25 July 2024

Dear HSRC Stakeholder,

Management has been made aware of several bank account scams involving HSRC stakeholders. Please note that the HSRC has not changed its banking details since the account was opened in 1991. The South African Banking Risk Information Centre (SABRIC) has also warned that a scam informing people of a 'Change in Banking Details' is rising in the country.

Criminals are always on the lookout for new ways to make easy money. However, most fraud is just old ideas that catch new people. Stakeholders must be aware of business-to-business **identity theft** scams involving fraudulent transactions into accounts not belonging to suppliers.

Perpetrators of this scam usually assume the identity of an entity, in this case, the HSRC. The fraudsters may call the targeted business to introduce themselves as the new account manager at the HSRC. An email or a letter using fraudulent letterheads is sent to inform the targeted business of changes in the HSRC's banking account details. The perpetrators will request that all future payments be made to the new account. Please be warned that the new bank details belong to an account under the control of the fraudsters.

This is an old scam, but the perpetrators' attention to detail makes these communications seem authentic, which can turn unsuspecting stakeholders into easy targets. These perpetrators ensure that correspondence from the targeted business to verify the notification is diverted to a member of their group who will confirm the instruction as legitimate. Businesses should take the time to verify the notifications for changes in banking details from their suppliers even when under pressure to do so at the end of the month unless the legitimacy of the notice is certain. Businesses should always ensure that they are satisfied with the validity of communication from the supplier.

Tips to avoid becoming a victim of change of banking account details scams include:

- Verify all notices of change in bank account details.
- Beware of false confirmation e-mails from almost identical e-mail addresses, such as .com instead of co.za, or slight variations from genuine addresses that can be easily missed.
- 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 (such as a letter) with your suppliers, 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 stakeholders into making payments to alternative accounts.
- Ensure that your company's private information is not disclosed to third parties who are not entitled to receive it, or third parties whose identities cannot be accurately verified.

Pretoria Office: 134 Pretorius Street, Pretoria, 0002, South Africa. Private Bag X41, Pretoria, 0001, South Africa.
Tel: +27 12 302 2000 Fax: +27 12 302 2299/2149
Cape Town Office: The Yacht Club, 2 Dockrail Road, Foreshore, Cape Town 8001, South Africa. Private Bag X9182, Cape Town, 8000, South Africa.
Tel: +27 21 466 8000 Fax: +27 21 461 2099
Durban Office: Connect Space, 102 Stephan Dlamini Road, Musgrave, Durban, 4001. PO Box 37429, Durban, South Africa.
Tel: +27 31 242 5400 Fax: +27 31 242 5401
Pietermaritzburg Office: Old Bus Depot, Mbubu Road, Sweetwaters. PO Box 90, Msunduzi, 3200, South Africa.
Tel: +27 33 324 5000 Fax: +27 33 324 1131

Please note that research teams will no longer issue HSRC invoices. From now on, the finance office will issue these. The two employees responsible are Ms Amanda Vers **AVers@hsrc.ac.za** and Ms Mpho Radingwane **MRadingwane@hsrc.ac.za**. HSRC invoices will be password-protected to ensure no changes can be made. For verification, HSRC-verified banking details are available on the National Treasury Centralised Supplier Database (**CSD**) as supplier number: **MAAA0057171**.

What can you do as a victim of this type of fraud?

- Once you are a victim of this type of fraud, 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.
- Finally, 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 stakeholders regarding the recovery of monies wrongfully deposited. The outstanding debt will remain until the amount is settled in our bank account.
Please contact the HSRC if you have received any correspondence regarding the change in banking account details. We would like to establish if any other stakeholders were targeted.

Please report any suspicious activity to the HSRC fraud to the hotline below:
Free Call number – Fraud Hotline: **0800 205 138**
Free Call number – Research Ethics Hotline: **0800 212 123**
SMS: **30916**
Email: **hsrc@thehotline.co.za**

Your cooperation in this regard will be highly appreciated.

Yours Sincerely,

Ms Jacomien Rousseau
Chief Financial Officer