South African Institute of Taxation

SAIT | Summit Place Business Park | Building 3, Ground Floor
221 Garsfontein Road | Menlyn | South Africa | 0081

www.thesait.org.za

31 October 2025

To: The Office of the Tax Ombud
Menlyn Corner, 2nd Floor,
87 Frikkie de Beer Street,
Menlyn,
Pretoria

Via Email: Communications@taxombud.gov.za

RE: DRAFT REPORT INTO ALLEGED E-FILING PROFILE HIJACKING

Dear Colleagues.

We attach hereto comments on the Office of the Tax Ombud's (OTO) Draft Report into Alleged eFiling Profile Hijacking.

We value the opportunity to participate in this process and welcome further engagement if required.

Please do not hesitate to contact us should you need further information.

The South African Institute of Taxation

1. Introduction

1.1. On behalf of our members, we would like to extend our sincere appreciation to the Office of the Tax Ombud for this comprehensive draft report on alleged eFiling profile hijacking (hereinafter referred to as the "draft report") and for undertaking such a thorough investigation into the persistent and evolving issue of alleged eFiling profile hijacking. This has been a long-standing challenge for our members and the broader tax community, and we are grateful for the diligence and commitment shown in addressing this systemic concern.

1.2. We note the finding that tax practitioners are most affected by eFiling profile hijacking. As a Recognised Controlling Body (RCB) with more than 8,000 tax practitioners as members, we welcome the comprehensive report and appreciate that the scope was extended to specifically include tax practitioners in their professional capacity in the mandate of the Tax Ombud.

1.3. On the basis that the findings indicate that the segment that is most affected is tax practitioners, we propose that an amendment be included to clearly include servicing tax practitioners in their capacity as practitioners within the Tax Ombud's mandate. We appreciate that by virtue of the fact that For brevity, inter alia we will make our comments in reference to the OTO's summary of recommendations to SARS as set out in the draft report.

2. Comments on the proposed recommendations

2.1. Ad par 1.8.1.1 - Strengthen authentication & access controls

2.1.1. Two factor authentication (2FA) has made notable improvements in relation to IT security; however, based on feedback from our members whose profiles have been compromised even with 2FA activated, this method of security has not proven to be guaranteed. We believe that it would be beneficial if a benchmarking is done with the security features in the banking industry.

2.1.2. We note that some banks have for instance moved away from using SMS and email services as 2FA specifically because it is susceptible to fraudulent sim-swaps and intercepted email accounts.[1] Some banks consider in-app 2FA as more secure. We welcome the recommendation in the draft report that refers to the utilisation of third-party authenticator apps. We would recommend that consideration be given to collaborating with SARS in this regard on the basis of the existence of the SARS MobiApp that could possibly be improved with authenticator and in-app approval functionalities.

2.1.3. In addition to the above, the recommendation could be amplified to include the functionality to link specific devices to eFiling profiles to allow eFiling

[1] https://www.absa.co.za/offers/sim-swap-fraud-protection/

administrators the ability to monitor and delink specific devices with access to the profiles. This will further enhance security and control over access to eFiling profiles.

2.2. Ad Par 1.8.1.3 - Strengthen fraud detection while enhancing service efficiency

2.2.1. We agree that the security measures should not be a hindrance to efficient service delivery to taxpayers especially for tax practitioners. Considering however that tax practitioners are most affected by profile hijacking, we believe that restricting practitioners from updating their clients' security details is a necessary security measure. The rationale is that if a practitioner's profile is compromised, the fraudster will be able to gain access to all their clients' security details thereby compromising their eFiling profiles as well. Changing and updating security details should be exclusively available to the profile owner.

2.2.2. We do note that the current 2FA process can at times be very slow with delays between when OTPs are requested and received. It could assist efficiency if the OTP's reach the users faster.

2.3. Ad Par 1.8.1.4 - Enhancement of security and prevention of fraud

2.3.1. In addition to allowing a detailed login history, it will also benefit if an activity log can be extracted by the profile owner. Once profile access has been reinstated / recovered by the legitimate profile owner, they need to determine exactly what details were changed or returns were filed to ensure it is corrected.

2.4. Ad Par 1.8.1.5 – Improve Refund Verification

2.4.1. We are concerned that a blanket approach to place a hold on refunds for additional verification if banking details were changed shortly before a refund is claimed could result in new delays in SARS paying legitimate refunds.

2.4.2. Individual taxpayers for instance will likely only change their banking details on SARS's records when it is time to submit their annual returns.

2.4.3. Amending the banking details in isolation shortly before a refund is claimed would not necessarily indicate a compromised profile. There are several actions that will precede the changing of banking details very often in a short space of time. For instance, the profile holder's security details would be changed, users might be added, contact details might be changed etc. SARS would, through its investigations, be able to establish specific modus operandi in these matters. These methods employed by fraudsters and sequences of events could be used to create specific risk profiles to determine if a hold should be placed on refunds for further verification.

2.5. Ad Par 1.8.1.6 – Improve SARS end to end digital fraud process

2.5.1. We welcome this recommendation especially for SARS to fast-track account recovery. This is especially a problem when the profiles are locked over deadlines for submission of returns.

2.5.2. This necessitates practitioners to request remission of penalties and interest after the fact and there is no guarantee that the requests will be approved.

2.5.3. SARS can extend the deadline for submission of returns in terms of s25(6) of the Tax Administration Act, No. 28 of 2011 (TAA). We would suggest that the recommendation could be amplified to allow automatic extensions to be granted for returns that are due during the period where taxpayers and practitioners are locked out of their eFiling profiles due to hijacking incidents. This will avoid the administrative burden and cost of applying for remission after the fact.

2.6. Ad Par 1.8.4.1 – Proposed changes to the TAA

2.6.1. We welcome the recommendation that legitimate refunds should be paid to taxpayers in instances where the refunds were diverted to unauthorised bank accounts.

2.6.2. We would propose that the funding model of this should be ventilated to consider the economic impact and the best use of taxpayer funds. There could again be a possible benchmarking with how banks finance reimbursements to clients whose bank accounts were compromised, if this has not been considered already.

2.6.3. We would also propose very specific criteria to be established under which a reimbursement will happen to avoid opening new avenues for fraudsters to exploit in conjunction with taxpayers who are due refunds.

2.6.4. We also welcome the proposal to prohibit SARS from taking collection steps against taxpayers who are victims of profile hijacking and fraudulent refunds were created without their involvement. On this recommendation though, we believe it could be considered to rephrase the reference to “no evidence” in the recommendation to “no prima facie evidence”. The rationale is that SARS will only be able to conclude that there is no evidence of taxpayer involvement after the investigation has been concluded whereas *prima facie* will allow SARS to determine if there is evidence of taxpayer involvement on face value when the investigation commences.

2.7. Ad Paragraph 1.8.6 - Recommendations to SARS and Banks

2.7.1. We agree with the recommendation especially because it considers a sequence of events that would create a risk and not be a blanket approach that could frustrate payment of legitimate refunds.

2.7.2. Generally, tax refunds must be paid into the taxpayer’s bank account, and one would not expect more than one refund to be paid into an account in the same tax period. While we do not expect the exact details of the modus operandi of

fraudsters to be publicly disclosed, there could be a possibility that fraudsters use one bank account for more than one scheme. If this is the case, the recommendation could be amplified for banks to flag any instance where more than one refund payment is made by SARS into the same bank account in the same tax period.

2.8. Ad Paragraph 1.8.8 – Recommendations to SARS and CIPC

2.8.1. Like the comment in par 2.4 above, we are concerned about the practicality of this recommendation if every change at the CIPC will result in holds to be placed on refunds. This not only has implications for refunds but could also frustrate other services by SARS for taxpayers and practitioners for instance it could delay updating details of Registered Representatives.

2.8.2. This could be alleviated if it is limited to a specific sequence of events that could indicate a possibility of profile hijacking or fraud.

3. Ad paragraph 4.3 – Types of e-Filing Profile Hijacking

3.1. We note with appreciation that Section 4.3 of your report details the various types of eFiling profile hijacking. We must make mention that these are precisely the types of profile hijacking we have previously communicated to you during our engagements, as listed inter alia in the respective meetings and correspondence between our members and your office, in the report.

3.2. However, we wish to draw your attention to a newly emerged and highly sophisticated form of eFiling profile hijacking, that has been brought to our attention by one of our members. In this instance, despite the fact that the taxpayer and their public officer having multi-factor authentication, including 2FA enabled on all profiles, and despite strict internal controls, the fraudster was able to change the security contact details and gain access to the profile.

3.3. Notably, in this instance, the public officer personally submits the company's EMP201 returns each month from their own login, and all users in the office are required to use MFA. What is particularly concerning is that the breach occurred without any evidence of email compromise, and the only other route would have been via eFiling using biometric authentication. This raises serious questions as to how the fraudster could have bypassed stringent measures such as the facial scanning protocols, and whether there may be an element of internal compromise within SARS systems.

3.4. Following the breach, the fraudster proceeded to revise the company's EMP501 reconciliation, replacing all the legitimate IRP5s with fraudulent ones for individuals who are not employees. It can be construed that the apparent intention was to submit income tax returns for these fictitious employees and claim fraudulent tax refunds.

3.5. This incident demonstrates a level of sophistication that surpasses previously documented methods. It is imperative that SARS urgently investigates this matter, as it suggests that even robust security measures may be vulnerable to advanced attack vectors.

3.6. We urge the consideration of this new modus operandi in future risk assessments and to have this brought to the attention of SARS as a means to strengthen internal controls and biometric verification processes accordingly.

End.