

Important!

Urgent Wallet ID Payment Scam ALERT

Dear Colleagues,

**Communication summary**

This pertains to a Wallet ID payment scam, and encompasses (1) How the scam works (2) Advice for clients who have received the link and NOT clicked it (3) advice for clients who have clicked the link

Please be advised that there is currently a **Wallet ID payment scam targeting Standard Bank customers**. The fraudsters orchestrate the scam using the following methods:

* sending an e-mail or SMS messaging embedded with phishing/smishing links,
* they telephonically contact unsuspecting victims with an intent to get them to compromise their card credentials and OTP required to enable cash out using the smart device /wallet ID payment platforms.

**How the scam works:**

* Customer will receive a link via e-mail or SMS
* The link may entice them with bargain deals
* Upon clicking the link, the customer may be requested to capture or update their card details
* The request is often accompanied by the threat that if the card details are not captured or updated, the customer’s card/account will be blocked
* If the customer receives a telephone call, the fraudster will ask the customer for their card details to capture the order on their behalf or to update their banking details
* Based on the above, the fraudsters then registers the customer for a wallet ID
* An OTP is generated to provision the card and the customer either captures the OTP or shares it with the caller
* [Click here](https://encrypt-track6.standardbank.co.za/w/track/FAQs/caT4_04bMjKzMDOytDQ1YDcxMzFm98nMS0nUK0vM80hNLUpJzXMoLkkEihSlJCXmZesl5-tVJbIDAAAA__8GOA73HIW) for FAQs

**Advising customers:**

|  |  |
| --- | --- |
| **Clients who have received the link and NOT clicked** | **Clients who have already clicked on the link** |
| * Do not panic * Do not click on the link * Do not capture you card number, expiry date and CVV number on a link shared * Do not share your CVV telephonically with a suspicious caller * Please share the suspicious emails or SMS with the Bank by creating a new email with the suspicious email or SMS as an attachment. * Take a screenshot of the SMS, include the cell phone number of the SMS it came from * Send it to [phishing@standardbank.co.za](mailto:phishing@standardbank.co.za) * Delete the e-mail or SMS immediately thereafter | * They should immediately call our fraud line on 0800 222 050 or report fraud on: [reportfraud@standardbank.co.za](mailto:reportfraud@standardbank.co.za)   **Please NOTE that Standard Bank:**   * Will NEVER send the customer an e-mail or SMS with a link asking you to capture your card details * Will NEVER send the customer an e-mail or SMS with a link to access your online banking profile |

If you would like to read about the scam in more detail, please refer to attachment 1 of this email.

Should you receive any queries from our customers in this regard, please follow the guidelines above.

Customers can also be directed to the Security Centre on the Standard Bank website for more information and tips on banking safely.

Regards

Fraud Risk Management

van Heerden, Linda L Dawson, Natalie N

VB Leadership VB Service Managers

**Email Attachment**

**How the Wallet ID payment scam works**

Please be advised that there is currently a Wallet ID payment scam targeting Standard Bank customers. The fraudsters orchestrate the scam using the following methods:

* sending an e-mail or SMS messaging embedded with phishing/smishing links,
* they telephonically contact unsuspecting victims with an intent to get them to compromise their card credentials and OTP required to enable cash out using the smart device /wallet ID payment platforms.

Customers are first enticed with a “too good to be true deal” or threatened that their accounts will be blocked should they not respond to the email (phishing), sms (smishing) or telephone call (vishing). This is followed by a link for the customer to capture their card details i.e card number, expiry date and cvv number.

Once the customer is compromised by clicking on the link and capturing their card details or sharing them telephonically, the customer’s card is then registered on the fraudster’s smart device. Upon registration, an OTP (one time pin/password) is required to provision the card for payments.

The fraudsters then contact the customer via e-mail, sms or telephonically advising them that they will receive an OTP to finalize their purchase. An OTP is generated for the provisioning of the compromised card to enable future payments. The customer unknowingly captures or shares this OTP with the fraudsters, thinking that they are finalizing their purchase.

Please note that the provisioning of the card for payments is ONLY done once and thereafter payments can be conducted without an OTP.