

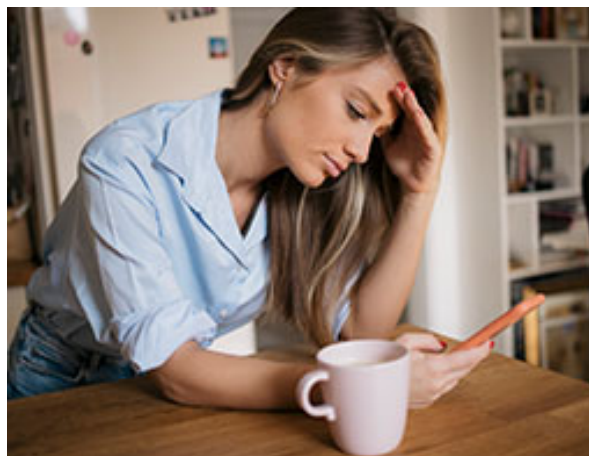


For the life
you're after

Welcome to the Spring edition of your AIB Newsletter

In this issue, we're chatting about how to recognise the warning signs of investment scams, the impact gambling harm can have, and what the recent increase in deposit protection means for you. We've also popped some handy tips into our 'Did you know?' section that you might find useful.

Investment Fraud



Investment fraud is when a criminal creates fake investment opportunity to convince you to put your money into investments that don't exist. You could be contacted by phone, email, social media message or WhatsApp. You might also see adverts on search engines and social media.

For investment scams, criminals might:

- Set up cloned websites pretending to be legitimate investment firms.
- Send you paperwork with official branding to add a layer of credibility to their scams.

- Send you initial payments to show "returns" on your investment, to convince you to invest larger sums of money.
- Use fake celebrity endorsements or fake testimonies from people who've allegedly received large profits.
- Provide you with details of your own previous or current investments to seem legitimate - they can spend hours researching you for a scam.
- Claim to be financial advisers and ask you to download screen-sharing software so they can make investments on your behalf - by downloading the software they gain access to your financial information.

Fake investment opportunities might include: shares and funds, cryptocurrencies, gold, property, carbon, or high-end goods such as wine or art.

Protect yourself from investment fraud:

- Avoid clicking on ads within your social media feeds
- Be cautious of celebrity endorsed investment ads or those offering very high returns on investments.
- If you're contacted out of the blue by phone, email or social media about an investment opportunity, do your research on the company first before you part with any personal or financial information.
- If you're offered a high return on your investment with apparently little or no risk and is also exclusive to you, this is a huge red flag.
- For some types of investment, criminals may pressure you into making a decision with no time for consideration. Only criminals will try to rush or panic you. You can say no and take your time to work out if it's legitimate or not.

Dealing with gambling harm?



Sometimes we recognise a particular pattern in how customers use their current account. For example, if we see gambling transactions on an account, we get in touch to see if we can help.

If you feel that gambling is becoming harmful and putting a strain on your finances, there are simple ways we can help you take control of your money and prevent any future impact on borrowings you may have with us.

We are here to help

- You can add a gambling block to your debit card which means that any transactions we can identify as gambling and betting will be declined. Contact us on **0345 646 0318***, Monday to Friday 09:00-17:00 (excluding Bank Holidays) to find out more and for other ways we can support you.
**Call charges may vary - refer to your service provider*
- Call into one of our seven branches across Northern Ireland (aibni.co.uk/branchlocator)

Don't worry, everything we talk about is confidential.

Other support available

There's also other support available to help you. You can:

- Visit our website which has more information on limiting your spending and taking control of it (aibni.co.uk/help-and-guidance/worried-about-gambling)
- Visit one of the many gambling help websites such as GamCare (www.gamcare.org.uk) or the NHS (www.nhs.uk)
- Consider contacting 'TalkBanStop' which is a combination of a support line and free website-blocking software to help people stop gambling. Call the National Gambling Helpline for further information on **0808 8020 133**

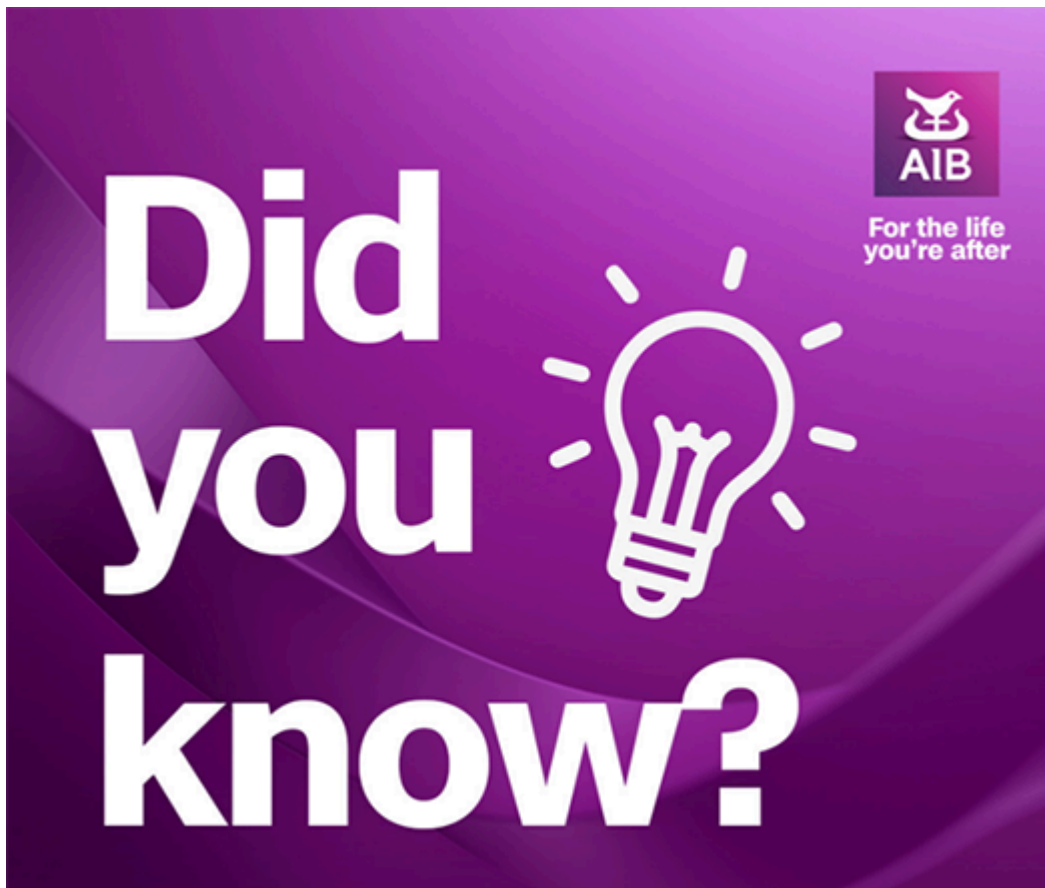
Increase in UK FSCS Deposit Protection to £120,000 - what does this mean for you?



Looking after your savings is important and so is knowing they're safe. The **Financial Services Compensation Scheme (FSCS)** deposit protection limit for eligible deposits has increased from £85,000 to £120,000 for each person as of 1 December 2025.

Some life events can give you a lot of money, for a short time. For example, selling your home or receiving an inheritance can do this. For these situations, the FSCS offers **Temporary High Balance (THB)** protection for up to six months. The THB limit has also increased from £1 million to £1.4 million. You can read more about THB here: fscs.org.uk/making-a-claim/claims-process/temporary-high-balances/

Online Banking for Personal, Personal Business and Partnership accounts



You can access up to 7 years of your bank statements through your app, no more digging through paper files!

Download, print, or review your statements anytime, anywhere and stay organised and in control of your finances.

Here's how you can do this:

1. Log in to the Mobile Banking App.
2. Select 'Settings' then 'Statements'.
3. Choose your account and pick the statement you need.

Your statements are always at your fingertips.

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 (09:00-17:00 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 aibni.co.uk.



The AIB logo and AIB (NI) are trade marks used under licence by AIB Group (UK) p.l.c. incorporated in Northern Ireland. Registered Office 92 Ann Street, Belfast BT1 3HH. Registered Number NI018800. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.