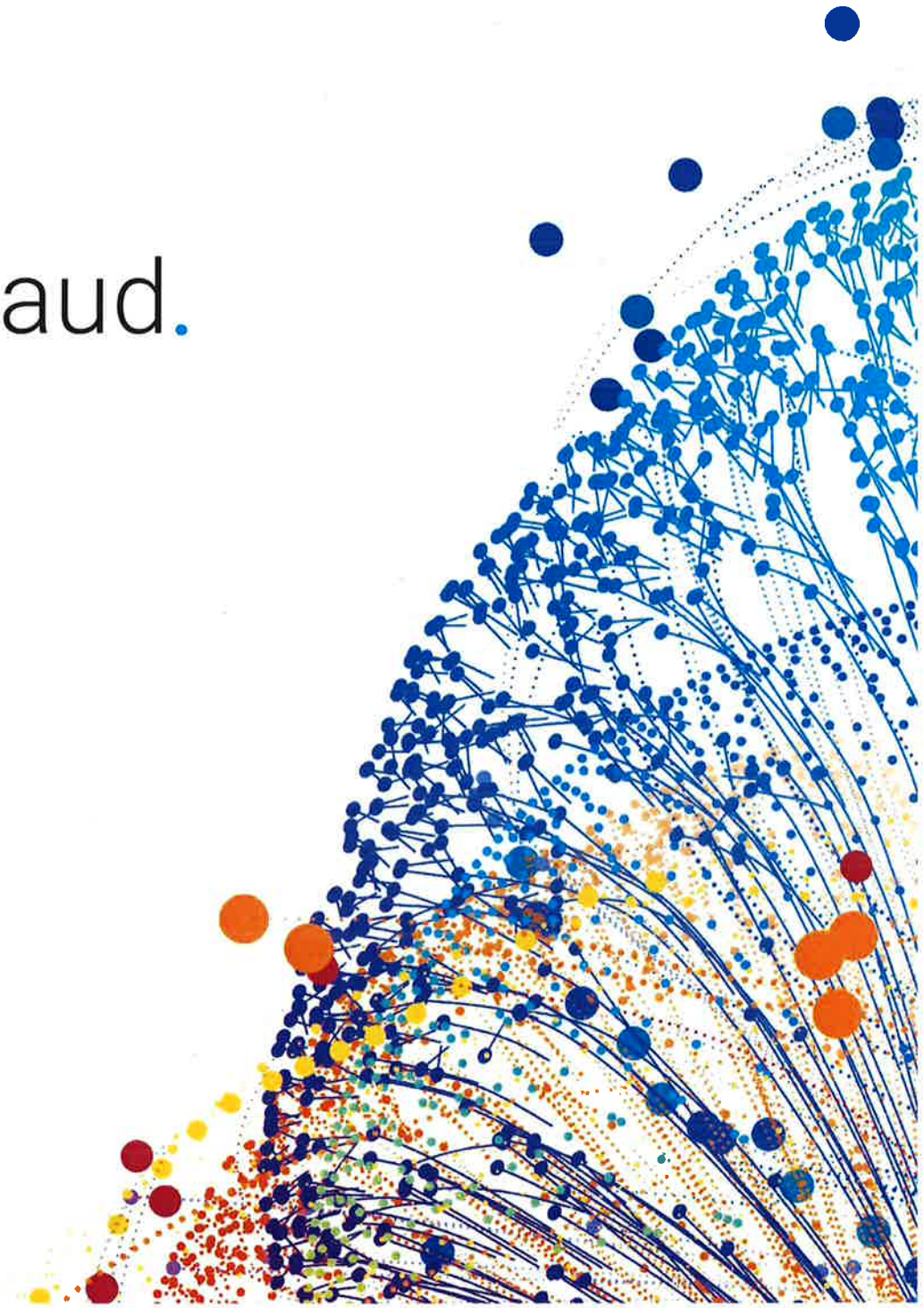
APP Fraud.



Money in Motion

APP Fraud

APP fraud stands for Authorised Push Payment fraud. It's a type of scam where fraudsters trick you into sending money directly to them, often through online banking or mobile apps

Remember: Prepaid Financial Services Limited (PFSL) will never ask you to transfer money to another account. If you're unsure about a request, hang up, delete the email, or ignore the text, and contact the PFSL Fraud team.

If you think you have been the victim of fraud or would like to report anything suspicious, please contact the PFSL Fraud Team via email; pfslfraudops@emlpayments.com

How do Fraudsters operate?

- **Impersonation**: Fraudsters often pretend to be someone you trust, like your bank, a government agency, or even a family member.
- **Urgency**: They create a sense of urgency, claiming you need to act quickly to avoid a problem, like a fraudulent transaction or a missed tax payment.
- **Persuasion**: They use convincing tactics to gain your trust and convince you to transfer money.

Common APP fraud scenarios include:

- **Romance Scams** – these fall into two main categories:
    - **Fabricated Online Profiles:** Fraudsters create fabricated profiles on dating sites and social media platforms to build trust with victims, often professing deep love and commitment.
    - **Financial Requests:** Once a relationship is established, scammers will ask for money for various reasons, such as travel expenses, medical emergencies, or business opportunities.
- **Fake bank scams:** Fraudsters claim to be from your bank, warning of suspicious activity and asking you to transfer money to a "safe account."
- **Impersonating loved ones:** Scammers pretend to be your child or grandchild in distress, requesting urgent financial assistance.
- **Phishing scams:** You receive emails or text messages that appear to be from legitimate companies, asking for personal or financial information.
- **Purchase scams:** You see an online advertisement for a product at a significantly reduced price. Once you pay, you never receive the item, or the quality is far below what was advertised.

How to protect yourself from fraudsters:

- **Be cautious:** Always verify the identity of the person requesting money, even if it seems urgent
- **Be suspicious:** If you are not expecting to make a payment, then think if the request is genuine or could be fraudulent
- **Don't rush:** Take your time and don't make hasty decisions
- **Be wary of unsolicited requests:** Don't click on links or download attachments from unknown sources
- **Monitor Your Accounts:** Keep a close eye on your bank card statements for any unauthorised activity

What to do if you think you've been the victim of fraud:

- **Contact PFSL immediately:** Report the fraudulent transaction as soon as possible - please report it to PFSL by email to pfslfraudops@emlpayments.com
- **Report the scam to Action Fraud:** Consider reporting it to Action Fraud - This is the UK's national fraud and cybercrime reporting centre.
- **Gather evidence:** Keep records of all communication with the scammer.

Remember: PFSL will never ask you to transfer money to another account.

If you're unsure about a request, hang up, delete the email, or ignore the text, and contact the PFSL Fraud team.
If you think you have been the victim of fraud or would like to report anything suspicious, please contact the PFSL Fraud Team via email; pfslfraudops@emlpayments.com

Further Advice on Fraud

Action Fraud – for details on how to report fraud
Take 5 – for help and advice on how to avoid fraud