Cyber fraud FAQs

What are the most common tactics used by criminals to access my money?

Criminals use many tactics to try and steal information or money, but the most common ones are:

- **Phishing** – an email is sent from an ostensibly trustworthy source in an attempt to trick you into providing sensitive information. This approach can also be used in text messages and phone calls.
- **Malware** – the criminal may distribute malware (malicious software) via email or compromised websites. The malware can then be used to capture sensitive information such as banking details and card numbers.
- **Social engineering** – the criminal will try to manipulate you psychologically. They may pretend to be a trusted source (as seen in phishing) and create a sense of urgency as a way of getting you to act quickly and send over sensitive information.

What resources are available to help me keep safe?

https://www.actionfraud.police.uk/

Action Fraud is the UK's national reporting centre for fraud and cybercrime. The site contains lots of information on how to protect yourself and what to look out for.

https://www.fca.org.uk/firms/financial-crime/fraud

The FCA regulates financial services firms and financial markets in the UK.

https://www.ncsc.gov.uk/

The NCSC is a part of GCHQ. Their website offers guidance and resources on cybersecurity, including information on cyber fraud and scams.

https://www.ukfinance.org.uk/

UK Finance represents the banking and finance industry in the UK. Their website provides information on various financial frauds, including cyber fraud, and offers prevention tips for individuals and businesses.

https://www.nationalcrimeagency.gov.uk/

The NCA's National Cyber Crime Unit focuses on investigating and preventing cybercrime, including cyber fraud. Their website offers insights into cyber threats and reporting mechanisms.

https://www.citizensadvice.org.uk/consumer/

Citizens Advice offers consumer advice and resources, including cybercrime and fraud guidance.

What are the signs of fraud that I should look out for?

- Unfamiliar transactions on bank statements.
- Unexpected account activity that wasn't initiated by you. For example, password resets and changes to personal information.
- Problems accessing online accounts, and login credentials that no longer work.

How can I avoid falling victim to cybercrime and fraud?

While it is not possible to completely prevent cybercrime and fraud from happening, there are measures that can be taken to reduce the likelihood of falling victim to it.

- Use strong passwords – make sure you have a different password for every account.
- Utilise multi-factor authentication (2FA) – this is an additional layer of security that requires a second form of verification, such as a unique code or a push notification to your mobile phone.
- Beware of phishing emails – if something seems too good to be true or doesn't seem quite right, avoid clicking on links or downloading attachments.
- Update your devices – often updates include patches for vulnerabilities that hackers can otherwise exploit.

AJ Bell Management Limited (company number 03948391), AJ Bell Securities Limited (company number 02723420) and
AJ Bell Asset Management Limited (company number 09742568) are authorised and regulated by the Financial Conduct Authority.
All companies are registered in England and Wales at 4 Exchange Quay, Salford Quays, Manchester M5 3EE. See website for full details.