Jersey Financial Services Commission

Press release **29 May 2026**

Fraud warning: Impersonation of bank fraud teams

Following our recent press release, we have become aware of a further cold-calling scam primarily targeting Jersey residents and Jersey-based businesses by pretending to represent various banks and bank fraud teams. They may call you unexpectedly and ask for sensitive security details, such as One-Time Passcodes, to access your online bank accounts and steal your money.

How to protect yourself

We are again urging you to:

- be wary of unexpected phone calls
- never share personal or banking details over the phone, or with anyone you do not know
- never share your security details, including passwords and PIN numbers, with anyone. Your bank will never request to share such details over the phone
- follow our guidance below on how to spot and protect yourself from scams

If you receive an unexpected phone call, message, email, or other contact claiming to be from your bank or other financial institution, check that it is genuine. Only use contact details from the official website or the back of your bank card.

Scammers may use real names, cloned websites, copied branding, and AI generated images or voices to impersonate banks or other financial institutions. Their aim is to convince you they are genuine and pressure you into sending money or sharing personal information.

How to spot a scam

If you receive an unexpected message, friend request, email, text, call or letter, stop, pause and look for signs that it could be a scam. These can include but are not limited to:

- requests for sensitive or personal information – especially if they claim to be preventing an ongoing fraud
- spelling mistakes and poor grammar
- pressure and urgency to do something – such as moving money to a safe account to stop a fraud
- asking or telling you to click on a link
- unusual payment methods
- unusual ways of contacting you
- promises or offers that seem too good to be true
- website addresses and social media accounts with small changes from genuine sites

What to do

STOP – pause before responding to unexpected calls, messages, or adverts, especially if you are being asked to act quickly.

CHECK – confirm who you are speaking to. Use contact details from an official website or bank card.

PROTECT – never share personal or financial information with someone you do not know. Even if they claim to be your bank or financial institution.

If you think you have been targeted

Please report it to:

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

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. Further guidance is available through your bank's website.

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

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