We all lead busy lives, and it just takes a second to be tricked by a scam unexpectedly. There is an ongoing threat of text message and phone call fraud.

It is essential to stay alert and protect your personal information. Fraudsters often use the names of legitimate institutions (including AIB) to trick individuals into sharing personal information.

Tips to safeguard yourself from scammers:

- Avoid clicking on links or calling numbers provided in suspicious messages.
- Never share your login details, passcodes, or card reader code in response to a call or text.
- Never give your card or PIN to anyone. We will never send someone to collect it.
- If you receive an unexpected call, hang up and call back on a known and trusted number.
- Never visit websites or download applications to your device on the back of a suspicious text message or phone call.

If you receive an unexpected message or call, consider whether it may potentially be a scam. Please report the fraud message to us using the form available on the security centre on our website aibni.co.uk/security-centre. Here, you will also find what supports we have available, including our 24/7 fraud support line if you feel you have been the victim of a scam.

We are always here to support you. Stay vigilant and contact us if you have any concerns.

Kind regards
UK Fraud Team

Be Fraud Aware

We want to help you understand more about how to protect yourself and your bank account from fraud.

Fraudulent texts:
Criminals can make fake text messages look like they come from us. They can even insert these fake messages into genuine text conversations we are having with you.
One way of spotting a scam is that our web address will have .co.uk at the end. If it has any other ending like .com, it is definitely a scam.
Be careful and never click a link in a text message - even if it appears to be part of a conversation with us. We don't put links into our text messages.

Fraudulent phone calls:
Criminals can call you pretending to be us. They can even mimic our phone number. But remember:
We will never text you a One Time Passcode to cancel a transaction.
We will never ask you to get a code from your Card Reader to cancel a transaction.
We will never ask you not to log back into your account.
You should not share a One Time Passcode code or Card Reader code with anyone if you get an unexpected call or text message, whoever they say they are, **even if they say they are from our fraud team**.
We will never call you to ask for a code we have sent to you, or to ask why you didn't complete the process in the text message.
These codes are the way to make money leave your account. Never share them with anyone including bank staff

Remember: AIB staff including those working in our Fraud teams will **NEVER** ask you for security information, or for you to transfer money out of your account in any of our email, phone or text communications.

If you do receive an email, text or a phone call that claims to be from AIB and asks you for personal information or to take urgent action, **please do not respond, do not follow the instructions and report it via the form at** aibni.co.uk/security-centre/contact-us/fraud-form or call 028 9034 6034 (8.30am to 5pm Monday to Friday, including bank holidays). We may record your call and there may be a charge from your service provider to call us.

If you notice anything suspicious on your bank account or you believe you have been a victim of fraud, contact us 24/7 on Freephone number 0800 0391 140.

For more security advice and pointers on how to protect yourself from Fraud, do refer to the Government 'scamwiseni' and 'TakeFive' initiatives, and to the list of AIB contact telephone numbers on our secure website www.aibni.co.uk.