

REPUBLIC OF SOUTH AFRICA



IN THE TAX COURT OF SOUTH AFRICA
(HELD AT JOHANNESBURG)

Case No: **VAT 2138**

- (1) REPORTABLE: **YES** / ~~NO~~
(2) OF INTEREST TO OTHER JUDGES: **YES** / ~~NO~~
(3) REVISED: ~~YES~~ / **NO**

13 August 2026
DATE

SIGNATURE

In the matter between:

TAXPAYER TQ

APPELLANT

and

**THE COMMISSIONER FOR THE
SOUTH AFRICAN REVENUE SERVICE**

RESPONDENT

J U D G M E N T

This judgment was prepared and authored by the Judge whose name is reflected and is handed down electronically by circulation to the Parties/their legal representatives by email and by uploading it to the electronic file of this matter on CaseLines. The date for hand-down is deemed to be on 13 August 2026.

MALI, J*Introduction*

[1] This appeal challenges the respondent's decision to dismiss the appellant's objection against two separate tax determinations: the assessment of Value-Added Tax (VAT) and the concurrent imposition of an Understatement Penalty (USP). The appellant is an entity, amongst others, consulting in information technology.

[2] The appellant claimed input tax for the 08/2017 VAT period in the amount of R1 946 952.13 and for the 10/2017 VAT period in the amount of R4 425 613.56. The total amount of input tax claimed was R6 372 565.69.

[3] The basis for disallowing the above-mentioned input tax claims is that the claims were made on fictitious supporting documentation, in contravention of section 16(2)¹ read with section 20(4) of the Value-Added Tax Act 89 of 1991² ("VAT Act").

¹ Section 16(2) of the VAT Act provides:

"No deduction of input tax shall be made in terms of this Act in respect of a supply, unless—

- (a) a tax invoice or debit note or credit note in relation to that supply has been provided in accordance with section 20 or 21 and is held by the vendor making that deduction at the time that any return in respect of that supply is furnished; or
- (b) a tax invoice is in terms of section 20(6) or (7) not required to be issued, or a debit note or credit note is in terms of section 21 not required to be issued; or
- (c) sufficient records are maintained as required by section 20(8) where the supply is a supply of second-hand goods or a supply of goods as contemplated in section 8(10) and in either case is a supply to which that section relates:..."

² Section 20(4) of the VAT Act provides:

(4) "Except as the Commissioner may otherwise allow, and subject to this section, a tax invoice shall contain the following particulars:

- (a) The words "tax invoice" in a prominent place;
- (b) the name, address and registration number of the supplier;
- (c) the name and address of the recipient;
- (d) an individual serialized number and the date upon which the tax invoice is issued;
- (e) a description of the goods or services supplied;
- (f) the quantity or volume of the goods or services supplied;
- (g) either—
 - (i) the total amount of the tax charged, the consideration, excluding tax, and the consideration, inclusive of tax, for the supply; or
 - (ii) where the amount of tax charged is calculated by applying the tax fraction to the consideration, the consideration for the supply, a statement that it includes a charge in respect of the tax and the rate at which the tax was charged."

[4] The Commissioner further imposed an understatement penalty (“USP”) for the 08/2018 VAT period at the rate of 150% in terms of sections 222 and 223 of the Tax Administration Act 28 of 2011 (TAA), consistent with the behaviour of intentional tax evasion and the conduct of a standard case. The USP amount imposed is R2 920 428.19.

[5] Section 222 of TAA governs **understatement penalties USP**), detailing when SARS must impose a penalty, how to calculate the shortfall, and the core definitions of an understatement. Section 223 of TAA sets out the understatement penalty percentage table and the rules for penalty remission.

Grounds of Appeal

[6] The appellant advanced the following four grounds of appeal:

- a. The USP is irrational and unreasonable, unfair, unlawful and premature alleging that the Commissioner failed to investigate the sole Director of the Company Mr Witness 2’s complaint that the appellant’s e-filing was compromised.
- b. The Commissioner failed to consider that the appellant’s email provided at the time and telephone numbers were no longer active;
- c. During the time when the input tax claims were made, *“the appellant was fully employed and that the activities of the intellectual properties were emanating from different country, mainly in the Republic of Zimbabwe”*; and
- d. At the time the appellant profile was utilised to conduct fraudulent filing of tax refund claims, the Commissioner *“in the light of its suspension should have at least required the appellant to take oath in form of affidavit binding himself and/or confirming the authenticity of the documents submitted to evade entertainment and processing of fraudulent claims as measure given the suspension then”*.

Facts

[7] It is common cause that the VAT201 return for the 08/2017 VAT period was submitted to SARS through the appellant’s profile, declaring output tax in the amount of R1 233 991.00 whilst claiming an input tax amount of R1 946 952.13, resulting into a refundable amount of R1 822 961.13.¹⁴

[8] SARS ‘verification process identified the declaration for verification audit due to the anomalies found. The appellant’s pattern was to submit NIL returns. The sudden jump in the appellant’s VAT 201 declarations from NIL returns to significant sum raised alarm with SARS.

[9] During the verification audit, SARS examined the suppliers' invoices and made telephonic enquiries with the suppliers to confirm whether they had issued the invoices to the appellant. The appellant was additionally requested to substantiate its dealings with the suppliers and was therefore expected to respond to the verification letter.

[10] On 10 September 2017, the appellant complied with this request by uploading supporting documentation through appellant's eFiling profile. The documents submitted included output tax and input tax schedules, supplier schedules, and several invoices, all of which bore appellant VAT registration number 4xxxxx. These invoices were allegedly issued by Company One, Company Two, Company Three, Company Four (Pty) Ltd.

[11] The abovementioned suppliers were contacted by SARS, and they uniformly denied issuing the invoices on which the appellant sought to rely. On the strength of those denials, SARS formed the view that the appellant's claim was underpinned by fictitious documentation. As for the October 2017 tax period, SARS followed the same verification procedure. Once again, the appellant furnished supporting documents which upon verification with the purported suppliers, were confirmed to be fictitious.

Issue

[12] The present dispute raises two primary issues for determination: first, whether the respondent acted justifiably in disallowing the input tax claimed by the appellant; and second, whether the understatement penalties imposed by the respondent were lawfully and correctly levied.

Law

[13] Section 102 of the Tax Administration Act 28 of 2011 provides as follows:

"Burden of proof.—(1) A taxpayer bears the burden of proving—

- (a) that an amount, transaction, event or item is exempt or otherwise not taxable;
- (b) that an amount or item is deductible or may be set off;"

Evidence

[14] The appellant's case is that it did not file any of the returns in question. According to the appellant, its eFiling profile was compromised, and the returns and supporting documents relied upon by the respondent were neither submitted nor authorised by the appellant. The appellant further contends that it has no knowledge of the documents referred to by the respondent.

[15] The appellant tendered evidence through two witnesses, Mr Witness 1, an erstwhile employee of the appellant, and Mr Witness 2, the director of the appellant. Mr Witness 1's evidence was that the IP address used to access the eFiling system and submit the returns originated from Zimbabwe. The appellant therefore contends that it could not have filed the documents in question. In support of this contention, the appellant submitted that its director/member, Mr Witness 2, was in South Africa at the time the returns and supporting documents were allegedly submitted.

[16] Mr Witness 2's evidence is that he was not aware who submitted the VAT201 returns on behalf of the appellant. He first learnt about the submission of the VAT201 returns on 12 March 2019, when he was contacted by SARS official during the verification process. At the time of the VAT201 returns were submitted, he was employed and accordingly did not have time to focus on the appellant's business and therefore the business was not active at that time.

[17] Following that discussion, he subsequently logged onto the appellant's profile when, he realised that there were fraudulent returns for the periods of 2017/08 and 2017/10, as well as fraudulent supporting documents that were submitted to the platform. He later approached a Ms Roses at SARS who according to him confirmed that there were fraudulent activities in the e-filing profile of the appellant. Accordingly, SARS failed to protect the appellant. As already submitted all this was argued without any technical or expert evidence. The only technical or expert evidence he relied on is the evidence of Mr Witness 1 who was not testifying as a technical expert. His evidence was, to the IP address where the returns originated from is in Zimbabwe.

[18] Four witnesses testified on behalf of the respondent. Ms Daisy and Ms Sunflower who are both verification auditors, Ms Roses a service consultant, and Mr Coffee, a digital fraud investigator within the respondent's digital fraud investigation unit.

[19] It transpired from the evidence of Ms Daisy that she conducted a verification audit, which was initiated by a verification letter issued by the Commissioner on 7 September 2017 requesting the appellant to review the VAT201 declaration and correct any errors identified by submitting a request for correction. As alluded in the background facts the suppliers contacted by SARS denied having issued the invoices relied upon by the appellant. Based on these confirmations, SARS concluded that the appellant's claim was supported by fictitious documentation.

[20] Ms Daisy's evidence is collaborated by Ms Sunflower's evidence, as the same *modus operandi* was used by the appellant. Although the suppliers contacted or used by the appellant were not the same as those contacted by Ms Daisy, nevertheless similar results were achieved in that the purported suppliers denied having conducted business with the appellant.

[21] Furthermore, Ms Sunflower testified that she requested the appellant's bank statements from ABSA. There were no payments made by the appellant to the suppliers. The first ABSA letter which the appellant submitted did not contain the registration number of the appellant. Upon follow up Ms Sunflower was informed by ABSA that it had no records for the appellant. This evidence has not been refuted by the appellant.

[22] Ms Roses confirmed that she had assisted Mr Witness 2, to open a case under case number 313063359 but, she could not have confirmed to him that there was fraud on the appellant's profile because at that time, she did not have access to eFiling.

[23] Mr Coffee, an Investigator from the Digital Fraud Unit testified for the respondent, stating that he began investigating the appellant's matter in March 2024. The investigation sought to establish whether fraud or compromise had occurred, or whether the eFiling system had been compromised. He concentrated on the August and October 2017 returns, where the vendor had claimed input tax and was later found to have acted fraudulently.

[24] His duties included identifying the individual who submitted the documents and registered the profile. He provided a clear explanation of the pre-2019 eFiling processes and the practice of password sharing.

[25] A taxpayer is assigned a tax user ID, and passwords are stored in encrypted or masked form, inaccessible to investigators in their original format. Each identical password produces a unique masking, meaning different passwords yield different maskings. He noted that several profiles were registered under the company in 2014.

[26] He cross-referenced the appellant's profiles by user ID, explaining that SARS assigns a user ID upon tax type registration, followed by a login name. He reiterated the password masking process and confirmed that different passwords produce different maskings. The masking evidence was tied to Mr Witness 2's testimony that an IP address registered in Zimbabwe was used while the Director was in South Africa. Mr Coffee testified that a Zimbabwean IP address could be masked to appear as though it originated elsewhere a practice known as IP spoofing, which complicates geographical verification.

[27] In his expert assessment, there was no evidence of password compromise. If the profile had been compromised, the appellant would not have continued using it, particularly as it remained in use beyond 2018. When SARS transitioned platforms in 2019, taxpayers were required to unify their profiles. The appellant did so on 1 July 2019, selecting a username and setting a password, and logged in successfully that same day. This suggests that any compromise would have been apparent to the appellant as early as 2017, when it was called upon to submit supporting documentation.

[28] After the submission of the returns, the appellant, represented by Mr Witness 2, was requested to make his laptop available for imaging. Mr Witness 2 failed to do so, advising that the laptop had been confiscated by his employer. In the light of this, Mr Coffee concluded that the e-Filing system disclosed no evidence of compromise and that it had consistently been utilised by the same individual. He further opined that had a third party accessed the profile, that party would have substituted the taxpayer's banking details with alternative details; however, the banking details on record remained unchanged. The evidence detailed above remained unchallenged.

Analysis

[29] The central contention advanced by the appellant, both in its pleadings and during the hearing, is that its email address and cellular telephone number on record with SARS had fallen into disuse, rendering them susceptible to exploitation by unauthorised third parties without the appellant's knowledge. The email address in question had previously belonged to the company; however, owing to the company ceasing operations, the email account was deactivated to curtail hosting expenses.

[30] The advent of digital communication and electronic record-keeping has fundamentally altered the evidentiary landscape in South African courts. The increasing prevalence of electronically generated records – including e-Filing data, IP address logs, cell phone records, and system access logs – necessitates a clear understanding of the principles governing the admissibility and evidential weight of such material. This judgment, which deals extensively with allegations of e-Filing compromise and digital fraud, calls for a restatement of the applicable legal principles.

[31] The starting point for any consideration of electronic evidence is the Electronic Communications and Transactions Act 25 of 2002 ("ECTA"). Section 15 of ECTA provides that the rules of evidence must not be applied so as to deny the admissibility of a data message on the mere grounds that it is constituted by a data message, or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in

its original form. The Act follows an inclusionary rather than an exclusionary approach to electronic evidence, seeking to facilitate rather than impede the admission of data messages.

[32] However, section 15 does not render a data message admissible without further ado. The section does not exclude the common law of evidence, and electronic evidence remains subject to the ordinary requirements of admissibility: relevance, authenticity, and reliability. As was held in *S v Brown*³ the first step in considering the admissibility of electronic evidence is to examine its nature to determine what kind of evidence one is dealing with and what the requirements for its admissibility are. It is further held that that given the potential mutability and transient nature of images generated, stored, and transmitted by an electronic device, they are more appropriately dealt with as documentary evidence rather than real evidence. This classification carries significant consequences: where electronic evidence is treated as documentary, the ordinary requirements apply the original document must be produced, and its authenticity must be proved.

[33] A critical question in the law of electronic evidence is whether a data message should be treated as real evidence or documentary evidence. This classification determines the admissibility requirements that must be satisfied.

[34] In *S v Ndiki*⁴ the court held that a data message the admissibility of which relies on the functionality of the electronic device and its accompaniments is classified as real evidence. Conversely, computer printouts whose veracity depends upon the credibility of a signatory are classified as documentary evidence.

[35] A preferable approach is to consider the nature of the data message and determine whether it relies on the credibility of a person or a machine. If the credibility of the evidence depends substantially upon a computer or mechanised process (such as automatically generated system logs, IP address records, or GPS data), then that evidence should be treated as real evidence. If the credibility depends substantially upon a person (such as emails or social media posts containing human statements), then it should be treated as documentary hearsay.

[36] The authenticity of digital evidence is a foundational requirement. Courts will only admit electronic records if they can be shown to be what they purport to be and are sufficiently reliable to be trusted. Given the ease with which digital evidence can be altered, manipulated, or preserved, the integrity of the evidence must be established.

³ 2016 (1) SACR 206 (WCC).

⁴ 2007 (2) All SA 185 (Ck).

[37] In determining authenticity and integrity, courts evaluate whether the data message has remained complete and unaltered; the reliability of the systems generating or storing the data; and whether the way the data was generated, stored, and communicated is sufficiently reliable.

[38] Section 15(1)(b) of ECTA provides that a data message is not inadmissible on the grounds that it is not in its original form if it is the best evidence that the person adducing it could reasonably be expected to obtain. This provision does not abolish the best evidence rule but rather qualifies it in recognition of the fact that electronic evidence frequently exists in multiple copies or layers, and requiring production of the “original” may be impractical or impossible.

[39] The onus rests on the party seeking to introduce digital evidence to prove its authenticity. Where the evidence concerns technical matters such as system compromise, IP address manipulation, or password integrity, the party bearing the burden must adduce appropriate expert evidence to establish the reliability and integrity of the systems in question. The absence of such expert evidence may be fatal to the admissibility or probative weight of the evidence, particularly where the defence rests substantially upon allegations of system compromise or unauthorised access.

[40] Where a data message contains statements made by a person, it may constitute hearsay and must be dealt with in terms of the Law of Evidence Amendment Act 45 of 1988. However, automatically generated records such as system logs or computer-generated printouts that do not depend on human credibility do not constitute hearsay.

[41] Electronic evidence is admissible under section 15 of ECTA but remains subject to the common law requirements of relevance, authenticity, and reliability. The first step is to classify the electronic evidence as either real evidence or documentary evidence, having regard to whether it depends substantially on a machine or a person for its credibility. The party adducing electronic evidence bears the burden of proving its authenticity and integrity.

[42] Automated or system-generated records do not constitute hearsay, but records containing human statements may do so. Expert evidence is required where the authenticity, integrity, or reliability of electronic systems is in dispute. The weight to be attached to electronic evidence depends on the reliability of the systems generating it and the way it was preserved and presented.

[43] Applied to the present case, these principles require that the appellant, having alleged that its eFiling profile was compromised by third parties, bore the onus of establishing that compromise through reliable evidence. In the absence of expert IT evidence addressing the integrity of the eFiling system and the alleged compromise, the appellant’s claim cannot

succeed. Furthermore, the evidence adduced by SARS including the Investigator's testimony regarding password masking, IP address logs, and system access pattern constitutes real evidence generated automatically by the eFiling system, the reliability of which was properly established through the Investigator's expert explanation of the relevant technological processes.

[44] However, section 15 does not render a data message admissible without further ado. The section does not exclude the common law of evidence, and electronic evidence remains subject to the ordinary requirements of admissibility, i.e. relevance, authenticity, and reliability. As was held in *S v Brown*⁵ the first step in considering the admissibility of electronic evidence is to examine its nature to determine what kind of evidence one is dealing with and what requirements for admissibility are.

[45] A preferable approach is to consider the nature of the data message and determine whether it relies on the credibility of a person or a machine. If the credibility of the evidence depends substantially upon a computer or mechanised process (such as automatically generated system logs, IP address records, or GPS data), then that evidence should be treated as real evidence.

[46] Although the burden of proof rests squarely upon the appellant to establish that its profile had been compromised, the appellant failed to adduce the evidence of an Information Technology expert in support of this proposition. Mr Witness 1, who testified on behalf of the appellant, is not an IT specialist. Notably, the entire defence and indeed the grounds of appeal rests upon alleged breaches of information technology systems, which are matters requiring specialised expertise. Despite this, the appellant persisted in its assertion that SARS had compromised its IP Address, without tendering any expert evidence to substantiate that claim. It is trite that in civil proceedings the burden of proof lies with the Plaintiff to establish its case on a balance of probabilities.⁶

[47] Furthermore, rule 6 of the SARS eFiling Rules imposes an affirmative obligation upon a registered user to change a compromised password. The Rule provides as follows:

"If the user ID or access code has been compromised or is suspected of being compromised in any manner, the registered user must inform SARS accordingly and must reset the access code without delay."

⁵ 2016 (1) SACR (WCC).

⁶ See *Pillay v Krishna and Another* 1946 (AD) 946.

[48] Notably, Mr Witness 2 remained conspicuously silent regarding the banking details, which were not altered by the alleged fraudsters. It stands to reason that any person seeking to benefit from the VAT refunds would have changed the banking details to facilitate payment into a fraudulent account. On the evidence adduced before this Court, the appellant was the party who either benefitted or stood to benefit from the VAT refunds in question.

[49] In any event, section 250(2) of TAA provides that a vendor or taxpayer is responsible for a return made or purporting to be made or signed by or on behalf of a person. The document is regarded as duly made and signed by the person affected unless that person proves that the return was not made or signed by that person or on that person's behalf. Subsection (2) applies mutatis mutandis to other documents submitted to SARS by or on behalf of a person.

[50] For the foregoing, Mr Witness 2 is found to be an unreliable witness. Having regard to the totality of the evidence presented herein, the appellant and/or vendor has failed to discharge its onus of proving that the VAT refund returns were not made, signed, and filed by it.

[51] Consequently, SARS was justified in disallowing the input tax claims and in imposing the understatement penalties. The appellant's argument that no prejudice was suffered by SARS because the refunds were not paid out is misplaced. Had SARS not identified the relevant VAT periods for verification, the refunds would indeed have been paid. In *Purlish Holdings (Proprietary) Limited v The Commissioner for the South African Revenue Service*,⁷ the Supreme Court of Appeal observed as follows:

“ ... This would have resulted in all the funds paid in by the appellant being reflected as a credit in the appellant's account with SARS, as a result of which SARS was unable to channel such funds for the relevant governmental activities. This evidence was not challenged under cross-examination. Mrs Porter further stated that SARS would have suffered substantial financial loss if it had acceded to the appellant's request for a refund without conducting an audit. It is also clear that had it not been for the audit, the appellant's liability to pay VAT would not have been exposed, as it had not registered for VAT. Further to that, Mrs Porter testified that the resource allocation in the form of additional time and human capital necessitated by the extensive audit also constituted prejudice to SARS, as such resources could have been utilised for other matters. Given the circumstances of this matter, I agree that the use of additional SARS resources for purposes of auditing the appellant's tax affairs indeed prejudiced SARS.

⁷ [2019] ZASCA 4; 81 SATC 204.

As correctly conceded by counsel for the appellant in argument before this court, prejudice is not only determinable in financial terms.”

[52] Section 222(1) of the Tax Administration Act 28 of 2011 reads as follows:

“In the event of an ‘understatement’ by a taxpayer, the taxpayer must pay, in addition to the ‘tax’ payable for the relevant tax period, the understatement penalty determined under subsection (2) unless the ‘understatement’ results from a bona fide inadvertent error.”

[53] In the premises, SARS was correct in disallowing the input VAT claims and in imposing the understatement penalties. Accordingly, the following order is granted:

Order

[54] The appeal is dismissed with costs.

NP MALI
JUDGE OF THE HIGH COURT
GAUTENG DIVISION, JOHANNESBURG

Date of Hearing: 01-02 September 2025 and 20-22 October 2025

Date of Judgment: 13 August 2026