granting the perpetrator unauthorised access to the taxpayer's eFiling profile. This unauthorised access allowed the perpetrator to:

- Alter the registered taxpayer details, including banking information.
- Submit fraudulent tax returns, resulting in the misappropriation of VAT refunds.

Upon discovering these unauthorised changes, the taxpayer reported the matter to SARS on 30 June 2023, submitting the RSN01(Reported Suspicious Non-compliance) form as part of their fraud report.

5.2.2 Fraudulent transactions and unauthorised SARS payments

Despite the fraud being formally reported, SARS processed fraudulent VAT refunds before corrective action was taken:

- R43,742.76 for the 05/2023 VAT period, paid on 28 June 2023 into the perpetrator's bank account.
- R416,639.89 for the 06/2023 VAT period, paid on 6 July 2023, again into the perpetrator's bank account.

The failure by SARS to place a stopper on the fraudulent transactions resulted in the taxpayer suffering significant financial losses.

5.2.3 Compliance consequences and SARS actions

The taxpayer's representation was correctly updated in SARS's system on 27 July 2023. However, the fraudulent transactions triggered compliance-related repercussions:

- On 01 August 2023, SARS selected the 06/2023 VAT period for verification and issued an additional assessment on 29 January 2024, resulting in a tax liability of R490,764.26.
- On 03 August 2023, SARS selected the 05/2023 VAT period for verification and issued an additional assessment on 29 January 2024, resulting in a tax liability of R52,910.96.
- These assessments negatively impacted the taxpayer's compliance status. Subsequently, SARS:
- SARS issued a final demand letter on 06 February 2024.
- This was followed by a third-party appointment on 21 February 2024 against the taxpayer.

5.2.4 Taxpayer's response and escalation to the OTO

Recognising the fraudulent nature of the VAT filings, the taxpayer:

- Lodged an objection on 22 February 2024, arguing that the VAT returns were fraudulently submitted.
- Filed a complaint with the SARS CMO on 06 May 2024. Despite the prescribed 21-business-day resolution timeframe, the CMO failed to resolve the matter.
- Requested a suspension of payment on 22 August 2024, which SARS approved on the same day.

5.2.5 Case resolution

Due to prolonged delays, the taxpayer escalated the case to the OTO on 30 August 2024. Upon review, the OTO issued formal recommendations, advising SARS to:

- Provide an outcome on the taxpayer's fraud report submitted on 30 June 2023.
- Resolve the matter or provide valid justification for non-resolution.

Following intervention by the OTO, SARS finalised the fraud investigation:

- On 02 October 2024, SARS ruled in favour of the taxpayer regarding their objection.
- On 22 November 2024, SARS completed its investigation and issued a Suspicious Activity Report Finalisation Letter, confirming that fraud had occurred.
- SARS updated the taxpayer's account, correcting fraudulent transactions and restoring hijacked refunds.
- The OTO officially finalised the complaint on 23 January 2025, marking the resolution of the case.

5.2.6 OTO's observations

Intervention by the OTO was necessary to finalise resolution. However, throughout the investigation

- Profile hijacking occurred through possible fraudulent changes at CIPC which impacted SARS systems, compromising taxpayer information.
- Unauthorised access to the eFiling profile led to the submission of fraudulent VAT returns and the theft of refunds. This resulted in SARS paying a total amount of R460,389.65 to a fraudulent bank account.
- SARS delayed in blocking fraudulent transactions despite early reports of fraud, causing significant undue hardship to the taxpayer. The taxpayer's tax compliance status was adversely affected pending the finalisation of the investigation, and in addition SARS initiated debt recovery proceedings.
- Slow correction of taxpayer details prolonged exposure to fraud risks.

5.2.7 Conclusion

This case study underscores critical inefficiencies in SARS's fraud detection, authentication protocols, and resolution mechanisms. Without immediate enhancements to fraud prevention frameworks, refund monitoring, and taxpayer communication, fraudulent activities will continue to compromise taxpayer security and financial stability. SARS must take proactive measures to

reinforce fraud safeguards, ensuring taxpayers receive swift, transparent, and effective resolutions.

5.3 CASE STUDY 3: DIGITAL FRAUD INVESTIGATION ON TAXPAYER'S EFILING PROFILE

5.3.1 Background

On 07 June 2024, a taxpayer visited a SARS branch to update their banking details. During the process, SARS officials discovered multiple bank accounts linked to the taxpayer's profile within the SARS system. Shortly thereafter, upon accessing their eFiling profile, the taxpayer encountered a notification stating the following: "*Refund status: Your profile has been flagged for investigation by the Digital Fraud Unit*." Concerned by this alert, the taxpayer contacted SARS telephonically on 28 August 2024 to seek clarification. SARS advised the taxpayer to submit supporting documentation for the fraud case, which was duly provided on 09 and 10 September 2024.

5.3.2 Escalation of the case

Despite providing supporting documentation, the taxpayer experienced prolonged delays in fraud resolution and non-payment of their refund. As a result, the taxpayer lodged a formal complaint with the SARS CMO on 30 September 2024. However, despite the prescribed 21-business-day resolution timeframe, the SARS CMO failed to resolve the matter.

5.3.3 Case resolution

Frustrated by the lack of progress, the taxpayer escalated the complaint to the OTO on 28 October 2024. Upon evaluation, the OTO formally accepted the complaint on 29 November 2024 and issued recommendations to SARS, as follows:

- The digital fraud investigation be expedited.
- The taxpayer should receive a formal case outcome.
- The refund, if deemed payable, be processed into the correct bank account.

Following OTO's recommendations, SARS completed its digital fraud investigation on 3 February 2025, confirming that:

- The taxpayer's eFiling profile had been secured.
- The banking details were updated to reflect the taxpayer's legitimate account.

On 29 January 2025, SARS processed and paid out the taxpayer's income tax refund of R10,594.42 into their registered bank account. The OTO finalised the complaint on 6 February 2025, marking the resolution of the case.

5.3.4 OTO's observations

- The taxpayer's eFiling profile was compromised with multiple unauthorised bank accounts linked, triggering a digital fraud investigation.
- Despite early detection in June 2024, SARS's investigation and resolution processes were significantly delayed, causing refund payment delays.
- The case exposes systemic inefficiencies in SARS's fraud detection, investigation, and communication, underscoring the need for improved controls and timely resolutions.

5.3.5 Conclusion

This case study highlights significant systemic inefficiencies within SARS's fraud detection, investigation, and resolution mechanisms. The delayed response, poor communication, and reliance on external interventions reflect broader patterns observed in eFiling hijacking cases. To restore taxpayer trust and operational efficiency, SARS must prioritise the implementation of proactive fraud detection systems, structured case resolution frameworks, and enhanced transparency protocols. By addressing weak authentication controls and prolonged investigation timelines, SARS can significantly improve taxpayer protection and digital security in eFiling transactions.

5.4 CASE STUDY 4: FRAUDULENT UPDATE OF TAXPAYER'S REGISTERED PARTICULARS ON EFILING

5.4.1 Background

On 03 August 2021, the taxpayer received an email notification from SARS stating that their registered particulars had been updated, despite not having initiated any changes. Subsequently, on 12 August 2021, a fraudulent income tax return for the 2021 assessment year was submitted on the taxpayer's profile. SARS processed a refund of R21,662.38 on 14 August 2021, paying the amount into a fraudulent bank account controlled by the perpetrator.

5.4.2 Taxpayer's attempt to rectify the issue

On 19 November 2021, the taxpayer contacted SARS telephonically to update their eFiling security details, to secure their profile. Later, on 2 February 2022, the taxpayer's tax practitioner attended a virtual meeting with SARS, where SARS provided instructions on formally reporting the fraudulent activity via its website, accompanied by supporting documentation. On 10 May 2022, the taxpayer lodged a formal complaint with the SARS CMO regarding the fraudulent modifications linked to their tax number. However:

- The CMO finalised the complaint on 24 March 2023, but failed to address the taxpayer's concerns, as SARS referenced a refund paid for the 2022 tax year, rather than resolving the fraud related to the 2021 tax year.
- SARS attempted to recall the fraudulently paid refund on 13 April 2023, but no available funds were found in the perpetrator's account.

5.4.3 Escalation to the OTO

Due to dissatisfaction with SARS's handling of the matter, the taxpayer escalated the complaint to the OTO on 29 September 2023. Upon review, the OTO formally accepted the case on 3 October 2023, issuing a recommendation advising SARS to:

- Finalise the fraud investigation.
- Communicate the investigation outcome to the taxpayer.

On 08 May 2024, the taxpayer submitted an RSN01 form, along with supporting documentation, reporting the unresolved suspicious activity linked to their tax number. Consequently, SARS proceeded to place a stopper on the income tax account there freezing all subsequent valid refunds from other periods from being paid out pending investigation.

5.4.4 Case resolution

Following further investigation, SARS finalised the digital fraud case on 13 November 2024, ruling in favour of the taxpayer. As part of corrective actions:

- The taxpayer's eFiling profile was secured.
- The taxpayer's correct banking details were reinstated.
- On 24 January 2025, SARS issued a refund of R71,154.73 to the taxpayer's registered bank account. This amount included R21,662.38 from the 2021 tax period, which was paid along with other outstanding refunds from different periods.

The OTO officially finalised the complaint on 31 January 2025, marking the resolution of the case.

5.4.5 OTO's observations

- The taxpayer's eFiling profile was fraudulently accessed and changed in August 2021, leading to an unauthorised refund of R21,662.38.
- The taxpayer contacted SARS in November 2021 to update eFiling security details and formally reported the fraud in February 2022, but the process was slow and guidance from SARS was unclear.
- SARS incorrectly focused on the 2022 tax year, ignoring the actual fraudulent activity that occurred in the 2021 tax year.
- A formal complaint lodged in May 2022 was only finalised in March 2023, with no resolution and failed attempts to recover the funds.
- This issue also impacted other income tax periods, leading to refunds being withheld pending a lengthy investigation. The investigation took nearly nine months to finalise, which adversely affected the taxpayer.

5.4.6 Conclusion

This case illustrates systemic deficiencies within SARS's fraud detection, taxpayer security, and refund recovery processes. The delayed response, ineffective case resolution, and inability to recall fraudulent refunds highlight critical weaknesses in SARS's fraud mitigation strategy. To restore taxpayer confidence, SARS must:

- Implement stronger authentication measures for eFiling security.
- Ensure timely fraud response and structured case resolution frameworks.
- Improve banking detail verification to prevent unauthorised changes.
- Enhance cross-sector collaboration with financial institutions for fraud prevention.
- Without urgent reforms, taxpayers will continue to face long-standing financial risks, fraud vulnerabilities, and unresolved complaints. Strengthening fraud response and preventative measures will be key to improving taxpayer trust in SARS's security framework.

5.5 CASE STUDY 5: FRAUDULENT EFILING REGISTRATION AND UNAUTHORISED TAX RETURNS

5.5.1 Background

Between 2012 and 2025, a taxpayer's income tax number was fraudulently used to register multiple eFiling profiles without the taxpayers' knowledge. This unauthorised registration resulted in the submission of fraudulent tax returns, misallocated refunds, and compliance challenges for the legitimate taxpayer.

5.5.2 Unauthorised eFiling registrations and tax return submissions

To authenticate the taxpayer's eFiling profile, SARS requested supporting documents multiple times between 2014 and 2019. However, there was no indication that these documents were submitted or processed. Fraudulent income tax returns were later submitted under the taxpayer's profile:

- 2015 Income Tax Return: Fraudulently filed on 05 February 2016.
- 2016 Income Tax Return: Fraudulently filed on 05 July 2016.

SARS paid the following fraudulent refunds:

- 1 November 2012: Refund of R1,554.42.
- 1 September 2014: Refund of R10,521.41.
- 18 February 2016: Refund of R10,546.87.

Following the payment of the fraudulent refunds, SARS selected the 2016 return for verification on 07 July 2016. SARS requested supporting documentation and finalised the verification on 14 November 2016, adjusting medical aid contributions accordingly. Similarly, SARS selected the 2015 tax return for audit on 31 March 2017, requesting documentation on 01 June 2017. Due to non-submission, the audit was finalised on 12 July 2017, adjusting medical scheme tax credits accordingly.

5.5.3 Discovery of fraudulent activity and taxpayer's actions

SARS attempted to contact the legitimate taxpayer regarding outstanding tax debt. After multiple unsuccessful attempts, SARS managed to reach the taxpayer, who then suspected fraudulent activities related to their tax number. On 01 July 2020, the taxpayer reported suspicious activities to SARS, stating that they had never received refunds. The taxpayer further indicated that they did not hold a fraudulent Bank 2 bank account, into which the refunds had been deposited. However, SARS's system automatically cancelled the fraud case, leading to delayed intervention and failure to address the issue in time. On 06 July 2020, the taxpayer submitted a request for dispute condonation, citing fraud in their 2015 income tax return. However, SARS declined the request on 12 August 2020, stating that:

- The taxpayer had already been informed of their outstanding tax debt.
- The taxpayer was registered on eFiling, and the refund was paid directly into their account.
- No exceptional circumstances were provided to justify the request.

5.5.4 Escalation to the OTO

On 23 November 2021, the taxpayer submitted 2017-, 2018-, and 2019-income tax returns. On the same day, SARS selected the 2017 return for verification, requesting supporting documents, which the taxpayer submitted on 2 December 2021. The verification was finalised on 07 December 2021, with SARS disallowing business expenses claimed. On 09 February 2024, the taxpayer submitted a request for suspension of payment along with a request for dispute condonation, citing fraud related to the 2017 tax return. SARS approved the dispute condonation request on 12 February 2024, allowing the objection and issuing a revised assessment. However, dissatisfied with SARS's delays in fraud case resolution, the taxpayer lodged a complaint with the SARS Complaints Management Office (CMO) on 12 February 2024. Despite the prescribed 21-business-day resolution timeframe, SARS CMO failed to resolve the matter, leading the taxpayer to escalate the complaint to the OTO.

5.5.5 *Case resolution*

Upon review and evaluation, the OTO formally accepted the complaint on 27 September 2024, recommending that SARS finalise the fraud case reported on 01 July 2020 and provide the taxpayer with an outcome or valid reasons for non-resolution. On 13 March 2025, SARS finalised the fraud investigation, confirming that the case was resolved in favour of the taxpayer. As a result:

- The taxpayer's profile was updated to correct fraudulent modifications.
- Adjustments were made to reverse hijacked payments.

The OTO formally finalised the complaint on 01 April 2025, marking the resolution of the case—nearly five years after the fraud was initially reported.

5.5.6 *OTO's observations*

- The taxpayer's income tax number was fraudulently used to create multiple eFiling profiles between 2012 and 2025, resulting in unauthorised tax returns and misallocated refunds.
- The fraudster exploited SARS's payment threshold, causing SARS to pay refunds before later requesting supporting documents, which were never submitted or processed.
- Fraudulent returns for 2015 and 2016 triggered refunds totalling over R22,000 paid into a fraudulent bank account.
- Despite the taxpayer reporting the fraud in July 2020, SARS's system prematurely closed the case, and the dispute condonation request was incorrectly denied.

5.5.7 *Conclusion*

This case highlights the urgent need for systemic fraud prevention enhancements within SARS's taxpayer verification, fraud detection, and refund recovery mechanisms. The extended delays, weak authentication protocols, and communication failures reinforce the necessity for structured fraud resolution frameworks. To restore taxpayer trust, SARS must implement proactive fraud

detection controls, expedite resolution processes, and strengthen security measures to ensure taxpayer protection and data integrity.

5.6 CASE STUDY 6: UNAUTHORISED ONE-TIME PIN (OTP) AND EFILING PROFILE FRAUD

5.6.1 Background

On 19 March 2024, a taxpayer contacted SARS regarding a OTP that the taxpayer received despite not submitting any service request. The taxpayer noted that similar unauthorised OTP requests had occurred previously, raising concerns about potentially fraudulent activity. On 04 July 2024, SARS auto-assessed the taxpayer for the 2024 tax year. Subsequently, on 16 July 2024, the taxpayer attended an e-booking appointment with SARS to update their banking details to the correct bank account, while removing fraudulent banking details that had been linked to their profile without authorization.

5.6.2 Identification of fraudulent activity

On 31 July 2024, the taxpayer reported suspicious activities linked to their income tax number to SARS. SARS requested supporting documents, which the taxpayer submitted the same day. However, shortly afterward, the taxpayer discovered that their banking details had been fraudulently altered again on their eFiling profile. To rectify the issue, the taxpayer visited a SARS branch on 18 September 2024, where they updated their banking details to reflect the correct information.

5.6.3 Escalation to the OTO

Due to SARS's failure to resolve the matter promptly, the taxpayer lodged a complaint with the SARS CMO on 30 September 2024, citing delays in addressing the fraud case. Despite the prescribed 21-business-day resolution timeframe, the CMO failed to resolve the complaint, forcing the taxpayer to escalate the matter further.

5.6.4 Case resolution

On 28 October 2024, the taxpayer sought assistance from the OTO, which accepted the case for review on 31 October 2024. The OTO issued formal recommendations, to SARS as follows:

- Finalise the digital fraud investigation.
- Determine whether the refund was payable.
- Ensure any applicable refund was paid into the legitimate bank account updated by the taxpayer.

Following OTO's intervention, SARS finalised the fraud case on 14 March 2025, securing the taxpayer's eFiling profile and updating banking details to the correct account. As a result:

- On 19 March 2025, SARS processed and paid a refund of R8,137.35 into the taxpayer's correct registered bank account.
- On 26 March 2025, the OTO officially closed the complaint, confirming case resolution.

5.6.5 OTO's observations

- The taxpayer received multiple unauthorised OTPs, raising early suspicion of eFiling profile fraud.
- Despite attempts to correct banking details at a SARS branch, the profile was repeatedly compromised.
- SARS failed to resolve the issue promptly, leading the taxpayer to escalate the matter.

5.6.6 Conclusion

This case highlights critical weaknesses in SARS's fraud detection mechanisms, banking security protocols, and case resolution frameworks. The unauthorised receipt of OTPs, repeated banking detail fraud, and delayed case investigation illustrate systemic inefficiencies that leave taxpayers vulnerable to identity theft. To enhance taxpayer security and fraud response, SARS must strengthen authentication measures, improve fraud case management, and ensure proactive resolution frameworks to restore public trust and operational efficiency in eFiling transactions.

5.7 CASE STUDY 7: FRAUD AND SIMULATED STOPPER

5.7.1 Background

On 29 January 2025, an email from SARS indicated that an unknown individual had requested access to a company's tax profile. The request was not authorised, and the individual was unknown to the company. On 31 January 2025, the company's tax practitioner reported being unable to access the eFiling profile. A case of fraud was reported to SAPS, and an affidavit was submitted. SARS was contacted via the call centre and email, and a case number was assigned.

5.7.2 Initial SARS intervention

On 01 February 2025, SAPS confirmed the case and assigned an investigator. After multiple follow-ups with SARS, the security contact details were corrected on 25 February 2025.

5.7.3 Reporting and investigation

Between 07 and 08 March 2025, tax profiles of the company were removed from the authorised users' eFiling profiles without notice. An unauthorised bank account was added to the company's profile and subsequently deleted. From 08 to 12 March 2025, security contact details were again fraudulently altered. On 12 March 2025, a formal fraud case was submitted to SARS for the company profile, and a fraudulent VAT claim of R689,000 was submitted. SARS acknowledged receipt of the fraud report. Attempts to book a SARS appointment were unsuccessful, with the earliest available date being 30 April 2025. SARS further failed to place a stopper on the VAT account. Despite the fraud report and affidavit submitted the previous day, the fraudulent VAT claim was purportedly paid out to an unknown account on 13 March 2025. On 14 March 2025, access to the VAT profile was regained, and the fraudulent submission was discovered. A correction was submitted, replacing the fraudulent return with the correct VAT return (R401,846.67 payable by the taxpayer). Between 31 March and 04 April 2025, multiple unauthorised access requests were received. The SARS system did not allow for proper review or

rejection of these requests. From 04 to 07 April 2025, the eFiling profile was again locked out due to unauthorised changes, and the profile was hijacked for the third time. On 07 April 2025, a fraudulent VAT claim was submitted. Contacting the SARS call centre resulted in a referral to the fraud department but attempts to reach the fraud department were unsuccessful. On 08 April 2025, assistance was again provided in restoring the profile and updating the password. This was the third instance of rectifying the profile due to fraudulent changes.

5.7.4 Escalation to the OTO

On 07 April 2025, the OTO was contacted to report the eFiling profile hijacking. On 17 April 2025, OTO sent recommendations to SARS, urging them to assist urgently in securing the taxpayer's eFiling profile to prevent further fraudulent activities and to finalise the digital fraud investigation. On 16 May 2025, concerns about the profile being hacked again were raised with OTO. On the same day, OTO phoned SARS, and SARS confirmed the following:

- A stopper was placed on the taxpayer account on both 30 April 2025 and 16 May 2025 after OTO contacted SARS. On close inspection by the OTO, it was however found that SARS simulated a stopper on the account on 30 April 2025, and that the stopper was only approved on 16 May 2025.
- A first payment was made on 12 March 2025, and a second payment was made on 07 April 2025.
- On 08 May 2025, there was a change of particulars on the taxpayer profile.

5.7.5 Case Resolution

The case has not been finalised by SARS and remains open with the OTO.

5.7.6 OTO's Observations

- Multiple instances of fraudulent activity were identified on the eFiling profile.
- Despite reporting the fraud and submitting affidavits, fraudulent claims were paid out by SARS.

- The SARS system failed to prevent unauthorised access and changes to the profiles.
- SARS placed stoppers on the taxpayer account, but fraudulent activities continued to occur.
- The investigation and resolution of the fraud cases were delayed due to workload and system inefficiencies.
- One of the system inefficiencies is the delay by SARS in approving the simulated stopper, which has allowed fraudulent activities to persist.

5.7.7 Conclusion

This case highlights significant vulnerabilities within the SARS eFiling system, which allowed multiple instances of fraudulent activity to occur despite repeated interventions. The taxpayer faced ongoing challenges in securing their tax profiles, with unauthorised changes and fraudulent claims being submitted and paid out. The involvement of the OTO brought some relief, but systemic inefficiencies and delays in addressing the fraud cases persisted. This situation underscores the need for robust security measures and efficient fraud detection mechanisms within SARS to protect taxpayers from similar incidents in the future.

5.8 KEY FINDINGS FROM CASE STUDIES

The analysis of multiple case studies highlights systemic challenges in SARS's fraud prevention, detection, and response mechanisms. These cases expose vulnerabilities in authentication protocols, inadequate fraud prevention measures, delayed investigative processes, and weak security controls for taxpayer profile modifications. Furthermore, the absence of a structured fraud case management system exacerbates the inefficiencies, leaving affected taxpayers financially vulnerable. This summary presents the key findings and recurring themes across the analysed cases.

5.8.1 Inadequate fraud prevention measures

- SARS lacks proper verification mechanisms for banking detail changes, enabling unauthorised refund transactions.
- Fraudsters exploit weaknesses in profile authentication to alter taxpayer representation details without validation.
- The absence of proactive fraud alerts allows suspicious modifications to bypass security checks.

5.8.2 Delayed response to fraudulent activity

- Investigation timelines are excessively prolonged, with some cases taking years to resolve.
- Despite early fraud reports, SARS often fails to act immediately, allowing continued financial harm.
- Escalation to external oversight bodies, such as the OTO, is frequently required to secure resolutions.

5.8.3 Authentication failures and security gaps

- Weak authentication protocols permit fraudulent taxpayer registrations and eFiling profile hijacking.
- Unauthorised one-time passwords (OTPs) indicate security vulnerabilities within SARS's identity verification framework.
- Attempts to manually correct fraudulent banking details are ineffective, as unauthorised modifications persist.

5.8.4 *Poor communication and case management deficiencies*

- Taxpayers receive limited or no updates on fraud investigations, leading to uncertainty and frustration.
- The reliance on manual tracking methods, such as spreadsheets, contributes to unresolved fraud cases.
- SARS's CMO frequently closes cases without addressing core fraud concerns.

5.8.5 *Compliance and debt collection consequences*

- Fraudulent VAT returns trigger compliance penalties, final demand letters, and aggressive debt collection measures against affected taxpayers.
- Despite taxpayer protests, SARS enforces additional tax assessments, exacerbating financial losses.
- The lack of structured fraud recovery mechanisms makes reclaiming lost funds difficult.

5.8.6 *Operational inefficiencies in fraud resolution*

- Fraud detection remains reactive rather than proactive, relying on taxpayer-initiated reports instead of automated monitoring systems.
- High-risk refunds continue to be processed despite reported fraud concerns.
- SARS fails to coordinate effectively with financial institutions to block fraudulent transactions in real-time.

5.8.7 *Dependency on external oversight for resolution*

- Many fraud cases remain unresolved until escalated to regulatory authorities such as the OTO.
- Taxpayer confidence in SARS's ability to handle fraud is severely undermined, prompting reduced engagement with digital tax services.
- Survey findings confirm that affected taxpayers often prefer alternative dispute mechanisms due to distrust in SARS's internal resolution processes.

6 SARS INTERNAL SYSTEMS AND INVESTIGATION CONTROLS

This section examines SARS's current processes, systems, and controls in light of the increasing prevalence of eFiling profile hijacking. It identifies critical risk areas and evaluates both systemic and communication-related gaps that must be addressed to ensure a secure and trustworthy digital tax environment for all taxpayers.

The OTO's review reveals that this is a multifaceted problem**,** driven by both external behavioural risks from taxpayers and practitioners and **i**nternal operational challenges within SARS.

6.1 INTERNAL OPERATIONAL CHALLENGES WITHIN SARS

SARS is currently experiencing several internal limitations that undermine its ability to respond effectively to eFiling profile hijacking, including:

- Challenges with the current case management system
    - Limited investigative personnel and capacity
    - Slow turnaround times
    - Challenges with fraud detection in eFiling profile hijacking cases
    - Slow response mechanism regarding eFiling profile hijacking investigation
- Absence of access to a formal Standard Operating Procedure for eFiling profile hijacking cases
- Limited oversight and absence of independent review of eFiling profile hijacking investigations

These challenges are discussed in more detail below.

6.1.1 SARS Case Management System and Impact on eFiling Profile Hijacking Investigations

According to the information provided by SARS, a dedicated unit responsible for investigating eFiling profile hijacking was established in ***October 2023***. Prior to this, fraud cases were handled through the **Remedy system**, which was not designed for taxpayer-facing solutions.

The transition has enabled fraud incidents to be reported through multiple channels (SARS website, walk-in branches, and call centres), with all cases now being formally logged in the SARS system.

SARS indicated that its Service Manager (SSM) system is used for the creation of case numbers, tracking, and finalisation of cases. While certain confidential details are not recorded within the system, SSM provides a structured platform for case management. Once a case is logged, SSM automatically accepts it and reflects it as part of the Digital Fraud Team's inventory. Cases are not rejected but are cancelled if the taxpayer fails to submit supporting documentation within 21 days. Cases are closed once a conclusion has been reached.

According to the information provided by SARS:

- **Average monthly intake:** 387 new cases
- **Active case inventory:** 8,956
- **Total cases:** 15,968
- **Average caseload per investigator:** 130 cases

The average turnaround time of **150 days** is routinely exceeded, with backlogs concentrated in Personal Income Tax (PIT) cases. The provinces of KwaZulu-Natal, Gauteng South, and the Western Cape account for a significant portion of the backlog.

Importantly, SARS reported that **94% of cases finalised in 2024** were resolved in favour of taxpayers. Over the past two years, approximately **R21,169,678.91** has been refunded to victims of eFiling profile hijacking. Although relatively small compared to overall revenue collections, this constitutes a direct fiscal loss.

6.1.1.1 Personnel Capacity and Skills in the Fraud Investigation Unit

According to SARS submissions, the fraud investigation unit has an approved structure of **19 posts.** This includes investigators, business analysts, compliance auditors, and operational managers. Of these:

- **13 posts** are permanently filled
- **3 members** are seconded
- **3 positions** are contract-based

That said, **6 posts** remain vacant or temporarily unfilled. Given the significant and rising caseload, the current staffing levels are inadequate. SARS must prioritise:

- Increasing personnel capacity
- Strengthening investigative skills and expertise
- Recruiting and retaining skilled investigators
- Building capacity for digital fraud detection

These steps are critical to improving resolution rates and reducing taxpayer vulnerability to eFiling profile hijackings.

6.1.1.2 Investigative Team Workload and Capacity Constraints

With an average of **387 new cases per month**, the pressure on SARS's limited investigative team is significant. The current structure consists of **19 approved** posts with only **13 permanently filled**, results in an average of **130 cases per investigator**. This imbalance places unsustainable pressure on investigators and contributes directly to growing backlogs and extended turnaround times.

SARS should urgently address these capacity constraints to enhance the responsiveness and effectiveness of its fraud investigation processes.

6.1.1.3 Turnaround Times and Case Resolution

Age analysis of open cases shows that many cases remain unresolved for **more than 150 days**, with some pending for over a year. These delays result in:

- Prolonged financial and compliance risk for taxpayers
- Delayed access to refunds (since refunds are paused until cases are resolved)

- Reduced public confidence in SARS's ability to protect taxpayer information

To improve turnaround times and resolution rates, SARS should consider:

- Redesigning investigative and case management processes
- Implementing automation and digital tools
- Improving resource allocation models
- Introducing case triage systems based on complexity

A differentiated case management system would allow simple cases to be resolved faster, while more complex cases receive appropriate resources and scrutiny.

6.1.1.4 Challenges with fraud detection in eFiling profile hijacking cases

Fraud detection at SARS is confronted by a range of operational and process-related challenges, particularly in the context of profile hijacking. The intake and triage of reported cases require submissions through multiple channels, with cases prioritized and distributed among investigators. However, high case volumes and limited resources often result in delays, making it difficult to ensure that urgent matters are addressed promptly and that no case is overlooked. For instance, there have been cases where, after a refund dispute was resolved in favour of the taxpayer and notification was provided regarding the processing timeline, the taxpayer later discovered that their banking information had been modified without their consent.

As a result, the refund was redirected to an unauthorised account and tax practitioner was locked out of the eFiling profile. The taxpayer practitioner was then advised to initiate a complaint but was unfamiliar with the process and required guidance on the necessary steps and documentation, including the submission of a bank confirmation letter, a sworn affidavit from SAPS with a case number, and a copy of their identification document. The investigation process is further complicated by the need to coordinate with various departments to correct records and recover funds where possible. These

challenges are compounded by the absence of integrated case management systems and the need for proactive anomaly detection, such as monitoring for unauthorized changes to banking details. Collectively, these factors underscore the importance of robust technology, streamlined communication, and clear procedures to enhance the effectiveness of fraud detection and to better protect taxpayers.

6.1.1.5 Slow response mechanism regarding eFiling profile hijacking investigation

Slow response mechanisms present a persistent challenge across the end-to-end fraud case management process at SARS, affecting both operational efficiency and taxpayer experience. Taxpayers may initiate fraud cases through various entry points, including the contact centre, branches, and escalation channels such as CMO, OTO, and the Office of the Commissioner. While these multiple channels are intended to improve accessibility, they can also result in fragmented case intake, duplication of effort, and delays in routing cases to the appropriate teams. Once a case is lodged, the standard turnaround time for finalising a complaint is up to 150 days; however, a significant number of cases extend well beyond this period, with some taking over a year to resolve. This slow response is particularly evident in regions such as KwaZulu-Natal, Gauteng South, and the Western Cape, which consistently record the highest volumes of both backlogged and finalised cases. During the investigation, taxpayers may face restrictions on their accounts and receive limited updates, leading to frustration and uncertainty. To address these challenges, it is essential for all SARS departments to coordinate closely, ensuring seamless handovers, clear communication, and targeted education initiatives for affected regions. Leveraging regional trend analysis and improving integration across all entry points will be critical to enhancing the efficiency, transparency, and overall taxpayer experience in fraud case management.

6.1.2 Absence of access to a formal Standard Operational Procedures for eFiling Profile Hijacking cases

As part of its investigation, the OTO formally requested SARS's Standard Operating Procedures (SOPs) relating to the handling of eFiling profile hijacking cases. SARS declined to provide the SOPs, citing that they are considered internal documents.

In lieu of the formal SOPs, SARS provided the OTO a summary of key procedural steps currently followed during the investigation and finalisation of such cases.

According to SARS, the process is divided into two investigative streams, namely, Restoration and Clean-Up of Tax Records and the Investigation Stream.

- **Restoration and Clean-Up of Tax Records**

Before a case can proceed to investigation under this stream, the following documents must be submitted by the taxpayer:

- A bank confirmation letter
- A SAPS affidavit detailing the fraud
- A certified copy of the taxpayer's ID

If any of these documents are missing, SARS contacts the taxpayer to request the outstanding items.

Once all documents are received and the case is under investigation, SARS reportedly follows these steps:

- Ensure the affected tax return has been corrected and adjusted
- Calculate and apply any interest due to the taxpayer
- Engage Debt Management division to attempt recovery of funds paid into fraudulent accounts

- Close the case in the SARS system and issue a formal outcome letter to the taxpayer
- Request the removal of automated stoppers on the Case Selection Application (CSA) following finalisation

- **Investigation Stream**

  This stream focuses on the forensic and procedural investigation of the profile hijacking incident. According to SARS, the following steps and standards apply:

  - Gather supporting evidence such as data downloads, system records and taxpayer interviews.
  - Compile an investigation report detailing findings
  - Maintain internal review notes, where applicable
  - Confirm with the taxpayer that their profile is secure and that banking details are accurate
  - Submit refund recommendations to the Refunds Committee (if applicable), followed by Finance processing

  While the summary provided by SARS outlines a degree of procedural structure, the absence of a formal, transparent, and accessible SOP presents a significant limitation. Without access to the complete SOP:

  - It is not possible to independently verify whether procedures are applied consistently across all cases
  - There is limited assurance that the process aligns with best practice standards
  - The lack of transparency reduces the ability of oversight bodies and taxpayers to hold SARS accountable

  The disclosure of a high-level version of the SOP, even in redacted form, would enhance governance, support audit and OTO oversight, and increase taxpayer trust in SARS's handling of eFiling profile hijacking cases.

6.1.3 Limited oversight and absence of independent review of eFiling profile hijacking investigations

SARS confirmed that eFiling profile hijacking cases are logged and tracked through its internal case management system, with structured reports generated for management oversight. According to SARS, standard reporting occurs on a monthly basis, providing divisional overviews of fraud case volumes and trends. Escalations, where necessary, are routed to the National Operations Centre (NOC) or Management Committee (MANCO), and significant exceptions are included in Enterprise Risk reports. These reports are also submitted monthly to the Head: National Operations Enablement (NOE).

Oversight decisions, risks, and recommendations are tracked within the broader SARS Governance Framework, which is built on the principles of risk-based governance, combined assurance, and accountability. SARS has indicated that this framework ensures fraud risks, including eFiling profile hijacking, are given attention proportionate to their assessed risk level. Implementation monitoring is conducted through existing governance committees, with overall efficacy assessed by the Auditor-General as part of the annual audit process.

SARS further stated that inventory data from SSM is being embedded into a Power BI dashboard report to support management reporting. While this represents a positive step toward improving oversight, the reliance on high-level tracking without full integration of investigative details limits the ability to assess investigative effectiveness. A more comprehensive system would support end-to-end tracking, provide real-time visibility of progress, and enable better accountability.

In terms of formal audits, SARS reported that both internal and external audits are conducted using a risk-based approach, with specific reviews scheduled as required. However, no dedicated internal or external audit of the Digital Fraud Team's operations, including those handling eFiling profile hijacking, had been undertaken.

This absence of independent review represents a governance and assurance gap. Without such reviews:

- There is **limited external assurance** regarding the efficiency, fairness, or consistency of fraud investigations
- Management may lack **objective insights** into operational risks or systemic weaknesses
- Stakeholder trust in SARS's ability to manage eFiling profile hijacking cases may be undermined

To strengthen governance and transparency, SARS should consider prioritising independent audits of its Digital Fraud Team's work. This would support continuous improvement and bolster public confidence in SARS's internal controls and accountability mechanisms.

6.2 CONCLUSION

The findings presented in this chapter highlight the complex, systemic nature of eFiling profile hijacking and the significant strain it places on SARS's internal systems, investigative capacity, and governance structures. While SARS has taken notable steps, such as establishing a dedicated fraud investigation unit and engaging in inter-agency and industry partnerships, several critical challenges remain that undermine the overall effectiveness and responsiveness of its fraud mitigation efforts.

Internally, SARS continues to face capacity constraints, including limited investigative personnel, slow turnaround times, and growing backlogs. The absence of access to a formal SOP, coupled with the lack of independent audits or external reviews, raises concerns about transparency, consistency, and accountability in handling these cases. While SARS reports regular internal oversight, the governance framework faces challenges due to the lack of independent assurance mechanisms, especially in relation to the operations of the Digital Fraud Team.

The growing incidence of eFiling profile hijacking demands an urgent and coordinated response. To address these vulnerabilities and build a more secure, resilient digital tax environment, SARS should prioritise improvements in the following areas:

- Strengthening personnel capacity and technical expertise within the fraud investigation unit
- Implementing a differentiated case management model, enabling faster resolution of simpler cases and targeted attention to complex ones
- Introducing regular, risk-based internal and external audits to enhance governance, oversight, and public confidence
- Disclosure (at least at a high level) of formal SOPs to support transparency and consistent application of procedures

Addressing these systemic issues will not only improve SARS's current fraud response capacity but also enhance its ability to safeguard taxpayer data, maintain public trust, and uphold the integrity of the digital tax system into the future.

7 SARS DIGITAL IMPROVEMENTS POST THE COMMENCEMENT OF OTO INVESTIGATION

Following the commencement of the OTO investigation into eFiling profile hijacking, SARS implemented several changes to its processes and systems. These enhancements have been positively received by the OTO. These enhancements include inter alia the following:

7.1 IMPLEMENTATION OF THE TAXPAYER VERIFICATION AND EDNA SYSTEM AT SARS BRANCHES

On ***21 August 2024***, as part of SARS' efforts to safeguard taxpayer information and prevent fraudulent activities, SARS implemented additional security measures across all its branches. The introduction of the Taxpayer Verification System (TPV) and the eDNA security system strengthens identity authentication processes for taxpayers who visit a SARS branch to update their banking details or registered information. These measures are designed to enhance security, prevent identity theft, and ensure the integrity of taxpayer records.

Taxpayers visiting SARS branches to amend their banking details or registered information will undergo authentication through the eDNA security system. This process includes biometric verification, where SARS officials will scan the taxpayer's fingerprint and capture their photograph. The fingerprint data is then cross-referenced with the records held by the Department of Home Affairs (DHA) to confirm identity authenticity.

Taxpayers registered for eFiling may update most personal details online. However, if banking detail validation is unsuccessful via eFiling, individuals will be required to visit a SARS branch for manual verification. Certain updates to registered details may also necessitate in-person authentication.

The Taxpayer Verification System applies to several key services, including:

- Entity maintenance and registration for Income Tax, Value-Added Tax (VAT), and Pay-As-You-Earn (PAYE).

- Updates to personal or registered details (e.g., banking details, identity number, name changes, trading name, contact details, address, and financial year-end).
- Legal entity deactivation and entity corrections, including entity merging.
- Requests for official documentation, including Notices of Registration (IT150, EMP103, VAT103).
- Debt management requests, including deferral arrangements.
- Dispute resolutions, such as Requests for Remission (RFR), Notices of Objection (NOO), Notices of Appeal (NOA), rejection reasons, and condonation requests.
- Requests for suspension of payments related to tax liabilities.

The taxpayer verification process involves the following steps:

- Provide a valid RSA identity document or ID card.
- Fingerprint scanning conducted by SARS agents.
- Photograph capture for identity verification.
- Fingerprint and identity confirmation against DHA records.

Tax practitioners and authorised representatives acting on behalf of taxpayers will also be subject to authentication before they are permitted to conduct transactions with SARS. Additionally, SARS officials performing certain security-sensitive tasks will undergo eDNA verification, requiring fingerprint scanning to ensure accountability and data protection.

7.2 ENHANCEMENTS TO TWO-FACTOR AUTHENTICATION AND EFILING PASSWORD SECURITY

On ***22 November 2024***, to strengthen the security of taxpayer information and mitigate the risk of malicious attacks on SARS data, SARS introduced enhancements to its 2FA system and eFiling password requirements. These measures are aimed at improving account protection by implementing multi-layered authentication protocols and enforcing stricter password criteria to prevent unauthorised access.

The 2FA system serves as an additional safeguard by requiring users to verify their identity using two distinct authentication methods before gaining access to their eFiling profile.

The authentication process consists of the following steps:

- **Primary Authentication:** Users must enter their username and password.
- **Secondary Authentication:** A One-Time-Pin (OTP) is sent to the taxpayer's registered security contact details. Upon successful OTP verification, users gain access to their eFiling account.

To enhance security, the following improvements have been implemented:

- **Mandatory Two-Factor Authentication for All Individual Profiles:** 2FA is now compulsory for all individual taxpayers, ensuring an extra layer of protection.
- **Verification and Updating of Security Contact Details:** Users are required to confirm and update their security contact details to prevent account compromise.

SARS has further reinforced password security standards to further prevent unauthorised access. The updated password criteria are as follows:

- Must contain a minimum of eight (8) characters.
- Must include at least one uppercase letter, one lowercase letter, one numeric character, and one special character.
- Must exclude personal information such as name, surname, email address, or username.
- Must avoid repetitive or sequential characters, e.g., "aaaaa" or "12345".

Additionally, a password strength meter has been integrated into the eFiling system to visually indicate the robustness of the password, assisting users in creating secure and reliable credentials.

According to the information from SARS, with effect from ***March 2025***, SARS introduced OTP on eFiling registration detail function for all bank detail changes. SARS should continue monitoring the effectiveness of the OTP implementation to ensure that it adequately addresses the underlying risks.

SARS also advised the OTO that they have implemented alert emails being sent to the taxpayer's security contact detail addresses for any changes to a taxpayer's registered details, including updates to security contact details. SARS should continue enhancing its security measures to ensure that its online platforms remain trusted, secure and user friendly for all taxpayers.

7.3 CONCLUSION

Despite SARS implementing these enhancements to its eFiling system after the OTO started its investigation, eFiling profile hijacking has not stopped. This indicates that the measures taken so far are insufficient to fully prevent or detect eFiling profile hijacking and fraudsters continue to exploit gaps faster than improvements are being implemented. A more integrated, proactive and taxpayer focused approach is needed beyond technical upgrades.

8 RELEVANT INFORMATION SHARING-ARRANGEMENTS BETWEEN SARS AND VARIOUS INSTITUTIONS

Currently, information sharing arrangements exists between SARS, banks, and other government agencies to detect, investigate and prosecute tax fraud including eFiling profile hijacking. That said, information from taxpayers and the results of the survey suggest that these mechanisms are not yet fully effective. Fraudsters continue to exploit weaknesses in the tax systems. These information sharing arrangements include the following:

8.1 INFORMATION SHARING BETWEEN SARS AND CIPC

8.1.1 Current arrangement

Currently, SARS has an information sharing arrangement with CIPC aimed at verifying registration data, detecting shell companies and fraudulent business profiles as well as ensuring tax compliance as soon as the business is registered with CIPC. For example, when a company is registered with CIPC, a SARS tax number is automatically generated.

8.1.2 Applicable legislation

Section 70(3*)(e*) of the TAA makes provision for a senior SARS official to disclose to the CIPC, the information as may be required for the purposes of carrying out the Commission's duties and functions under the Companies Act, 2008.

8.1.3 Key findings with the current arrangement

Taxpayer reports and case data suggest that syndicated VAT fraud often begins with unauthorised or fraudulent changes to the information of directors of companies at the CIPC. These unauthorised changes allow syndicates to:

- Take control of company tax profiles
- Open bank account in the company name
- Submit fraudulent VAT claims via eFiling and redirect VAT refunds to be paid into the fraudster bank accounts.

8.1.4 Recommendations to SARS and CIPC

Based on the above, it is recommended that:

- CIPC must notify SARS immediately and automatically of any changes to directors or company ownership information and SARS should use this notification to temporary freeze payment of VAT refunds until the new information is verified.
- Any changes to the directors of company information submitted to CIPC should be pre-validated by SARS.
- SARS and CIPC should establish a joint vetting process of high-risk changes aimed at flagging frequent changes to directors of companies, changes to directors of companies closely followed by large VAT refunds.
- CIPC should maintain a publicly accessible audit trail of historical changes to directors of companies for transparency and due diligence.

8.2 INFORMATION SHARING BETWEEN SARS, SAPS AND NPA

8.2.1 Current arrangement

Currently, SARS has an information sharing arrangement with SAPS to investigate and prosecute profile hijacking, digital crime and organised tax crime. For example, SARS refers suspected criminal tax matters to the National Prosecuting Authority (NPA).

8.2.2 Applicable legislation

Section 69(2)(*a*) of the TAA makes provision for a senior SARS official, to disclose to the SAPS or the NPA, information that relates to and constitutes material information for the proving of a tax offence.

8.2.3 Key findings with the current arrangement

Tax practitioners and victims of profile hijacking report that SAPS stations are often unable to categories or escalate cases of tax profile hijacking.

8.2.4 Recommendations to SARS and SAPS

Based on the above, it is recommended that:

- SARS in collaboration with SAPS should develop and provide standardised training modules to SAPS station level personnel covering the following: what is tax profile hijacking, how to identify digital tax fraud, how to escalate these matters to National Prosecuting Authority.
- SARS should work with SAPS to develop a national Standard Operating Procedure for reporting and handling tax profile hijacking.

8.3 INFORMATION SHARING BETWEEN SARS AND SARB

8.3.1 Current arrangement

Currently, SARS has an information sharing arrangement with SARB aimed at monitoring cross border financial transactions, especially those linked to illicit financial flows.

8.3.2 Applicable legislation

Section 70(3)(*a*) of the TAA makes provision for a senior SARS official, to disclose to the Governor of SARB, the information as may be required to exercise a power or perform a function or duty under the South African Reserve Bank Act, 1989.

8.3.3 Key findings with the current arrangement

Case study data and victims of profile hijacking suggests that fraudsters continue to open fraudulent bank accounts, particularly with digital banks and redirect fraudulent tax refunds into these accounts.

8.3.4 Recommendations to the SARB

Based on the above, it is recommended that SARB should conduct a compliance review in respect of banks that are repeatedly used in tax refund fraud.

8.4 INFORMATION SHARING BETWEEN SARS AND FIC

8.4.1 Current arrangement

Currently, SARS has an information sharing arrangement with FIC aimed at detecting suspicious financial activities and money laundering.

8.4.2 Applicable legislation

Section 70(3)(c) of the TAA makes provision for a senior SARS official, to disclose to the FIC, the information as may be required for the purposes of carrying out the Centre's duties and functions under the Financial Intelligence Centre Act, 2001.

8.4.3 Recommendations to SARS and FIC

SARS should strengthen the current information sharing arrangement to highlight the importance of profile hijacking cases.

8.5 INFORMATION SHARING BETWEEN SARS and DHA

8.5.1 Current arrangement

Currently, SARS has an information sharing arrangement with DHA aimed at preventing the use of fraudulent identity numbers for fraudulent taxpayer profile creation.

8.5.2 Recommendations to SARS and DHA

SARS should strengthen the current information sharing arrangement with DHA to highlight the importance of identity verification for purposes of limiting profile hijacking cases.

8.6 INFORMATION SHARING BETWEEN SARS AND BANKS

8.6.1 Current arrangement

Currently, SARS has an information sharing arrangement with Banks aimed at verifying and monitoring taxpayer banking details and fraudulent bank accounts that receive fraudulent tax refunds from SARS.

8.6.2 Key findings with the current arrangement

Despite having bank detail verification process in place, fraudsters are still able to exploit the onboarding loopholes, particularly with digital banks and redirect fraudulent tax refunds into these accounts.

8.6.3 Recommendations to SARS and BANKS

Based on the above, it is recommended that SARS should collaborate with banks to:

- flag new accounts receiving refunds tied to new bank accounts (created within the last 90 days and/or with no transaction history), recently changed CIPC entities, large VAT refunds amounts, unusual VAT refunds amounts (for example similar amount in month 1 and month 2).

- Flag bank accounts previously used in VAT fraud schemes and blocks or delays refund to those accounts pending investigation.
- Strengthen the real time pre-refund validation with all banks.
- Revise its MOU with the banking sector to include:
    - Sector wide minimum compliance standards for bank detail validation.
    - Turnaround time guarantees for verification requests.
    - Joint escalation pathway for fraud investigation

8.7 CONCLUSION

The findings from this investigation underscore the urgent need for enhanced coordination, automation and accountability in how information is used, not just shared. SARS and its partners must move beyond reactive measures and toward predictive risk-based monitoring, improved incident response protocols and stronger public communication strategies. Without these improvements, information sharing remains a theory, rather than a practical issue. Protecting taxpayers and restoring trust in the SARS eFiling system will require not only technical upgrades but also institutional commitment.

9 KEY FINDINGS AND RECOMMENDATIONS

9.1 KEY FINDINGS

9.1.1 Key Finding 1: Highest Prevalence of eFiling profile hijacking in tax practitioners followed by individual taxpayers.

During stakeholder engagements with the OTO, tax practitioners reported that they are mostly affected by eFiling Profile Hijacking. This is backed by the survey results which indicate that tax practitioners are affected more by eFiling profile hijacking at 48.3%, followed by individual taxpayers at 32.7%, followed by individuals represented by tax practitioners at 13.8% and lastly corporate represented by tax practitioners at 5.1%.

9.1.1.1 Tax Practitioners

The rationale for tax practitioners to be the most affected target for eFiling Profile hijacking include amongst others the following:

- High exposure and access volume:
  - Tax practitioners often handle multiple taxpayer accounts, which requires them to log into various taxpayer profiles. This frequent switching and elevated level access make them attractive targets to profile hijacking.
- Target value:
  - Compromising a tax practitioner account may give hackers access to hundreds of taxpayer profiles.
- Weak Digital security measures:
  - Some tax practitioners may not use strong digital security measures, for example, weak passwords, reused credentials, making these tax practitioners to be easy targets.

9.1.1.2 Individual Taxpayers

The rationale for individual taxpayers to be the second most affected target for eFiling Profile hijacking include amongst others the following:

- Less technological knowledge:
    - Many individuals may not understand or implement strong digital security practices.

- More susceptible to phishing:
    - Individuals are more likely to fall for social engineering attacks.

- High numbers, low complexity:
    - Since individuals represent a large number of the taxpaying population, even a small percentage affected translates to significant absolute numbers.

9.1.1.3 Individual Taxpayers represented by Tax Practitioners

The rationale for this group to rank behind the above-mentioned categories is that it overlaps with both categories, additionally it is because of the following:

- Double exposure:
    - The profile of this group is accessed by both them and tax practitioners thereby:
        - increasing the number of potential entry points for hijackers.
        - The more people who access a profile, the greater the attack surface.

9.1.1.4 Corporate Taxpayers represented by Tax Practitioners

The rationale for this group to rank the lowest is because of the following:

- Stricter Internal Controls:
    - Companies typically have more robust digital security policies and IT departments monitoring for suspicious activities.
- More sophisticated systems:
    - Companies use secure channels and dedicated portals for tax compliance, thereby reducing risk.
- Fewer login points:

- Unlike individual accounts, access is often centralised and monitored, companies use secure channels and dedicated portals for tax compliance, thereby reducing risk.

9.1.2 Key Finding 2: Incidents of eFiling Hijacking are common with Personal Income Tax followed by VAT.

According to the cases reported to the OTO and based on discussions during stakeholder engagements, PIT is mostly affected by eFiling Profile hijacking. This is evidenced by the survey results which indicate that PIT is mostly affected by eFiling Profile hijacking at 65%, compared to VAT at 20% and CIT at 15%. The rationale why PIT is mostly affected target for eFiling Profile hijacking include amongst others the following:

9.1.2.1 PIT involves individuals not corporates

- PIT is filed by individuals, who often have weaker digital security, e.g., weaker passwords, limited use of multifactor authentication.

9.1.2.2 High volume of individual taxpayers

- The number of PIT taxpayers is much higher than VAT and CIT simply because there are more individual taxpayers than registered companies. This increases the pool of potential targets for profile hijackers.

9.1.2.3 Lower awareness of digital security risks

- Individuals are often less informed about online threats compared to business that may have dedicated IT compliance departments.
- Many individuals do not monitor their tax profiles regularly, making it easier for hijackers to operate undetected.

9.1.2.4 PIT refunds are attractive

- Hijackers often target PIT accounts to intercept tax refunds, which are more common on PIT than VAT and CIT.
- It is relatively easy to redirect a PIT refund to fraudulent bank account if the profile is compromised.

9.1.2.5 Greater scrutiny for VAT and CIT returns

- VAT and CIT returns are typically filed by professionals, tax consultants, and filing undergoes greater scrutiny.
- Transactions for VAT and CIT are often cross verified with other data/transactions, thereby reducing opportunities for successful manipulation via hijacked profiles.

9.1.3 Key Finding 3: Estimated value of fraud in most eFiling profile hijacking cases is below R10 000, but a considerable number also fall within R10 000 to R100 000.

The survey results indicate that the estimated amount of fraud in most eFiling profile hijacking cases which is less than R10 000 is at 37%, the estimated amount of fraud ranging from R10 000 to R99 999 is at 33%, the estimated amount of fraud ranging from R100 000 to R999 999 is at 14% and the estimated amount of fraud more than R1 million is at 16%.

9.1.3.1 Estimated amount of fraud that is mostly less than R10 000

The reason the estimated amount of fraud for profile hijacking is mostly less than R10 000 include amongst others that SARS has automated risk detection systems (risk engines) that flag refund claims above certain thresholds such as R10 000 or R15 000 for audit or verification. Fraudsters are aware of this and therefore they:

- Deliberately submit refund claims just below these thresholds to avoid detection and increase the chances of payouts.

- Aim for smaller, quicker wins that are less likely to trigger a delay or review.
- Staying under R10 000 is a tactical move to reduce the chance of SARS intervening.

9.1.3.2 Targeting lower/middle income individuals

Fraudsters often hijack the profiles of lower- and middle-income taxpayers because:

- These individuals have less digital security awareness and weaker protection of login credentials.
- These individuals may not regularly check their SARS profiles or eFiling accounts, which means fraud can go undetected for longer periods.
- Some of these individuals tax returns often qualify for quick refunds, making them easy targets.
- Some of these individuals are below the tax threshold and are therefore not required to submit tax returns.
- Bogus tax practitioners submit tax returns using their credentials, and claim false expenses such as medical expenses, disability expenses, tax deductible donations, to manufacture refunds, which are then redirect into the bogus tax practitioners own accounts.

9.1.3.3 Small refunds are less likely to raise suspicion

Smaller fraudulent refunds are less likely to raise suspicion, for example, a fraudster can hijack 100 profiles and claim R2000 from each, totalling R200 000, with a low risk of triggering audit.

9.1.3.4 Syndicated level fraud: Amounts from R10 000 up to R1 million and above

Unlike the smaller, individual profile hijackings that aim for less than R10 000, the syndicated level of fraud involves mostly VAT refunds frauds and often involve the following:

- Fictitious or hijacked companies with forged or manipulated VAT returns claiming large input VAT amounts.
- Repeated claims over months before SARS can stop/notice.
- CIPC manipulation, where fraudsters change the names of directors to gain control of legitimate registered companies.
- Fraudsters exploit weaknesses of systems in inter-entity coordination and sometimes internal collusion or identity theft of company directors.
- Since these companies appear to be large businesses, their refunds are sometimes processed with less initial scrutiny, or the volume of returns makes scrutiny harder.
- Syndicates often act fast, exploiting the window before SARS detects irregularities.

9.1.4 Key Finding 4: Challenges on the authentication systems and security measures have created vulnerabilities that fraudsters exploit.

After the Minister granted approval for the OTO to conduct systemic investigation on eFiling Profile hijacking, SARS has:

- Introduced 2FA and eDNA system which includes biometric and identity verification for new filing registration and as an optional feature for existing taxpayers/tax practitioners. This applies prospective and not retrospective and came in a little bit too late after taxpayers/tax practitioners have been vulnerable to profile hijacking. That said, the introduction of these measures has not stopped profile hijacking as some taxpayers and/or tax practitioners are still subject to profile hijacking.
- Developed systems to detect and prevent fraudulent activities, including the use of One Time Pin for authentication.

9.1.5 *Key Finding 5: Challenges with fraud detection and slow response mechanisms allow hijackers to access and misuse eFiling profiles undetected including:*

- SARS's reliance on taxpayer-initiated fraud reports rather than automated fraud detection systems.
- Fraudulent details are removed and reinstated before SARS intervention.
- Victims of fraud often wait for months before cases receive any meaningful action.

9.1.6 *Key Finding 6: Taxpayers and tax practitioners encounter ineffective communications channels and limited support from SARS when trying to resolve eFiling profile hijacking cases.*

- 89% of respondents rated SARS's fraud response as ineffective due to delays and poor engagement.
- Tax practitioners face bureaucratic hurdles when attempting to assist clients with hijacked profiles.
- SARS rarely provides estimated resolution timelines or case status updates.

9.1.7 *Key Finding 7: Syndicated tax fraud begins with unauthorised or fraudulent changes to the information of directors of companies at the CIPC.*

- Taxpayer reports and case data suggest that Syndicated VAT fraud often begins with unauthorised or fraudulent changes to the information of directors of companies at the CIPC. These unauthorised changes allow syndicates to:
    - Take control of company tax profiles
    - Open bank account in company name
    - Submit fraudulent VAT claims via eFiling and redirect VAT refunds to be paid into these fraudster bank accounts.

9.1.8 *Key Finding 8: Victims of profile hijacking report that SAPS stations are often unable to categorise or escalate cases of tax profile hijacking.*

There is lack of coordinated effort between SARS and SAPS and taxpayers often struggle to obtain meaningful recourse for fraud cases without escalating to OTO.

9.1.9 *Key Finding 9: Fraudsters continue to open fraudulent bank accounts, particularly with digital banks, and redirect fraudulent tax refunds from SARS into these bank accounts.*

According to the information from taxpayers, fraudsters frequently open bank accounts with certain banks and deposit fraudulent tax refunds from SARS to these bank accounts. These tax refunds are often deposited into these bank accounts within seven days of the account being opened and these refunds are frequently processed by SARS officials after hours.

9.1.10 *Key Finding 10: Alleged Internal fraud and insider involvement.*

The survey participants expressed concerns about potential internal fraud as one of the key contributors to profile hijacking and the subsequent fraudulent of processing of tax refunds.

9.1.11 *Key Finding 11: Taxpayers lack digital security awareness.*

Some of the key contributors for eFiling Profile Hijackings amongst individual taxpayers are the following:

- Lack of knowledge about threats and secure online behaviour increases vulnerability.
- Taxpayers using weak or reused passwords.
- Taxpayers falling for fake emails or SMS that mimic SARS communication and steal login credentials.
- Taxpayers sharing SARS eFiling login details with third parties.

- Taxpayers logging into SARS profiles on public or unsecured networks can lead to data interception.
- Taxpayers negligently leaving tax documents (with ID numbers, tax reference numbers) exposed.
- Taxpayers not regularly checking their SARS profiles or eFiling accounts, which means fraud can go undetected for longer periods.
- Bogus tax practitioners submitting tax returns using credentials of taxpayer that are below the tax threshold, and claim false expenses such as medical expenses, disability expenses, tax deductible donations, to manufacture refunds, which are then redirect into the bogus tax practitioners own accounts.

9.2 RECOMMENDATIONS

9.2.1 Recommendations to SARS

9.2.1.1 Strengthen Authentication and Access Controls

- Compulsory 2FA for all users
    - With effect from ***22 November 2024***, SARS made 2FA compulsory for individual taxpayers and tax practitioners. SARS should implement graded 2FA policies based on activity risk level.
    - According to the information from SARS, with effect from ***March 2025***, SARS introduced OTP on eFiling registration detail function for all bank detail changes. SARS should continue monitoring the effectiveness of the OTP implementation to ensure that it adequately addresses the underlying risks.
    - SARS also advised the OTO that they have implemented alert emails being sent to the taxpayer's security contact detail addresses for any changes to a taxpayer's registered details, including updates to security contact details. SARS should continue enhancing its security measures to ensure that its online platforms remain trusted, secure and user friendly for all taxpayers.
- Address known 2FA weaknesses
    - SARS should continue monitoring the implementation of notifications to taxpayers and tax practitioners when:
        - high risks changes are made to their profiles, for example, passwords resets, banking detail changes, changes to the director/s of company, new access grants.
        - Login attempts are made from unusual devices or unusual locations.

- SARS should consider introducing additional measures such as:
    - Enable OTP location/device verification with alerts (e.g., “OTP requested from a new device/IP”).
    - Add optional authenticator app support (e.g., Google Authenticator, Microsoft Authenticator) rather than relying solely on vulnerable SMS OTPs.
    - 2FA reset protocols requiring full identity re-verification, especially when suspicious activity is detected.

9.2.1.2 Enhance biometric security across all profiles

- Current biometric application is limited
    - Biometric authentication implemented in August 2024 is currently only used for new eFiling registrations.
    - SARS must retrofit biometric re-verification for:
        - All existing taxpayer profiles (individual and business).
        - Key changes to existing taxpayer profiles (banking details, tax representative changes).
    - SARS should create a biometric check-in schedule for dormant profiles (e.g., if no activity for 6–12 months, biometric re-authentication is triggered before allowing access).

9.2.1.3 Strengthen fraud detection while enhancing service efficiency

- Currently SARS is restricting tax practitioners from updating security details on behalf of clients, even when a valid Power of Attorney (POA) is provided. While this control is aimed at reducing fraud, SARS should enhance it to strike a balance between fraud prevention and service accessibility. The current approach inadvertently hinders efficient service delivery to taxpayers.

9.2.1.4 Enhancement of Security and Prevention of Fraud

- SARS should allow taxpayers to view a detailed login history (IP address, device, location) from within their profile.

- During the risk period of SARS tax filing season, SARS should consider introducing a profile lock option that allows taxpayers to voluntarily freeze changes to their banking details by those taxpayers who do not expect to make changes in this regard. This measure would help prevent unauthorised updates and reduce the risk of eFiling profile hijacking during times of increased fraudulent activity.

9.2.1.5 Improve Refund Verification

- SARS should hold refunds for additional verification when banking details are changed shortly before a refund is claimed.
- SARS should increase pre-refund verification steps for all VAT refunds above certain thresholds.
- SARS should ensure that stoppers (not simulate stoppers) are implemented immediately on taxpayer accounts as soon as the taxpayer or tax-practitioner reports the incident of eFiling Profile Hijacking.
- SARS should adjust its refund audit triggers to not only flag high value claims but also:
    - Unusual refund patterns.
    - New or recently modified new bank details, company directors' profiles, tax practitioner profiles.
    - Frequent/similar amounts refund requests from the same entities.
- Implement automated alerts for refunds processed after hours or within days of bank account creation or change in banking details.

9.2.1.6 Improve SARS End to End Digital Fraud Process

- SARS should ensure that the SARS digital fraud unit is adequately capacitated to provide timely responses and regular updates to fraud victims, thereby preventing gaps in communication.
- SARS should ensure that the SARS digital fraud hotline is up to standard.

- SARS should clearly communicate the steps taxpayers need to take if their profile is hijacked.
- SARS should ensure that they fast-track account recovery so that tax practitioners do not wait for too long before their profile is updated as this renders them unable to work or provide services to their clients.
- SARS should ensure that eFiling profile hijacking cases are concluded within a reasonable time frame of 150 days to prevent prolonged taxpayer uncertainty. This should be clearly communicated to taxpayers in the service charter.

9.2.1.7 Strengthen Internal Controls and Processes

- SARS should conduct periodic independent audits on SARS eFiling systems and Mobi APP.
- To reduce the risk of internal fraud and insider involvement. SARS should initiate or continually improve on:
    - regular audits on system logins, employee access history and refunds processed after hours or within days of bank account creation or change in banking details.

9.2.1.8 Communication and Education

- SARS should launch nationwide taxpayer awareness campaigns targeting:
    - Digital security, phishing scams and best practices.
    - Taxpayers to monitor eFiling access and refund activity.
    - Provision of step-by-step guidelines on how to report eFiling profile hijacking.
- SARS should provide targeted services for vulnerable groups, for example:
    - Mobile support units or community service desks in low-income earners to assist with reporting, education and follow up on unresolved complaints.

9.2.2 Recommendations to Tax Practitioners

9.2.2.1 Strengthen third-party access controls.

9.2.2.1.1 Tax practitioners should work with SARS to:

- Strengthen two factor authentication for all tax practitioner logins to eFiling profiles.
- Implement a specific user ID and password for each individual user in a practice, rather than using shared credentials.
- Implement automatic real time email/SMS notifications to taxpayers when:
    - Tax practitioners request access to taxpayers' profiles.
    - High risk changes are made to taxpayer profiles such as:
        - changing banking details
        - updating tax practitioner details
        - changing directors of company information.

9.2.2.2 Tax practitioners should submit taxpayer details when they are registering to act on behalf of a taxpayer. This assist to create a direct association between the tax practitioner and the taxpayer themselves.

9.2.2.3 SARS should provide taxpayers with a login history visibility where they can:

- View all active tax practitioners linked to their profile.
- Monitor recent activity on their account.

9.2.2.4 SARS should require additional verification if tax practitioners must make high risk changes to taxpayer profiles such as:

- changing banking details
- updating tax practitioner details
- changing directors of company information.

9.2.2.5 Improve Code of Conduct between Tax Practitioners and SARS

- Tax practitioners should engage with SARS to improve the current code of conduct in relation to digital security.

9.2.3 Recommendations to Taxpayers

9.2.3.1 Use strong, unique passwords

- Taxpayers should create complex passwords using a mix of letters, numbers, symbols.

9.2.3.2 Use Two Factor Authentication System

- Taxpayers should use the recently introduced two factor authentication on individual SARS eFiling profile to add extra layer of security.
- Taxpayers should use the recently introduced Biometrics on individual SARS eFiling profile to add extra layer of security.
- Taxpayers should use a trusted authenticator app or SMS verification.

9.2.3.3 Beware of phishing scams

- Taxpayers should never click on suspicious links or open attachments from unknown sources.
- Taxpayers should verify emails or SMS claiming to be from SARS via the official SARS website, SARS call centre or OTO call centre.

9.2.3.4 Keep login credentials private

- Taxpayers should not share their SARS eFiling login details with anyone, including tax accountants, without secure arrangements.

9.2.3.5 Secure e-mail account

- Taxpayers should use strong passwords and two factor authentication their emails as it is linked to their SARS profiles.
- Taxpayers should regularly monitor their emails for unauthorised access.

9.2.3.6 Avoid using public Wi-Fi for tax transactions

- Taxpayers should perform SARS related tasks on secure, private networks only.

9.2.3.7 Update software regularly

- Taxpayers should ensure that their operating system, browser and antivirus software are up to date to avoid malware risks.

9.2.3.8 Monitor SARS profile activity

- Taxpayers should regularly log into their SARS eFiling account to check for unusual activity or unauthorised changes.

9.2.3.9 Use trusted devices

- Taxpayers should avoid logging in from shared or public computers where keyloggers may be installed.

9.2.3.10 Report suspicious activity immediately

- If taxpayers suspect that their profiles have been compromised, they should contact SARS immediately to secure their accounts.

9.2.4 Recommendations to National Treasury

9.2.4.1 Proposed changes to the TAA

It is proposed that the following changes should be made to:

- insert a provision that expressly provides that in instances where a taxpayer's profile has been unlawfully accessed and hijacked, resulting in a refund being fraudulently redirected to a third-party bank account, SARS shall remain obligated to pay the legitimate refund to the affected taxpayer, after the investigation is done and there is no evidence of taxpayer involvement , notwithstanding the prior payment of a refund to the fraudulent bank account.

- insert a provision that expressly prohibits SARS from initiating or continuing recovery actions against a taxpayer, until the investigation is done and there is no evidence of taxpayer involvement, in instances where the taxpayer's profile has been hijacked and false deductions, such as fictitious expenses, have been claimed by fraudsters in the taxpayer's tax return in order to generate artificial refunds subsequently paid into fraudulent accounts.

9.2.4.2 Establishment of an Inspector General as recommended by the Nugent Commission of Inquiry

One of the recommendations of the Nugent Commission of Inquiry into SARS was the establishment of an Inspector General. If established, the Inspector General would amongst other things, be responsible for:

- Conducting proactive investigations into high-risk areas where internal fraud or collusion is most likely to occur.
- Implementing continuous risk assessments and internal control evaluations to identify and address vulnerabilities in SARS systems and processes.
- Monitoring and evaluating the effectiveness of SARS internal anti-fraud measures and making recommendations improvements.
- Providing a secure and independent reporting system accessible to all SARS employees. This system would allow employees to report, without fear or favour, colleagues suspected of internal fraud and/or insider involvement in profile hijacking.
- Ensuring timely follow up on those reports with independent oversight.
- Publishing periodic reports on the nature and resolution of internal fraud cases, to promote transparency and organisational accountability.

9.2.5 Recommendations to the South African Reserve Bank

- It is recommended that the incidents that the OTO have identified with the specific banks should be reported to the Prudential Authority of the South African Reserve Bank for their consideration.

9.2.6 Recommendations to SARS and Banks

- It is recommended that SARS should collaborate with banks to:
  - flag new accounts receiving refunds tied to new bank accounts (created within the last 90 days and/or with no transaction history), recently changed CIPC entities, large VAT refunds amounts, unusual VAT refunds amounts (for example similar amount in month 1 and month 2).
  - Flag bank accounts previously used in VAT fraud schemes and blocks or delays refund to those accounts pending investigation.
  - Strengthen the real time pre-refund validation with all banks.
  - Revise its MOU with the banking sector to include:
    - Sector wide minimum compliance standards for bank detail validation.
    - Turnaround time guarantees for verification requests.
    - Joint escalation pathway for fraud investigation.

9.2.7 Recommendations to SARS and CIPC

- It is recommended that:
  - CIPC must notify SARS immediately and automatically of any changes to directors or company ownership information and SARS should use this notification to temporary freeze payment of VAT refunds until the new information is verified.
  - Any changes to the directors of company information submitted to CIPC should be pre-validated by SARS.
  - SARS and CIPC should establish a joint vetting process of high-risk changes aimed at flagging frequent changes to directors of

companies, changes to directors of companies closely followed by large VAT refunds.

- CIPC should maintain a publicly accessible audit trail of historical changes to directors of companies for transparency and due diligence.
- SARS and CIPC should encourage business owners to regularly check CIPC status and company director records.

9.2.8 Recommendations to SARS and SAPS

- It is recommended that SARS in collaboration with SAPS should:
  - develop and provide standardised training modules to SAPS station level personnel covering the following: what is tax profile hijacking, how to identify digital tax fraud, how to escalate these matters to National Prosecuting Authority.
  - develop a national Standard Operating Procedure for reporting and handling tax profile hijacking.

10 CONCLUDING REMARKS

Although there is a growing number of cases of eFiling profile hijacking, it is important to emphasise that eFiling system remains a critical pillar of South African tax administration system. It enables accessibility, efficiency and facilitates auto-assessments. These are key features of a modern and effective revenue service.

The investigation by the OTO takes place at a time when South Africa urgently needs revenue. SARS is under significant pressure to fulfil its constitutional mandate of collecting revenue effectively and equitably. The OTO acknowledges and supports the ongoing efforts by SARS to modernise its systems and improve tax compliance.

However, the findings of this investigation reveal that eFiling profile hijacking poses a serious threat, not only to taxpayer trust in the SARS eFiling system but also to the long-term credibility, security and efficiency of the whole tax system. While this investigation exposed a pattern of fraudulent activities, it also highlighted a service delivery failure by SARS in assisting taxpayers who fall victim to eFiling profile hijacking.

Despite the introduction of various security measures by SARS, for example, Two Factor Authentication System and SMS notifications, these have proven insufficient in proactively preventing unauthorised access by fraudsters.

Moving forward, it is important that SARS, guided by the OTO recommendations in this report, implements a more robust and holistic risk-based fraud prevention strategy. This includes enhancing the current two factor authentication for all user categories, introducing profile lock features during risk period of SARS tax filing, enhancing biometric verifications for both new and existing profiles, improving taxpayer support and fostering cooperation with its partners.

Strengthening these controls will not only mitigate the incidence of eFiling profile hijacking but also help restore public trust in the SARS eFiling system. Ultimately, such measures are essential to safeguarding taxpayer rights and upholding the integrity of South African tax administration system.

11 ABBREVIATIONS

- **AI** – Artificial Intelligence
- **APP** – Application
- **BASA** – Banking Association South Africa
- **CIPC** – Companies and Intellectual Property Commission
- **CIT** – Corporate Income Tax
- **DHA** – Department of Home Affairs
- **EDNA** – Electronic Digital National Authentication
- **FICA** – Financial Intelligence Centre Act
- **IT** – Information Technology
- **NPA** – National Prosecuting Authority
- **OTO** – Office of the Tax Ombud
- **OTP** – One-Time Pin
- **PIT** – Personal Income Tax
- **POPIA** – Protection of Personal Information Act
- **RCB** – Recognised Controlling Body
- **RCBS** – Recognised Controlling Bodies
- **RSA** – Republic of South Africa
- **RSN** – Reported Suspicious Non-compliance
- **SAFPS** – Southern African Fraud Prevention Service
- **SAPS** – South African Police Service
- **SARS** – South African Revenue Service
- **SATPU** – South African Tax Practitioners United
- **SMS** – Short Message Service
- **SOP** – Standard Operating Procedure
- **SOQS** – SARS Online Query System
- **TAA** – Tax Administration Act
- **VAT** – Value-Added Tax