

15 March 2024

**TO: CUSTOMERS/DEBTORS OF THE HSRC**

The management of the HSRC has recently been alerted to several bank account scams targeting its customers. Kindly note that it is our top priority to maintain the integrity of our financial transactions and protect you as our clients from fraudulent activities. To this end, HSRC's banking information has remained unchanged since the account's inception in 1991, underscoring our commitment to stability and security against fraud.

The South African Banking Risk Information Centre (SABRIC) has issued a warning about the alarming rise of scams, particularly those involving false notifications of banking detail changes. As a result, we intend to keep our customers informed.

It's crucial to understand that criminals are constantly devising new ways to exploit unsuspecting victims. However, many scams are just recycled tactics meant to deceive new victims. Therefore, all government departments, universities, and research partners must be on high alert for business-to-business identity theft scams. These scams involve the fraudulent rerouting of payments into accounts that do not belong to the intended suppliers.

Scammers are not to be underestimated. They often exploit the good reputation of credible organisations like the HSRC and pretend to be the 'new account manager.' They then send an email or letter, complete with fraudulent letterheads, to inform the targeted business of changes in banking account details. They will insist that all future payments be made into the new account. But make no mistake, these new bank details are under the control of the fraudsters.

While this may be an old scam, the attention to detail by the perpetrators can make their communication appear genuine, putting unsuspecting HSRC clients such as government departments, universities, and research partners at risk. Also, fraudsters ensure that any correspondence from the targeted business to verify the notification is redirected to a member of their group who will confirm the instruction as legitimate. It is crucial for all entities, including government departments, universities, and our research partners, to rigorously verify any such communication about changes to banking details. Authentic verification channels should always be utilised before adjusting payment instructions.

The HSRC is registered on the Central Supplier Database (CSD) as supplier MAAA0057171. The National Treasury has verified the banking details of the HSRC.

**Prevention Tips:**

- Verify all notices of change in bank account details.
- Beware of false confirmation emails from almost identical email addresses, such as .com instead of co.za, or slight variations from genuine addresses that can be easily missed.

**HSRC Board:** Dr Reginald Cassius Lubisi (Chairperson), Dr Kgomotso William Kasonkola, Dr Deenadayalen Konar, Prof. Ibbo Day Joseph Mandaza, Ms Shameme Manjoo, Dr Alex Mohubetswane Mashilo, Prof. Zerish Zethu Nkosi, Adv Faith Dikeledi Pansy Tlakula, Prof. Fiona Tregenna, Prof. Sarah Mosoetsa (CEO)

[www.hsrc.ac.za](http://www.hsrc.ac.za)

- The identity of the person your business is dealing with must always be confirmed.
- Never throw away your business (and suppliers') invoices or any communication material that contains letterheads. Instead, you must shred all unused documents.
- Verify any request for or changes to information with the supplier over the telephone, ideally with someone you have known for some time.
- Use your database contact details to confirm notifications for any changes of banking details via official correspondence with your suppliers (such as a letter), preferably before processing the next payment.
- Do not publish your bank account details on the internet. This private information can be used fraudulently to trick genuine customers into making payments to alternative accounts.
- Please do not disclose your company's private information to third parties who are not entitled to receive it or third parties whose identities cannot be accurately verified.

### **If you fall victim to this type of fraud:**

- It is always prudent to first notify the Police.
- You can also commence a civil recovery of these monies against the fraudster. It may also be necessary to use tracing mechanisms to trace the identity of the fraudsters or even freezing injunctions to freeze the assets of the fraudsters.
- Check with your insurer to see if it is an insurable loss.

As the HSRC is not a party to the transaction, we cannot act on behalf of the government departments, universities, and research partners regarding the recovery of monies wrongfully deposited. The outstanding debt will remain until the amount is settled in our bank account.

Do not hesitate to contact the HSRC if you have received any correspondence regarding alleged changes in the HSRC's banking account details. We would like to establish whether other government departments, universities, and research partners' customers were targeted.

Contact the Office of the Chief Financial Officer: Brilliant Ndubane at [BNdubane@hsrc.ac.za](mailto:BNdubane@hsrc.ac.za)

The HSRC also has a fraud hotline for anonymous reporting.

Free Fraud Hotline:	0800 205 138
Email	<a href="mailto:hsrc@thehotline.co.za">hsrc@thehotline.co.za</a>
SMS	30916
Fax	086 726 1681
Website	<a href="http://www.thehotline.co.za">www.thehotline.co.za</a> with number 0800 205 138 to report

We value your cooperation and vigilance in these efforts. Together, we can protect our community of stakeholders from fraudulent activities.

**Jacomien Rousseau**  
**Chief Financial Officer**