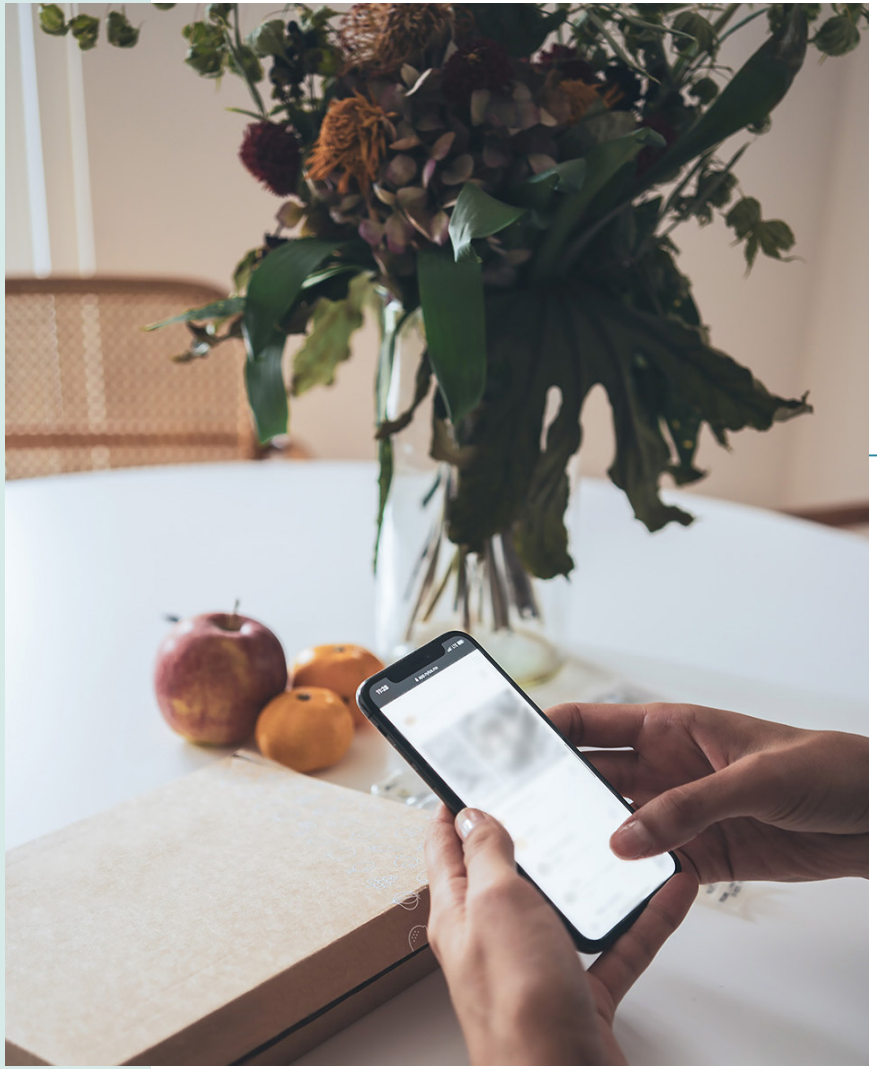
ARBUTHNOT LATHAM

Bankers since 1833

Fraud Update - April 2023



Scammers are constantly finding new ways to try and steal your money and information. In our update, we focus on some of the latest scams.

Remember our **three key fraud messages**:

Three key *fraud messages*

01 Never disclose a **one-time passcode (OTP)** to someone over the phone.

02 Always independently **confirm account information** when paying a new account.

03 **Call your relationship manager immediately** on 020 7012 2500 if you have any fraud related concerns. For card fraud, call 020 7012 2900.

Fraud email payment
are you scam aware?

Payment requests and invoices are regularly submitted via email, but would you spot a scam, especially if the request seemed to come from a trusted person or supplier?

Below are some examples of how fraudsters can try and trick you when sending a fake payment request:

JohnJones@αrbuthnot.co.uk
The Greek letter **α** replaces the **a**

SteveA1an@arbuthnot.co.uk
The number **1** replaces the **l**

0scarSmith@arbuthnot.co.uk
The number **zero** replaces the **0**

Dave5mith@arbuthnot.co.uk
The number **5** replaces the **s**

Ben.Jackson@arbuthnot.co.uk
The name has been spaced with a dot (**.**)

GeoffAdarns@arbuthnot.co.uk
An **r** and **n** has been used to replace an **m**

Be fraud aware

Scammers use innovative ways to convince you they are someone you trust, a business, or a friend. They might try to impersonate that person using an email address, website, or phone number that looks very similar to one you have on record.

If you authorise a payment to a fraudster, we might not be able to recover the money for you.

Our best practice advice

When receiving email payment instructions, it is vital to examine the email address and compare it to any address you have on record to ensure you have an exact match. If you hover over the email address, you might find a different email address underneath.

Never set up a new payee without verifying the details first. We recommend this is done verbally via a trusted telephone number, either a number you hold on record or a number taken from the sender's website (if applicable). Do not just rely on the telephone number in the email.

If you enter a new payee via online banking, and the Confirmation of Payee result does not match the name on the account (or is unable to verify), you should take steps to independently verify the details you have.

How secure is your *mobile phone?*

Our mobile phones have become increasingly vital in managing our finances.

Banking applications are both convenient and aid security with users being able to monitor their accounts and block cards from their devices.

Be fraud aware

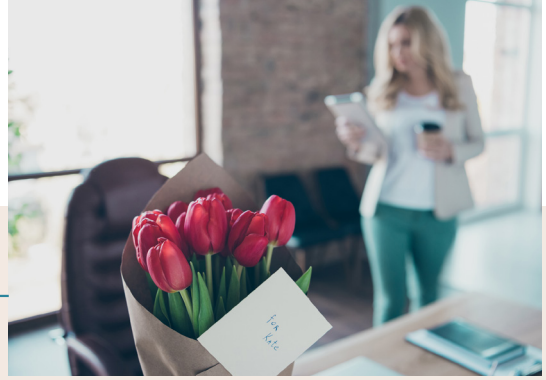
Have you ever thought about the security of the applications on your phone?

If someone saw you enter your PIN to unlock your phone, what could they access? Do you use the same PIN or password to access your banking applications?

Our best practice advice

- be mindful of using your mobile phone in public. Ensure no one can see you enter your PIN
- ensure your PINs or passwords used to unlock your phone are different than for your banking applications
- log out of apps when not in use
- enable face or fingerprint ID where possible, as well as two-factor authentication
- do not store login details in your phone's Notes app
- if your phone is lost or stolen, report it to your bank immediately
- do not use your banking apps on unsecure public WiFi

Romance is *in the air*



Online dating is often used by criminals to target those looking for love.

A particularly prevalent issue are romance scams, where the person you are 'dating' is actually a criminal who is socially engineering you to steal your money.

These scams can be particularly damaging due to the level of trust and subsequent betrayal, as well as the life-changing sums of money that can often be involved.

Many of the criminals performing these scams play the long game, taking their time to build an emotional bond before requesting money.

Online dating red flags

- a request for money should always be treated as a major red flag. This could be for an emergency, an operation, to aid travel to meet in person, an investment opportunity, or to help unlock an inheritance. The size of the request may start small but then get larger
- the person you are speaking to is trying to isolate you by encouraging you not to talk about your relationship with family or friends
- the person you are dating is keen to move away from the dating app messaging service
- the person you are dating always comes up with excuses for why they cannot chat on video or meet in person
- there is a very strong display of affection very early on such as the use of 'pet' names

For business. For family. For life.

Contact Information

Arbuthnot Latham & Co., Limited

Registered Office

Arbuthnot House
7 Wilson Street
London EC2M 2SN

+44 (0)20 7012 2500

banking@arbuthnot.co.uk
arbuthnotlatham.co.uk

Bristol

St Catherine's Court,
Third Floor
Berkeley Place, Clifton
Bristol BS8 1BQ

+44 (0)117 440 9333

Exeter

The Senate,
Ground Floor
Southernhay Gardens
Exeter EX1 1UG

+44 (0)1392 496 061

Manchester

82 King Street
(8th Floor)
Manchester
M2 4WQ

+44 (0)161 413 0030

Registered in England and Wales No. 819519. Arbuthnot Latham & Co., Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Arbuthnot Latham & Co., Limited is on the Financial Services Register under Firm Reference Number 143336.

AL356 / 04 April 2023