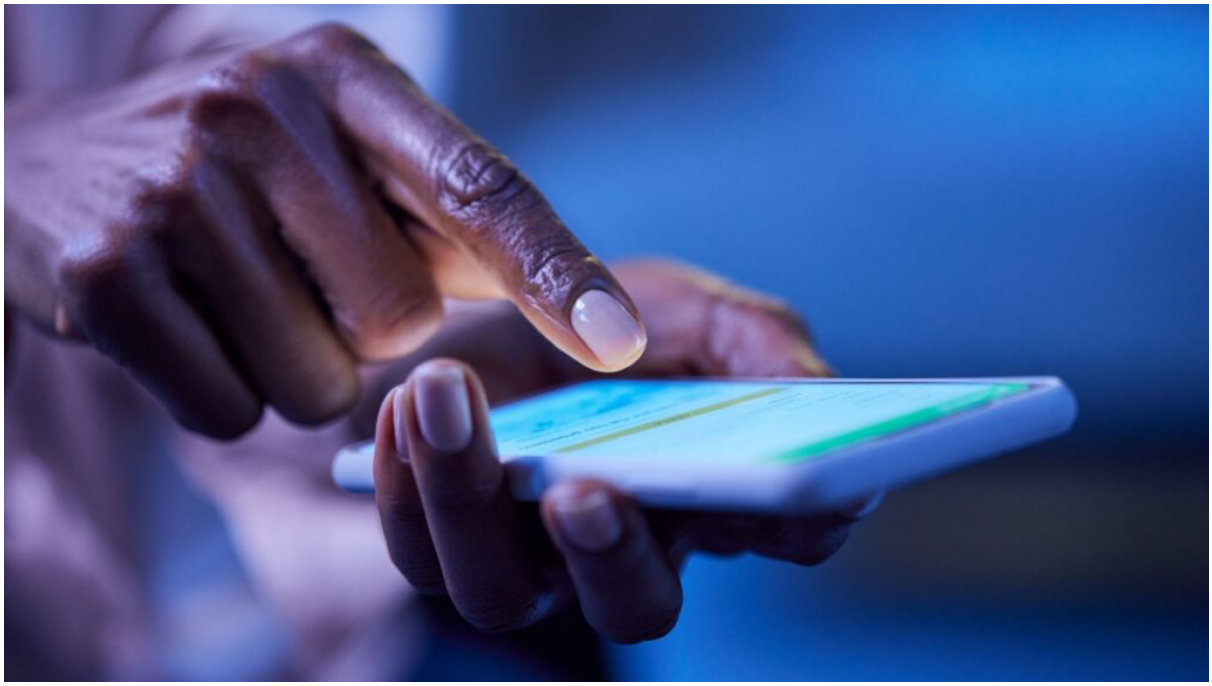
Warning to South Africans with banking apps on their phones



The National Financial Ombud Scheme (NFO) has warned South Africans that fraudsters are increasingly targeting banking apps and virtual cards, with one victim losing R500,000.

Virtual banking cards have become a standard feature across all major digital banking platforms. They allow customers to make payments online or in-store by simply tapping their phones or wearable devices.

With unique card numbers, expiry dates, and CVV codes, they are designed to be a secure and convenient alternative to physical cards or cash.

They cannot be lost, stolen, or duplicated in the same way traditional cards can. However, according to the NFO, fraudsters are increasingly targeting them, and the rise in related scams is alarming.

The NFO has recorded a steep 73% increase in digital banking fraud complaints, jumping from 1,436 cases between January and May 2024 to 2,483 during the same period this year.

Between January 2024 and May 2025, digital fraud complaints exceeded ATM fraud cases by 3,350 incidents, indicating a clear shift from physical to virtual card fraud.

Nerosha Maseti, the Lead Ombud for Banking and Credit at the NFO, said the convenience of virtual cards is undeniable, but so are the risks.

“While virtual cards offer enhanced convenience and security, they are not immune to fraud, and opportunities for fraudsters to exploit unsuspecting bank customers remain,” she said.

Maseti explained that virtual cards are typically compromised through unauthorised access to a customer’s banking app.

Cybercriminals rely on phishing, smishing, and vishing tactics to trick people into sharing personal information. In most reported cases, fraud occurs only after a customer’s digital banking credentials have been stolen.

“Fraudsters can create virtual cards and then use the virtual card credentials to perform transactions once gaining access to a customer’s digital banking profile,” she said.

“This happens when bank customers have compromised their confidential access credentials, shared One Time Pins (OTPs), or accepted authentication messages to create virtual cards.”

Big money is at stake

Nerosha Maseti, the Lead Ombud for Banking and Credit at the NFO
In many cases reported to the NFO, victims were unaware they had virtual cards linked to their accounts.

Despite awareness campaigns by banks, including SMS, email, and in-app warnings, most complainants said they were unfamiliar with how virtual cards work or the risks involved.

Maseti cited a case where a consumer fell victim to a vishing scam. Fraudsters, pretending to be from the bank, convinced her to hand over her online banking credentials.

They used this access to create multiple virtual cards and make online purchases totalling R500,000. The transactions were authenticated through in-app approvals on the victim's own phone.

The bank refused to refund her, arguing that the compromised transactions were approved from her device using her correct login details.

It provided proof of the virtual card creation, the authentication messages sent to her phone, and confirmation that she had approved them.

The NFO agreed with the bank, ruling that there was no evidence of maladministration or security failures on the bank's part.

"The facts showed that the consumer had compromised her online banking credentials and approved the in-app messages required to authorise the online card purchases in question," Maseti said.

"Consumers are responsible for keeping their confidential access credentials safe and secure. The bank will never request disclosure of this information."

Maseti stressed that prevention is the only effective defence against virtual card fraud. Consumers should never share their PINs, passwords, OTPs, or virtual card details.

They should carefully read all notifications before approving transactions, as fraudsters may disguise fraudulent requests as legitimate ones.

To stay safe, Maseti recommended enabling multi-factor authentication on banking apps, using secure internet connections instead of public Wi-Fi, and setting strong, unique passwords, ideally stored in a password manager.

Consumers should set transaction limits on virtual cards, avoid saving card details in browsers or apps, and disable auto-save features.

If fraud is suspected, it must be reported to the bank immediately, as only the bank can block cards or recover funds.

The NFO cannot intervene until the bank has responded to a customer's complaint. If the bank's resolution is unsatisfactory, the matter can then be referred to the NFO for investigation.