Ref:

31 October 2025

Ms Y Mputa
Menlyn Corner
87 Frikkie De Beer Street
Menlyn
Pretoria
0063

Per email: ymputa@taxombud.gov.za
mmalakalaka@taxombud.gov.za

Dear Ms Mputa

SAICA COMMENTS ON THE OFFICE OF THE TAX OMBUD'S DRAFT REPORT ON ALLEGED EFILING PROFILE HIJACKING

SAICA welcomes the opportunity to comment on the Draft Systemic Investigation Report issued by the Office of the Tax Ombud (OTO) on 1 October 2025, in respect of Alleged eFiling Profile Hijacking (draft OTO report).

This submission consolidates SAICA's detailed review comments, in Annexure A, referencing the different sections in the draft OTO report.

SAICA believes that in a global digital economy, characterised by a continually modernised fiscal environment and the increasing integration of multiple systems from different parties, proper collaboration and an appropriate design methodology are necessary, instead of allowing a single party to dictate a complex integrated path that serves only its interests. The digital economy and fiscal crimes will only continue to increase as new integrated fiscal technologies are adopted (e.g., e-invoicing) and can only be mitigated through collective wisdom and expertise.

South Africa just exited the FATF Greylist with much relief, though many of the original findings related to investigation and enforcement of financial crime. Our general observation and concern regarding the particular factual findings are the lack of disclosure of critical facts in determining cause and consequence. This is imperative to understand where corrective action and training is required.

Furthermore, there are no statements as to whether criminal investigations and internal consequence management followed any of the matters, given the prevalence of findings as to **seemingly either criminal conduct or gross negligence**. Some of the findings indicate that the relevant information required as to refunds or tax profile, which enabled targeting such profile, could only be obtained directly from the SARS system. Of concern is that only taxpayers and tax practitioners were seemingly required to file SAPS affidavits of their "innocence of involvement" as if the fraud was perpetuated on them, rather than correctly on SARS as per the factual findings. In this regard, we would recommend that the OTO confirm in its final report that in all matters where a fraud was perpetuated on SARS (i.e. SARS suffered the loss), SARS process dictated, and it was in fact reported to SAPS as a crime for investigation. These are not just matters for "internal investigation" and require proper investigation by the relevant authorities like SAPS, Reserve Bank, Public Protector and the Auditor-General South Africa (AGSA), all who have the relevant mandates to address these matters properly, especially as some of these matters date back to a period starting in 2012.

Given the multiparty nature of the required investigations, it would also be advisable that the OTO raise the matter with Parliament, which is able to initiate cross disciplinary accountability and oversight into the progress of investigations.

Please do not hesitate to contact us should you have any queries in relation to our submission.

Yours sincerely,

Tarryn Atkinson
Chairperson: NTC

Dr Muneer Hassan
Deputy Chairperson: NTC

Pieter Faber
Head: Taxation

Somaya Khaki
Lead: Tax Advocacy (Administrative Law)

The South African Institute of Chartered Accountants

ANNEXURE A:

Contents

ANNEXURE A

CLARIFICATION OF CONCEPTS

1. SAICA notes with concern that the draft report does not consistently distinguish between key concepts such as “hijacked,” “compromised,” “submission of fraudulent return”, and “fraudulent refund.” This lack of clarity makes it difficult to understand the nature of the breach in each case study, assess the adequacy of SARS’ response or the response by other parties involved, and determine whether the taxpayer was prejudiced or merely exposed to risk.

2. Factual clarity will also enable stakeholders to address where the key risks are that require mitigation through system and process enhancements and enhanced training.

3. To support a more accurate and actionable analysis, SAICA proposes the following definitions and/or distinctions be considered in the final report to give proper legal context to some of these colloquial terms. This is based on our understanding of the terms used in context with the findings in the report. The OTO’s understanding may be different, and the OTO should then, regardless, give the terms proper context and meaning through clarification of terms used consistently to indicate a particular conduct or occurrence.

4. Conceptually there seems to be **system breaches** (i.e., system hijacked or compromised) and **data alteration** (i.e., unlawfully altered with or without a system breach). The OTO report states that the latter is always present in these crimes, while the former may or may not occur.

What does it mean for a profile to be “Hijacked”?

5. A **hijacked profile** refers to a SARS eFiling account that has been unlawfully accessed and taken over by an unauthorised party by means that require the use of valid eFiling account credentials obtained or created through illegal means. The hijacker assumes control of the profile, typically by:

   - Using illegally obtained valid login details.
   - Resetting or creating login credentials illegally.
   - Potentially modifying tax practitioner representation to gain rights within the system.
   - Altering public officer details to gain rights within the system.
   - Hijacking a related system e.g. SIM swap or the Companies Intellectual Properties Commission (CIPC) system, to achieve any of the above.

6. This may result in the taxpayer and/or tax practitioner losing access and control over the profile. Hijacking is a full or partial takeover and is often accompanied by identity theft or impersonation.

7. This could also involve compromising other systems e.g. a SIM swap to redirect security features, like the one-time-pin or illegally creating a bank account with a fake identity, enabling a complete takeover of the profile.

What does it mean for a profile to be “Compromised”?

8. A **compromised profile** (i.e., hacked) refers to a breach of integrity within the eFiling account

and system where access to the eFiling account is obtained without the valid eFiling account credentials. This may involve:

- Public exposure of login credentials.
- Hacking of the eFiling system.
- Exploiting a vulnerability in the eFiling system.

9. While the taxpayer may retain access, the profile is no longer secure.

What does it mean for a profile to be "Unlawfully Altered"?

10. An **unlawfully altered profile** refers to where the eFiling account's data has been modified or transacted on or wilfully / negligently allowed to be modified or transacted on by an unauthorised party or by an authorised party by manually overriding or undermining the normal standard operating procedure. These include unlawfully:

    - Changing banking details.
    - Changing the public officer.
    - Changing contact details.
    - Changing information or adding information to a return.
    - Submitting or cancelling a return or other transaction.
    - Creating new or parallel profiles.

Distinction between "Fraudulent Submission" and "Fraudulent Refund"

11. SAICA notes that the report frequently refers to "fraudulent refunds" without clarifying whether the refund itself was invalid or whether the refund was valid but misappropriated. This has to be inferred by reading the recommendation, which may mention whether or not the refund was 'reinstated' or paid to the taxpayer.

12. This distinction is critical in understanding what transpired. To our understanding:

    - A **fraudulent submission** refers to a tax return that contains false information – e.g., fictitious expenses – to generate an "artificial refund". In this case, both the return and the refund are fraudulent, and therefore no refund should be paid based on such fraudulent return.

    - A **fraudulent refund redirection** occurs when a legitimate refund – based on valid return information – is intercepted and redirected to a fraudulent bank account. The refund is not fraudulent; however, it is redirected to a different bank account – not authorised by the taxpayer. Potentially, someone other than the taxpayer fraudulently submitted the valid return information. However, the information in the return is correct, and the refund is validly due to the taxpayer.

13. In several of the case studies, the report initially refers to the refund as fraudulent but later notes that the refund was reinstated to the taxpayer. This implies that the return information was valid, and the refund was legitimate, but the payment was intercepted and misdirected due to hijacking, compromise of the system, or unlawful alteration.

RECOMMENDATION

14. Without clear and consistent definitions, it is impossible to:

- Determine whether the eFiling system or an external system (or both) were “breached”.
- Determine upon whom the fraud was perpetrated.
- Determine whether SARS’ fraud detection protocols were triggered appropriately.
- Assess whether the taxpayer was unfairly subjected to recovery actions.
- Understand whether the refund should have been withheld, redirected, or reinstated.
- Evaluate the nature of the breach – that is, whether it was due to a weakness in authentication procedures or a tax return submission based on fictitious information.
- Determine whether appropriate and legally required reporting to relevant authorities and consequence management was applied.

15. Submission: SAICA recommends that the final report adopt definitions to clarify concepts (similar to the abovementioned definitions or suitable variations thereof) and apply them consistently across all case studies and recommendations.

16. This will ensure that systemic vulnerabilities are accurately diagnosed and that recommendations are appropriately determined.

1.8.4 RECOMMENDATIONS TO NATIONAL TREASURY

17. A proposal is 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.’

18. Whilst this proposal will provide welcome relief to affected taxpayers, it may not take into account the fact that the fraud could be perpetrated due to a fault on the part of the taxpayer or tax practitioner if “taxpayer involvement” means “wilful assistance”, rather than just gross negligence e.g. “reckless sharing” of login details.

19. If this proposal is legislated in a strict sense, it could mean that SARS is carrying an unjustified cost due to fraud perpetrated through no fault on the part of SARS – placing an undue burden on the State. We, however, agree that a greater burden of proof and onus to investigate should lie with SARS as the system owner, and that the taxpayer should not suffer financial detriment on mere allegation without SARS proving “taxpayer involvement” i.e. mere allegation should not suffice to delay the refund rectification.

20. Submission: this proposal, while appreciated for placing some responsibility on SARS to investigate and demonstrate ownership of the system, should be reconsidered and refined in light of the concerns raised above.

21. It is recommended that taxpayer involvement should encompass both "direct involvement in the fraud" and "contributory gross negligence." It is submitted that contributory negligence is too broad

and will merely result in disputes over who was more negligent – SARS, the taxpayer or a third party.

22. Furthermore, though the restoration of any monies is important, equally important is the impact on the taxpayers' tax compliance status. As demonstrated in the OTO findings, some of these matters took months, if not a year, to resolve after being reported. It is recommended that a specific provision be added to exclude any such affected monies as "tax debt" and prohibit SARS from considering such monies in any tax compliance status determination from the date it is reported by the taxpayer or his/her representative, until a final investigation outcome is achieved to determine "taxpayer involvement".

CASE STUDIES

23. Based on our review of the case studies, there are a number of factual issues that require clarification in the draft report to address some of the questions raised by the case studies as they relate to the involved parties' conduct and the processes applied. These are detailed under individual headings below.

Case Study 1: Compromised Profile and Refund Redirection

24. From the information provided, it is not clear as to how the taxpayer's profile was accessed. Was there a complete 'hijacking' of the profile or was it otherwise compromised and if so, how did the fraudster gain access?

25. What type of return was submitted – was it an individual or a corporate? Based on the quantum of the refund, it is assumed that this was an individual taxpayer.

26. It's unclear how the bank detail change was made: on the RAV01 or tax return? When a taxpayer makes a change on their profile, they usually receive a notification from SARS – was such a notification sent at the time, or was this feature not operational at that time?

27. What were the verification steps required of the taxpayer in the circumstances? Our understanding is that the majority of the time, SARS requires a selfie of the taxpayer or registered representative to verify who is initiating the change. Was this a requirement at the time?

28. How was it possible for the verification to be overridden on the basis that it was completed, and what checks does SARS have in place to prevent fraud?

29. Since the verification was overridden without any explanation or reason, it can be inferred that there may have been involvement from within SARS based on the information provided. If this did occur, what consequence management was taken against the individual/s involved in cancelling the verification, and were there broader motives, if any, determined (see OTO Draft Report key findings 1.7.7 and 1.7.10)?

30. Was the matter reported to the South African Police Service (SAPS), and what was the outcome of the investigation?

31. Regarding the second bank details verification triggered in August 2023, what triggered this, and was the person who 'cancelled' that verification identified? How were they dealt with?

32. With respect to individual tax returns, as SAICA is aware, it was not possible for tax practitioners or tax administrators to submit returns more than five years old via eFiling. It is not clear if the same applies to taxpayers filing their own returns. It would be helpful if this could be clarified.

Submitting returns older than five years

29 July 2024 – SARS has recently received complaints from tax practitioners regarding difficulties in accessing their clients' returns older than five years. To address this issue, tax practitioners are required to reconfirm their status on eFiling before attempting to request or submit such returns. Once their status has been successfully reconfirmed, tax practitioners may proceed with these requests or submissions.

Additionally, it has been noted that tax administrators linked to tax practitioners are currently unable to request or submit old returns, placing an undue burden on the tax practitioners. In response, SARS has implemented a change allowing tax administrators linked to tax practitioners to request or submit returns older than five years.

33. Furthermore, eFiling was not even available until 2006. How was it possible to submit returns from 1999, even if individual returns were available for more than five years prior?

34. If returns were not submitted for five years, were penalties imposed? If so, why was this not set off against the refunds due? Alternatively, was the taxpayer not required to submit?

35. If no returns were required to be submitted by the taxpayer, how did the fraudster know to target this profile with no returns required and possible "lawful refunds" i.e. there would be low detection risk as the taxpayer would not manage the profile and the monies were in fact claimable but not claimed?

36. What platform did the taxpayer use to report the case? As per the below, SARS introduced the SOQS process for reporting such cases on 27 October 2023. At the time, SARS informed stakeholders that when they reported such issues using the relevant SOQS form, the system would immediately place a stopper on the profile. If this case was reported using this platform, why did the system not initiate the stopper?

Digital fraud reporting now online

27 October 2023 – If you suspect that your tax profile has been compromised, you can now report it electronically. As part of our ongoing efforts to enhance taxpayer confidence, we are introducing a new feature today. Simply click here to report the incident and follow the prompts to register your case. This will assist SARS to manage and prioritise your case while making it easier for you to interact with SARS when it comes to digital fraud.

See the updated SARS Online Query System Guide here.

37. If the above platform was not used, what reason did SARS provide for delaying the stopper for five months?

38. Given that the refund was paid to the taxpayer, the returns were not fraudulent, but the person submitting, submitted fraudulently. How did they have access to the taxpayer's information – sufficient to complete the return?

39. When was the matter reported to the OTO, and what was the turnaround time for recommendations to be made to SARS? Did the OTO communicate with the taxpayer to keep the taxpayer apprised of the progress?

40. Submission: we respectfully request the OTO to address the questions above, by providing full details in the final report.

41. Recommendation: Legally, it seems that when taxpayers are not required to submit returns – as per the annual notice to submit returns, in terms of section 25 of the Tax Administration Act, 2011 (TAA), – section 99, TAA will not find application to stop these historical returns and assessments in instances where taxpayers chose not to submit and claim valid deductions, as there was never an original assessment. This seems to be a particular vacuum in law and process exploited by this relevant fraudulent activity.

42. The OTO should consider a recommendation to SARS and National Treasury to address the vacuum in law and process in the final report.

Case Study 2: Practitioner Representation Hijacked

43. How were the director's details changed with the CIPC? Was it done through the CIPC portal or manually, and what checks were in place to verify the change?

44. Were there checks to verify the Registered Representative (RR) and bank details changes on SARS' side and were they properly applied by the relevant SARS official? Was a notification sent to the RR when the details were changed?

45. What reasons did SARS provide for not taking timeous action once the fraud was reported? Specifically, with respect to the refund paid on 6 July, this was after the fraud was reported (on 30 June) – how did SARS explain this payment without verification? What triggered the verification after the refund was paid?

46. Were the refunds paid into the perpetrator's account 'valid' refunds for the taxpayer, or was there fictitious information submitted to create fictitious refunds? Towards the end of the cases study, it is indicated that the hijacked refunds were restored, potentially meaning the information in the returns were correct and the refunds validly due to the taxpayer. Alternatively, does it mean the refunds were reversed?

47. On what basis did SARS issue an additional assessment and what was the process followed to initiate the additional assessments? Is it the OTOs view that the correct process was followed or was there malicious intent to intimidate the taxpayer?

48. What checks were done before issuing the final demand? Did the system not flag that there was fraud resulting in the refunds, in which case – how did SARS justify issuing a final demand to the taxpayer, in the circumstances?

49. There are no indications in the feedback that SAPS was involved. Was the matter reported to the SAPS, and what was the outcome of that investigation?

50. Submission: we respectfully request the OTO to address these issues by providing full details, to the extent allowed in law, in the final report.

Case Study 3: Digital Fraud Investigation

51. The case study notes that the taxpayer visited a SARS branch to update their banking details. No information has been provided as to what triggered this. This is important, as it may provide answers as to where and how the fraud started.

52. It is not clear how multiple bank accounts could be linked to one profile (i.e., as opposed to one account per many profiles), as our understanding is that taxpayers may select only one bank account to link – i.e., in order to transact with SARS. What is meant by this statement, and were the multiple accounts found to be validly linked, or did it include accounts the taxpayer was not aware of?

53. More detail is required as to what triggered the investigation, by the Digital Fraud Unit and what documents were required of the taxpayer to conduct the investigation.

54. Was the matter reported to the SAPS, and if so, what was the outcome of the investigation.

55. Were the Financial Intelligence Centre (FIC) or the banks engaged to investigate the opening of multiple bank accounts, assuming these were fraudulently opened? What was the outcome of their investigation and what steps will be taken to resolve any security concerns?

56. The escalation notes mention that it was not possible to pay a refund to the taxpayer as a result of the investigation that had been initiated. Details are required as to the nature of the refund – i.e. was it due to a return submitted by the taxpayer or was the return submitted by the person perpetrating fraud on the taxpayer?

57. If this was due to a fraudulent submission or merely an attempt to redirect a refund created through a valid return submission – how did the perpetrator know that there was a valid refund due to the taxpayer?

58. Details are required as to why it took so long for SARS to finalise the case, given that a special unit was set up to focus purely on these cases.

59. Furthermore, what consequence management is in place when the SARS Complaints Management Office (CMO) does not deal with cases within a reasonable turnaround time – 21 days as prescribed by SARS?

60. It was also noted that the OTO took a month to 'accept' the complaint from the taxpayer. What was the reason for the delay?

61. Submission: we respectfully request the OTO to address these issues by providing full details in the final report.

Case Study 4: Registered Particulars Changed

62. Insufficient details were provided as to how the perpetrator was able to submit returns on the taxpayer's profile. Details are required as to how this was facilitated – i.e., was the profile 'hijacked' or compromised in another way, potentially through the back end of the SARS system?

63. Details are required as to whether this was reported to the SAPS.

64. Furthermore, were the bank/s and/or the FIC engaged in respect of any of these cases, and if so, what was the outcome? What was the outcome of their investigation, and what steps will be taken to resolve any security concerns?

65. The OTO report initially refers to the refund as 'unauthorised'. However, in the Case resolution, it is noted that the refund was eventually paid to the taxpayer. This would indicate that the refund was valid but rather unlawfully redirected. This needs to be clarified.

66. If it was a valid refund, details are required as to how the perpetrator knew that a valid refund was due to the taxpayer, as is the case in the majority of these case studies.

67. What is also interesting in this case is that the taxpayer received an email notification of changes made to the profile. Why was this not the case in the other case studies? In those cases, changes were made, and presumably the taxpayer or registered representative was not made aware of this. Was there a system change?

68. Submission: we respectfully request the OTO to address these issues by providing full details in the final report.

Case Study 5: Fraudulent Registration and Return Submission

69. Details are required as to how the perpetrator was able to register multiple profiles and for thirteen years.

70. Further, this case study refers to returns under the taxpayer's profile, but the taxpayer did not create those profiles. This needs to be clarified.

71. It is noted that SARS requested certain supporting documents, which the person never provided. It is concerning that this did not trigger further investigation. What are the usual steps that SARS is meant to follow in such cases and why were the profiles not blocked?

72. How were the supporting documents requested, and is there evidence that they were sent to the taxpayer or a different contact?

73. At 5.5.3 in the OTOs report, it is noted that a fraud case was created and then 'automatically cancelled' by the system. How was this facilitated and is this a standard process that enables automatic cancellation for such a serious matter without Senior SARS Official (SSO) involvement?

74. Did the OTO request SARS feedback as to why managerial oversight is not required to facilitate cancellation of fraud cases, and if so, what was SARS' response?

75. Details are required as to what consequence management there was given that the SARS CMO did not deal with the case within a reasonable turnaround time – 21 days as prescribed by SARS.

76. At 5.5.6, it is noted that 'the fraudster exploited SARS's payment threshold, causing SARS to pay refunds before later requesting supporting documents, which were never submitted or processed.' Firstly, how did the fraudster know what these thresholds are/were? Secondly, what is the standard process to release refunds where a verification is in progress – does this not require a manager or supervisor sign off?

77. Details are required as to reporting on the matter to the SAPS and the outcome of the investigation.

78. Submission: we respectfully request the OTO to address these issues by providing full details in the final report.

Case Study 6: OTP Circumvention and Profile Fraud

79. At the outset, it was noted that the taxpayer received the OTP on multiple occasions, indicating multiple attempts to unlawfully access the taxpayer's eFiling profile. Is there any indication that the taxpayer tried to change their login details to secure their profile?

80. Regardless, the prior OTP notifications indicate that the taxpayer had set up two-factor authentication (TFA). How was it then possible for the fraudster to access the profile and change banking details without the taxpayer entering the OTP to allow the login to eFiling? Was there any investigation into whether the taxpayer SIM was cloned?

81. Does the SARS system allow someone to go through the back end to access a taxpayer's profile without an OTP, as well as allowing changes to details?

82. Again, in this case, the refund that was redirected was then paid to the taxpayer – indicating that it was validly due to the taxpayer. Details are required as to how the perpetrator knew that a valid refund was due to the taxpayer – this seems to be a common thread in these case studies.

83. Details are required as to what consequence management there was given that the SARS CMO did not deal with the case within a reasonable turnaround time – 21 days as prescribed by SARS.

84. Submission: we respectfully request the OTO to address these issues by providing full details in the final report.

Case Study 7: Simulated Stopper Failure

85. The background notes that an unauthorised individual tried to gain access to the company's eFiling profile. Was this reported immediately by the taxpayer, and if so, what action was taken by SARS?

86. Details are required as to how the tax practitioner's access was removed from the taxpayer's eFiling profile. As far as SAICA is aware, this would require the profile being 'requested' by another tax practitioner and the RR then having to approve the transfer. Details are required as to how this process was circumvented.

87. The background notes that the fraud case was reported via the call centre but only 'formally' reported to SARS on 12 March 2025. Why was there a delay? Was the recording of the call to the call centre listened to, to determine if the SARS agent advised the tax practitioner or RR to report the case via the form on SOQS to ensure automatic stopping of any refund?

88. Assuming the agent did not inform the contact person of the correct process to follow, what steps were taken to address this failure?

89. Details are required as to how information in the company's eFiling profile was removed from the authorised user's eFiling profile, after security contact details were updated on 25 February 2025.

90. Given that the case was formally reported – we assume this means that it was reported on SOQS. If so, why was the stopper not automatically placed, by the system? SARS advised that reporting via SOQS would ensure that no refunds would be paid until the investigation was finalised.

91. Details to be provided as to how it was possible for the same account to be 'hijacked' multiple times. It seems that the taxpayer tried to 'secure' the profile by changing login details multiple times, with assistance from SARS.

92. Was the failure therefore from a SARS perspective – i.e., despite best efforts by the taxpayer, the profile was still hijacked due to circumvention of controls from inside SARS?

93. In all of this, there is not a single example of the taxpayer's login details being compromised. Details on how the account was 'hijacked' are imperative to understanding what went wrong.

94. At 5.7.4, mention is made of a 'simulated stopper'. Further details are required to clarify what is meant by this. Furthermore, if approval for a stopper is required, does this mean that reporting cases on SOQS no longer immediately places a stopper on the profile?

95. Details are required as to the progress by SAPS in terms of their investigation into this matter.

96. Submission: we respectfully request the OTO to address these issues by providing full details in the final report.

Key Findings from Case Studies – General comments

97. In all of the case studies documented, there was not a single example or allegation of tax practitioner or taxpayer login details being compromised through phishing scams, spyware or hacking, etc. – unless this was the case but not explicitly stated in the report. If it was the case, such fact should be disclosed.

98. No details are provided regarding consequence management – that is, dealing with CMO delays, cases closed without authorisation, refunds paid without supporting documentation, etc.

99. No details are provided of any criminal investigations reported by SARS or investigated by SAPS, the Public Protector or the Reserve Bank and the outcome of such investigations. If there were such external criminal investigations, this should be disclosed, even if it's just noted as "ongoing".

100. Submission: further details are required as to consequence management where there was clear failure on the part of SARS to adequately and timeously deal with matters, or where internal Standard Operating Procedures (SOPS) were not followed.

101. In addition, details regarding exactly how the profiles were hijacked or compromised, are required.

102. Given repeated service failures by the CMO, it may be necessary for the OTO to consider requesting the Minister to approve a systemic investigation into the effectiveness of the CMO by the OTO.

INTERNAL OPERATIONAL CHALLENGES WITHIN SARS

103. With respect to statistics on the number of cases reported, it is not clear if these are all unique cases or include follow ups on unresolved cases. Clarity is required.

104. Further details would be useful – that is, details on how many cases relate to multiple incidents on the same profile.

105. Regarding the absence of access to SARS's SOPs relating to the handling of eFiling profile hijacking cases, it is not clear why the OTO was prevented access given that staff have security clearance to access SARS internal documents. This is potentially a deficiency in the privilege allowed to staff of the OTO and restriction on access to information to carry out their duties, especially as to investigating facts and reviewing the effectiveness of internal administrative SARS processes.

106. SARS Annual Report 2023/2024[1] pg. 5 does note significant challenges and concern by the Commissioner of SARS (CSARS) with respect to refund fraud. However, we see no mention of third-party fraud or internal fraud, inferring that this is taxpayer refund fraud. Pg. 44 only mentions collaboration with law enforcement on tax evasion related crimes (23) and State Capture (13). As relates to Mechanisms in Place to Report Fraud and Corruption on pg. 87, it commendably covers all types of fraud and corruption and states:

> *'Where the matter is recommended for disciplinary action, it is referred to the relevant unit for evaluation and recommendation to line management on whether to proceed with disciplinary action. When an internal investigation concludes that an employee has committed fraud or corruption, a criminal case is registered and SARS will assist SAPS and NPA until the case concludes in court.'*

107. Given the above as relates to the +/-16 000 cases, it should therefore be possible to obtain confirmation that all +/-16 000 were reported to SAPS and also to obtain information as to how many of these cases resulted in criminal cases against SARS officials.

108. At point 6.1.2 (Investigation Stream), no reference is made to SAPS. Details are required as to how the SAPS reporting and investigation fall within this process.

109. At 6.1.3, (Limited oversight and absence of independent review of eFiling profile hijacking investigations), it is noted that the efficacy of implementation of the SARS Governance Framework is assessed by the AGSA, annually. This raises the question as to the AGSA's involvement in a specific investigation on the issue of Alleged eFiling Profile Hijacking – given the material number of cases (+/- 16 000 cases) that are on record and that this has been going on for more than a decade.

110. Submission: we request specific insights on the above to be shared in the final report.

SARS DIGITAL IMPROVEMENTS POST THE COMMENCEMENT OF OTO INVESTIGATION

111. It is noted that additional controls were implemented following the investigation – apparently to

[1] SARS-AR-29-Annual-Report-2023-2024.pdf

improve verification prior to updating of details such as bank account. However, it is not clear how this will circumvent any unlawful internal overrides to bank detail verifications and refund approvals.

112. Whilst there were enhancements to the two-factor authentication process, this did not prevent the scenario in Case Study 7. This raises questions as to the effectiveness of these controls in the face of internal security process circumvention.

113. The OTO noted that the additional controls did not prevent the profile 'hijacking'. However, no firm proposals were made to address this.

114. Submission: without detail on how certain security processes were circumvented internally, it is not possible to determine the effectiveness of new controls implemented by SARS. This needs to be addressed.

115. In addition, two-factor authentication, whilst being a step in the right direction, also has its own challenges if applied to standard operations such as checking correspondence or viewing statements of accounts. It is suggested that two-factor authentication be specifically implemented on high-risk actions such as:

- Processing refunds.
- Updating banking details.
- Changing public officer information.
- Amending business addresses.

INTER-AGENCY COORDINATION

Companies Intellectual Property Commission (CIPC)

116. At 8.1.4, recommendations are made to circumvent the risk of unauthorised changes to the public officer with CIPC (registered representative on the SARS system).

117. There are concerns that some of these recommendations may prove cumbersome and will cause unnecessary and significant red tape for legitimate changes. In respect of point 1, there is a further concern that this will contribute to delays already experienced with respect to the payment of VAT refunds.

118. Insufficient detail is provided as to how the SARS pre-validation (point 2) will work.

119. Point 3 makes better sense around cooperation to flag high risk areas, for example, where there are frequent changes to directors.

120. Submission: due to the burden that these recommendations may place where legitimate refunds are due and details were legitimately changed, timelines should be imposed to ensure that these processes don't unjustly impact taxpayers.

121. Furthermore, there needs to be adequate, timeous communication to affected taxpayers to ensure that they are able to take steps to promptly resolve any 'frozen accounts' to avoid unnecessary delays in legitimate payments of refunds.

122. The proposal for the publicly accessible audit trail of historical changes to directors of companies for transparency and due diligence, makes sense.

South African Police Service (SAPS)

123. The report acknowledges that taxpayers are required to report profile hijacking incidents to SAPS and obtain a case number. We are in agreement with this, based on experiences shared.

124. We are in support of the recommendations made by the OTO in respect of this.

125. Regarding the cases already reported, the OTO report lacks sufficient details on the outcome of the SAPS investigations as well as the turnaround time of such cases.

126. There is no recommendation as to SARS having to file criminal cases to SAPS in all these cases, nor that SAPS and SARS report on the progress of these cases.

127. Submission: we request that a report on SAPS eFiling 'fraud' cases be included in the final OTO report with statistics of:

128. Number of cases reported; Who reported the case – that is, SARS, CIPC or the taxpayer; Turnaround time on resolution of cases; Common trends identified.

129. It is recommended that if not already a SOPS, SARS be required to file a fraud case with SAPS for every fraud instance perpetrated on SARS or involving a SARS system, irrespective of how it happened or who suffered the loss.

South African Reserve Bank (SARB)/Banking Association

130. Whilst it is admirable that there is information sharing between SARS and SARB on certain matters, it seems that these matters persist creating the perception that nothing has been done to address the poor controls in opening accounts with certain banks.

131. It was our understanding that this would form part of the investigation.

132. Submission: the OTO to advise if the banks 'implicated' as identified in the related survey, as the most common banks that came up in these cases were engaged as to the ease of opening bank accounts without verification of the taxpayer.

133. Additionally, after identifying the 'common banks', it may be worthwhile analysing the information to identify the geographic location of the branches involved (where relevant) and proximity to SARS branches where taxpayers subject to the fraud are registered.

Financial Intelligence Centre (FIC)

134. Again, it is admirable that SARS has an information sharing agreement with the FIC. However, it is not clear how or if this was used to assist in the investigation into the alleged eFiling profile hijacking – specifically with respect to the creation of fraudulent bank accounts and tracing of funds until it exited the banking system.

135. In our view, this presents a major risk for our country, given that we have just exited the "Greylist" with the FIC and other organisations having introduced additional stringent measures to prevent money laundering etc.

136. Submission: the OTO to provide more detail of investigations by the FIC into the banks 'implicated' by virtue of responses to the related OTO survey as well as specific case studies.

Public Protector

137. The OTO currently maintains a Memorandum of Understanding with the Public Protector, whereby both parties agree to work closely to address any taxpayer complaints against SARS. It is not clear if the outcome of this investigation into Alleged eFiling Profile Hijacking will be referred to the Public Protector.

138. Based on the findings, it is clear that:

- SARS failed to act on reported hijacking incidents within reasonable timeframes.
- Recovery actions are initiated against victims despite clear evidence of fraud.
- Internal controls are found to be inadequate despite repeated warnings.

139. In our view, these may constitute matters within the Public Protector's mandate and violate constitutional rights to fair administrative action.

140. Submission: While not explicitly referenced in the draft report, SAICA believes that the systemic nature of SARS' failures and the administrative harm caused to taxpayers warrants referral to the Public Protector.

Auditor-General South Africa (AGSA)

141. There is no recommendation as to engaging the AGSA, given the finding in 6.1.3 of limited independent review and assurance.

142. We have also not been able to confirm in prior years in the SARS Annual Reports or AGSA Reports that these +/-16 000 profile hijackings were audited and raised as an "*emphasis of matter*" in the audit report. The OTO report notes that SARS stated:

'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.'

143. Submission: Given the other findings on process failure and SARS' confirmation of the role of the AGSA, it is recommended that the OTO engage the AGSA on its findings in the final report, for consideration in both audit risk and disclosures.

KEY FINDINGS AND RECOMMENDATIONS

144. Concerns are raised regarding specific key findings and recommendations as noted below.

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

145. The statement regarding this finding seems to infer that these categories of persons suffer the highest incidence of profile hijacking.

146. Based on the seven case studies included in the draft OTO report and the other data noted, there were no factual findings of tax practitioner or taxpayer systems being hacked or compromised or that their valid login details were used to commit such acts.

147. Should these be confirmed to have occurred, such findings should be included in the report.

148. It would rather seem that the finding supports that detection and mitigation incidences are the highest by tax practitioners, which would make sense as these are the most active users of SARS eFiling.

149. Submission: Should the wording incorrectly infer our concerns, it should be clarified to indicate detection as opposed to system compromise.

150. Should it correctly infer, as the finding suggests, that taxpayer systems are compromised, more factual support is required to conclude that the highest prevalence of eFiling profile hijacking was perpetrated on tax practitioner profiles.

151. Specific examples and statistical data are required to validate the above claim.

152. It seems that what wasn't considered in the draft OTO report, was that the eFiling profile hijacking seemed to spike soon after SARS did a security update.

153. Before this update, tax practitioners held the tax types and would release them on request – specifically for individual taxpayers.

154. Following the update, this security measure was removed, and the taxpayer (or someone hacking the taxpayer) could remove the profile without the tax practitioner being informed or having to authorise this.

155. This function was removed for tax practitioners to release the profile, due to some tax practitioners acting unethically and withholding taxpayer profiles due to, for example, non-payment of fees.

156. In our view, SARS should have continued to deal with those tax practitioners specifically – a number of cases were referred to SAICA for disciplinary action in the past.

157. The current process means that tax practitioners are unable to safeguard their clients' profiles due to the significant risk that profiles may be hijacked despite controls in place on the side of the tax practitioner. To revoke the tax practitioner access, the client's profile is the one being targeted.

158. There is also a concern that SARS removing the security measure without consultation on

alternatives or improvements to address concerns from tax practitioners, directly contributed to the finding, and a more collaborative approach should be followed by SARS.

159. Submission: the OTO to consider the impact of the abovementioned security update on the escalation of eFiling profile hijacking of individual taxpayer profiles.

160. To further consider if restoring the process to how it operated in the past may alleviate the number of profile hijacking incidences.

161. In our experience through engagement with SAICA members and other recognised controlling bodies (RCBs) – as well as engagements with SARS over the years – SARS systems are not properly integrated/synchronised. There are different profiles or parts of the SARS system which appear to have different contact details for the same taxpayer. For example, the debt management system may have different details to that on the compliance system.

162. This is evident given that certain correspondence may be sent to certain contact details, whereas other correspondence is sent elsewhere. There have also been cases reported of SARS sending correspondence to tax practitioners who have never engaged the specific taxpayer. This has been reported to SARS over the years, but no conclusive explanations were provided.

163. Tax practitioners have also noted that in some instances, even where the details have been updated by the taxpayer or tax practitioner, some SARS systems revert to the previous contact details which at times may be the taxpayer's previous tax practitioner or a past employee whose email address is no longer valid. In some cases, correspondence is being sent to personal email addresses of registered representatives, as opposed to the designated work email address provided.

164. Submission: the OTO to engage SARS to understand how the different databases are integrated and what processes are in place to ensure that only the most updated details for the taxpayer, as per the RAV01 is used in all instances.

165. An additional concern is where a tax practitioner is expected to retain the taxpayer profile of an ex-client, that is, after having terminated that tax practitioner's services. This occurs where such taxpayer does not request the profile back nor is there a transfer to another tax practitioner. In that circumstance, if the tax practitioner that just terminated services with the taxpayer simply deletes the profile, according to SARS, the history of that profile is permanently lost. For this reason, SARS has requested tax practitioners to retain the profile – a matter that SAICA has been requesting a solution for, for the last few years.

166. In these circumstances, if the tax practitioner retains the profile – given that SARS has not developed an alternative solution – and that taxpayer's profile is hijacked, the tax practitioner can potentially be held liable. This would create a significant risk for tax practitioners – created purely because SARS systems cannot accommodate an alternative.

167. Submission: the OTO should recommend that SARS, in collaboration with the RCBs, provide guidance to tax practitioners on managing terminated engagements with taxpayers specifically for cases where the terminated taxpayer has not requested or transferred their eFiling profiles; or

168. Alternatively, introduce a release function that notifies both the taxpayer and the current tax

practitioner of the release activity.

169. The notification should include details of the tax practitioner initiating the release. It is further recommended that the release function should be limited to specific activities and to include options that perhaps advise that the release is initiated due to termination of services. Additionally, the transfer could perhaps be complemented with a two-factor authentication prompted with the taxpayer, to mitigate any further risk of potential profile hijacking.

9.1.1.2 Individual taxpayers

170. The draft OTO report makes the point that individual taxpayers are 'more susceptible to phishing', on the basis that they are more likely to fall for social engineering attacks.

171. No basis for this conclusion has been provided in the report.

172. Submission: statistical data to be provided to validate this claim.

9.1.4.4 Corporate Taxpayers represented by Tax Practitioners

173. It is noted in the draft OTO report that companies typically have more robust digital security policies and IT departments monitoring for suspicious activities and that due to all the controls in place, they have the lowest risk.

174. That said, in Case study 7, despite the best efforts to report quickly and to secure the profile, the profile was repeatedly 'hijacked'.

175. In addition, the current SARS implementation of a single login for all eFiling profiles linked to a user – whether personal or corporate – has introduced significant vulnerabilities for corporate taxpayers.

176. Examples of Risk:

177. **Unintentional exposure via tax practitioners:** A corporate employee may share their login credentials with a tax practitioner to assist with their personal tax return. If the practitioner uses those credentials to access the eFiling system, they may inadvertently gain access to the corporate profile linked to the same login.

178. **Profile transfer missteps:** In some cases, users transfer their personal profile to a practitioner's account, not realising that this also exposes the corporate profile. This often occurs due to a lack of understanding of the implications of SARS's login structure.

179. **Use of unregistered tax practitioners:** Individuals may engage unregistered or informal tax practitioners to file their personal returns. These practitioners, using shared credentials, may unknowingly gain access to sensitive corporate tax data.

180. **Data breach potential:** In one instance, a user's personal login was compromised through phishing. Because the same login granted access to the corporate profile, unauthorised parties were able to view and potentially alter corporate tax information.

181. These risks are compounded by the fact that many users are unaware of the consequences of sharing credentials or linking profiles. The current system design inadvertently facilitates these exposures.

182. Submission: more detail is required as to how the above transpired, despite companies being low risk and a recommendation suggested that SARS reconsider the single log-in functionality due to the risks noted above.

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

183. The draft OTO report notes that there is a higher incidence of eFiling profile hijacking amongst individuals – for various reasons, which seem reasonable.

184. However, what is not noted is how the perpetrators know that a refund is due to the targeted taxpayer. If we have understood it correctly, in all the cases highlighted, the refund was validly due to the taxpayer but merely redirected to the fraudster. In one instance the taxpayer seemingly never submitted returns, nor claimed any of the valid expenses for the refund.

185. This would seem to indicate that the perpetrators are targeting specific types of accounts and there may be common 'criteria' for selection thereof. This would, in our view, include that PIT accounts where there is no tax practitioner are the least monitored due to mainly annual tax submissions.

186. Submission: it would be helpful for the OTO to extend its investigation to determine the common thread between the different PIT cases reported to enhance the investigation outcome and recommendations.

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

187. As noted earlier in the submission, the finding that perpetrators are targeting taxpayers with refunds below a certain threshold is indicative of 'insider' knowledge of SARS' practice and thresholds.

188. Submission: the OTO final report to provide details on whether this aspect was investigated further and if so, the outcome thereof.

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

189. The OTO draft report notes that survey participants raised concerns of 'potential internal fraud as one of the key contributors to profile hijacking and the subsequent fraudulent processing of tax refunds.'

190. In certain cases, it does appear that this could be inferred from the information provided. However, the OTO does not explicitly state if this was identified in its investigations and we believe the report is lacking in this regard.

191. Submission: more detail is required in each of the case studies reported, as well as statistics on those cases not included in the report – to indicate in how many instances there were internal overrides which effectively facilitated the fraud. Whether it was on allowing bank detail changes; refunds without supporting documents; or changes to security contact details or the RR.

192. This will align with the OTOs values of ensuring transparency in all processes, transparency being a quality that SARS also aspires to as part of its strategy.

9.1.11 Key Finding 11: Taxpayers lack digital security awareness.

193. There are various statements regarding how individual taxpayers lack 'digital security awareness'. However, no data has been provided to validate this claim.

194. To assist members and the public in addressing the right concerns, SAICA would need factual data showing areas of key concerns.

195. Submission: the OTO to include in the final report, statistical data to validate the claim of lack of digital security awareness of taxpayers.

9.2.1.6 Improve SARS End-to-End Digital Fraud Process

196. The OTO draft report proposes that SARS should ensure that the SARS digital fraud hotline is 'up to standard'. However, no guidance is provided as to how this can be achieved. Specific details need to be provided to outline exactly what is needed to achieve this: for example – the number of resources allocated, availability of staff, response time etc.

197. Submission: the OTO to provide more detailed recommendations in this regard.

9.2.6 Recommendations to SARS and Banks

198. Various recommendations were made for collaboration between SARS and the Banks to address the issue of bank accounts fraudulently opened in the taxpayer's name.

199. However, no details have been provided as to what measures are already in place, how this has already been facilitated, and whether FIC requirements were complied with by the relevant Banks.

200. Submission: the OTO to provide more detail regarding the above, in the final report.

9.2.8 Recommendations to SARS and SAPS

201. As noted earlier, whilst we support the recommendations to be adopted going forward, in all of the cases highlighted as well as others reported to SARS – a crime was committed and needed to be reported to the SAPS.

202. With close to 16 000 cases reported to SARS, over more than a decade – it would be reasonable to expect that many of these cases would have been finalised, and findings issued. It is not clear as to whether any of these outcomes were reviewed by SARS and/or the OTO. These findings are important to decide on the most appropriate action to be taken going forward.

203. Submission: more details regarding the outcome of SAPS investigations and any criminal prosecutions related to the eFiling profile hijacking or profile compromise should be shared in the final OTO report on this systemic investigation.