Jersey Financial Services Commission

Press release

Fraud warning: impersonation of Nedbank Private Wealth Limited, Jersey Branch (NPWL)

Issued: 22 June 2026

We are warning members of the public about a scam that has targeted a Jersey resident. We are aware that a Jersey resident has been cold called by scammers that have spoofed a legitimate NPWL telephone number (+44 1624 645000) and falsely claimed they are part of NPWL's fraud team. We are also aware that the scammers are using the name 'Michael Stevens', when contacting Jersey residents.

Spoofing is when someone disguises themselves as a trusted person or business to deceive their victim. Common types of spoofing include:

- **caller ID spoofing:** manipulation of the caller identification to display a trusted name or number
- **email spoofing:** fraudsters can forge email addresses, so it appears to come from a legitimate source
- **website spoofing:** fake websites can look identical to official logins to steal your credentials
- **SMS spoofing:** fraudsters send text messages that appear from legitimate sources and often include links to websites that require your details

You can verify that you are corresponding with the genuine NPWL by:

- only using contact details outlined on its official website: Private Wealth Planning & Banking for High Net Worth Clients
- using the contact details found on the reverse of your NPWL debit card
- following NPWL's guidance on fraud, for example: Staying vigilant to impersonation fraud and the use of fake websites - Nedbank Private Wealth

Scams are increasingly prevalent across the banking sector, driven by advances in technology and the growing sophistication of fraudsters. Criminals are exploiting digital channels such as online banking, mobile apps, and social media to target customers with highly convincing phishing and impersonation tactics.

We urge you to:

- be wary of unexpected calls, texts and emails and do not act immediately, especially if there is urgency in the contact
- contact a firm directly to verify the request is legitimate using official contact details
- refuse to disclose any personal or banking information, banks will never ask you for passwords, security information, or one-time passcodes

Remember, if you're not certain that the call, text, or email is legitimate, immediately hang up, do not respond, or click on any links.

If you think you have been targeted

Please report it to:

- the JFSC's Enforcement Division
- the States of Jersey Police
- your bank – if you have already made a payment

Fraud prevention resources

You can follow the Jersey Fraud Prevention Forum on Facebook or LinkedIn for guidance on avoiding scams and what to do if you think you have been scammed:

- https://www.facebook.com/jsyfraudforum
- https://www.linkedin.com/company/jersey-fraud-prevention-forum/

For further enquiries, please contact the JFSC's Enforcement Division.

You can also contact the JFSC's confidential whistleblowing line on +44 (0)1534 887557.