As spring approaches, we are urging customers to remain vigilant against fraud as it can affect any of us at any time.

Criminal activity continues whatever the time of year. We want to alert you to common scams that have been prevalent. We all lead busy lives, and it just takes a second to get caught off guard and fall for a scam. Here is some information and ways to avoid being scammed.

1. Text message fraud

Fraudulent text messages claiming to be from reputable banks, delivery or utility companies and government departments are common. Take a moment and ask yourself does this seem legitimate. Don't click the link in the text message or share your personal or financial information.

Often these messages are followed by a phone call claiming to be us, sometimes even using our actual phone number. End the call immediately. We will never call you and request security codes sent by text message, push message (pop up message) or from your card reader. We will never send a taxi or courier to collect your physical card, PIN or any security details.

2. Phone call fraud

Fraudsters often use phone calls to get your personal and financial information for their own financial gain. They may pretend to be from a legitimate company and may even display a genuine phone number. Common tricks used on these calls is to offer to fix an issue with your broadband or offer a refund. They may try to take control of your device. Never download software or apps, that they suggest, onto your computer or mobile phone as this will allow fraudsters access to your information.

End any unexpected calls. Call the company back on a known and trusted number to verify the call.

3. Investment fraud

Investment frauds and scams are on the rise, with criminals using social media to advertise highly profitable investments. These ads often use advanced technology to appear legitimate.

Always ask yourself, is this too good to be true? Such high return investments are usually not genuine. Before investing your money take some time to research the provider, verify their existence and that they are regulated and always seek independent financial advice.

4. Purchase scams

Online shopping is convenient and popular, but criminals can clone genuine websites to offer fake discounts to target unsuspecting customers. This can happen with any site, including clothing, homewares, or heavy goods vehicles such as diggers, campervans and boats. These cloned sites often look and feel genuine.

When shopping online, check for a padlock symbol in the address bar, research the site for negative reviews, and verify contact details. Avoid direct bank transfers. Ask yourself, is this price too good to be true?

5. Money mules

Being a money mule is a criminal offence.

Criminals use others' accounts to transfer stolen money to conceal their crime. They can trick anyone into using their accounts. Without access to your account, criminals will not be successful.

They may approach you online, in person, on social media or through fake job adverts asking to move money through your accounts or to open a bank account in your name for them. They may even offer you some money as payment. This use of your account, even if you don't know where the money has come from or is going to, means you are becoming a money mule. This may result in your bank account being closed or a criminal conviction for money laundering.

Parents should also be aware that teenagers and young adults are often targeted by criminals, with the promise of quick cash so sharing this information with family members can also be helpful.

For more information on the latest frauds and scams visit the security centre on our website at aibni.co.uk/security-centre and aibni.co.uk/business/security-centre

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.

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.