App Scams: What are they? How to avoid them? How to get reimbursed?

28 March 2025

Andrew Boardman, Ben Woodside, Luke Firmin

Aluska Wildash, Scott Lewis, Arun Chauhan

A joint webinar: ICAEW and The Fraud Advisory Panel

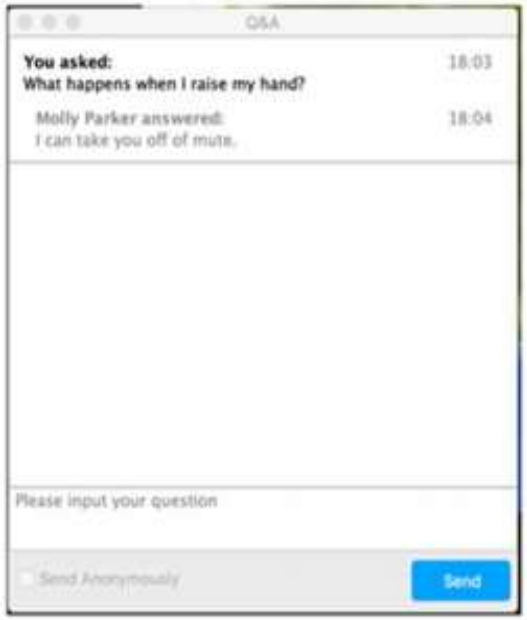
Did you know?

ICAEW's revised Continuing Professional Development (CPD) Regulations brought in new CPD requirements, including a minimum number of hours and an ethics requirement.

This webinar could contribute to up to 1 hour and 15 mins of verifiable CPD, so long as you can demonstrate that the content is relevant to your role.

Find out more about how these changes affect you at icaew.com/cpdchanges.

Ask a question



To ask a question

Click on the **Q&A** button in the bottom toolbar to open the submit question prompt.

Type your question and click send

NOTE: If you wish to ask your question anonymously check the **send anonymously** box shown on the illustration.

Today's speakers

Andrew Boardman
ICAEW

Ben Woodside
PSR

Luke Firmin
Forvis Mazars

Aluska Wildash
Forvis Mazars

Scott Lewis
Nationwide

Arun Chauhan
Tenet Law / Fraud Advisory Panel

Contents:

1. Introduction	*Andrew Boardman*	***ICAEW***
2. Reimbursement, wider work	*Ben Woodside*	***PSR***
3. Case Study: Deep Fake	*Luke Firmin, Aluska Wildash*	***Forvis Mazars***
4. A Building Society's perspective	*Scott Lewis*	***Nationwide***
5. The FOS, Unauthorised	*Arun Chauhan*	***Tenet Law***
		Fraud Advisory Panel
6. Q&A	*Panel*	

What is an APP Scam?

"APP scams happen when **someone** is **tricked** into **sending money** to a fraudster posing as a **genuine payee**."[1]

- "*someone*" = a consumer (for more – see PSR slides)
- "*sending money*" = online banking transfer – from your bank account to the fraudster's account (Faster Payments Scheme – FPS. See PSR slides for more)
- "*tricked…..posing as genuine payee*" = you think you're transferring the money to intended person
- *Authorised* = you have given "explicit consent"[2] to execution of the payment or series of payments
  Unauthorised = the fraudster authorises the transaction, not you e.g. credit card theft
- *APP* = authorised push payment (i.e. authorised FPS transfer)

Example: a fraudster phones you **posing as the "police"**, says that your bank **account is under attack**, and asks you to transfer your funds **to a "safe account"** (being that of the fraudster).

[1] PSR: https://www.psr.org.uk/our-work/app-scams/ [2] PSR: Specific Direction 20 (July 2024), Para 14.4:

Types of APP Scam

UK Finance has categorised APP scams into 8 types[1]:

	Type	Description	Example
Consumer	**Purchase Scam**	Victim pays in **advance**, for **goods** or services that are **never received.**	E.g. victim sees a secondhand car advertised on eBay, at a very good price.
Consumer	**Investment Scam**	Victim moves money to a **fictitious fund** or **fake investment,** offering **very good returns.**	E.g. purchase of cryptocurrency, offering potential 500% gains.
Consumer	**Romance Scam**	Victim pays someone who **they believe they are in a relationship with**. Often met via online/ social media/ dating app.	E.g. with trust established, the beneficiary asks for urgent payment to cover hospital fees.
Consumer	**Impersonation: Police/ Bank**	Fraudster contacts the victim, **posing as the police or the bank**, and convinces the victim to transfer money to fraudster's account.	E.g. phone call from "the police", saying victim's account is under attack, transfer funds to safe account.
Consumer	**Impersonation: Other**	Fraudster claims to **be utility company, mobile/ broadband provider or government**. Often a fictitious fine, overdue tax or erroneous refund.	E.g. an urgent request to settle unpaid tax or face a fine.
Consumer	**Advance Fee Scam**	Victim pays a **fee** which fraudster claims will **result in the release of a much larger payment**, or as a deposit for high-value goods and holidays.	E.g. winning an overseas lottery, gold or jewellery held at customs, or an inheritance is due.
Business or consumer	**CEO Scam**	Fraudster **impersonates the CEO** (or senior executive), convincing the employee to make an urgent payment to the fraudster's account.	E.g. Fraudster spoofs company email and requests urgent changes to payment details for an invoice.
Business or consumer	**Invoice Scam**	Victim attempts to pay an **invoice to a legitimate payee**, but fraudster **intervenes** to convince the victim **to redirect the payment**.	E.g. Fraudster poses as conveyancing solicitors, builders etc. or supplier to a business, with new account.

[1] UK Finance: Annual Fraud Report 2024, Section 09, page 47

Why do APP Scams matter?

Overall:

- **£460m** was lost to APP Scams in 2023. That's £8 per UK adult. And an **average loss per case of £2k.**
- 232,000 cases were reported in 2023. That's **1 case per 250 UK adults**.
- …..plus, **emotional/ psychological harm** to victims and loved ones.

By type:

- Purchase scams are **high volume** (67%) and **low value** (£550)
- Investment scams, romance and impersonation (police/ bank) are **high value** (£10k) and **low volume** (10%)

Value: ranked by share

Type	Share (%)
Investment Scam	23%
Purchase Scam	19%
Impersonation: Police/ Bank	17%
Impersonation: Other	12%
Invoice	11%
Romance Scam	8%
Advance Fee Scam	7%
CEO	3%

Volume: ranked by share

Type	Share (%)
Purchase Scam	67%
Advance Fee Scam	10%
Impersonation: Other	10%
Impersonation: Police/ Bank	5%
Investment Scam	4%
Romance Scam	2%
Invoice	1%
CEO	0.2%

Average Loss: ranked

Type	Avg case value (£)
CEO	28,224
Invoice	16,174
Investment Scam	10,542
Romance Scam	8,774
Impersonation: Police/ Bank	7,448
Impersonation: Other	2,432
Advance Fee Scam	1,312
Purchase Scam	549

Sources: UK Finance: Annual Fraud Report 2024, ONS. (Adult = 15+ years).

PSR Payment Systems Regulator

PSR OFFICIAL

APP reimbursement

APP Fraud: the problem

In the lead up to HMT directing the PSR to implement the reimbursement requirement, APP fraud losses were rising rapidly. Although there has been a modest drop-off recently, APP fraud losses remain around £0.5bn per year.

Losses

Total value of gross losses

	2020	2021	2022	2023	CHANGE
Unauthorised	£783.8m	£730.4m	£726.9m	£708.7m	-3%
Authorised	£420.7m	£583.2m	£485.2m	£459.7m	-5%
Total	**£1204.6m**	**£1313.6m**	**£1212.1m**	**£1168.4m**	**-4%**

Cases

Total number of confirmed cases (where a loss has occurred)

	2020	2021	2022	2023	CHANGE
Unauthorised	2,910,509	2,912,467	2,781,311	2,734,934	-2%
Authorised	154,614	195,996	207,372	232,429	12%
Total	**3,065,123**	**3,108,463**	**2,988,683**	**2,967,363**	**-1%**

APP fraud is a threat to growth in the payments industry. Our research shows that victims' perceived confidence in making payments drops after experiencing fraud. A third of victims (32%) also say they have lost confidence in using new payment methods. (2024 Survey of 668 victims)

Our approach

The PSR has a duty to ensure that payment systems are operated in a way that considers and promotes the interests of all the businesses and consumers that use them.

We first set out our policy programme to tackle APP scams in 2021 consisting of three measures:

1. Harnessing data – the data publication regimes
2. Supporting information sharing – Confirmation of Payee, Enhanced Fraud data and Overlays
3. The reimbursement requirement

In concert with the governments approach to reduce fraud, our strategic approach is to **prevent fraud** and associated harms happening in the first place. We are making sure that everyone has an **incentive** to act to make it harder for criminals to abuse Faster Payments

The Reimbursement Requirement at a glance

***From 7 October 2024**, PSPs in scope of the policy **must reimburse** victims of APP scams **within five business days** of the consumer making a claim.*

Cost of reimbursement is split 50/50 between the sending and receiving PSP.

The maximum level of reimbursement per claim is £85,000.

The consumer must be reimbursed within 5 business days. PSPs can 'stop the clock' for defined reasons e.g. to seek more information.

The policy covers domestic Faster Payments or CHAPS payments made on or after 7 October 2024.

Consumers must make a claim within 13 months of the last payment to the fraudster.

£100 claims excess (applied at claim level, not transaction level).

We have set a consumer standard of caution to reduce risk of moral hazard + an exception for first party fraud.

We're protecting vulnerable consumers. The excess, and the consumer standard of caution do not apply to vulnerable consumers.

Policy scope

Consumer	• Individuals, micro-enterprises, small charities • Only applies to the sending account, not receiving account
Time limits	• Payments made before 7 October 2024 are out of scope . • Claims made more than 13 months from the date of the final payment of the claim are out of time, but the PSP can reimburse voluntarily, or subject to any other relevant regulation, legislation or code.
'On us' payments	• Payment must be made over FPS or CHAPS • Some 'on us' payments do pass over a payment system; but others don't and are out of scope
Jurisdiction	• Payment must be executed in UK and received in a relevant account in the UK

Implementation update

- The PSR's policy came into effect on 7 October and has embedded well.
- Initial data indicates:
  - **89%** of money lost to in-scope APP scams has been **reimbursed**
  - **claim volumes are around 40% lower** than in 2023.
- No evidence of increases in first party fraud or spikes in other types of fraud.
- System stability on both RCMS and BPS has been good, and where minor data or system incidents have arisen, they have been quickly fixed with no material incidents affecting firms.

- But we continue to monitor closely. We will continue to work with Pay.UK and industry – and welcome any evidence on the impacts of the policy.

Monitoring and evaluation

- We have committed to commissioning an independent evaluation of our policy after 12 months
    - Important to have 12 months of data and observations
    - But if significant issues arise, we may review elements of the policy before that

- Also monitoring impacts on an ongoing basis, including through the data we are receiving from UK Finance and Pay.UK and regular engagement with industry, consumer groups, other regulators, government departments and law enforcement agencies.

- Our policy represents a significant step change in protections for consumers, but we expect our policy to evolve over time.

- Important to remember the policy is a package of measures (also complemented by other initiatives such as Confirmation of Payee and publication of fraud performance data)

PSR's wider work on APP fraud

Fraud origination data

- In December we published data for the first time on how fraudsters exploit major platforms to scam consumers
- Fraudsters use major social media platforms, technology platforms, and the telecommunications sector to commit APP scams against UK consumers, leading to losses in the hundreds of millions.
- Our data showed that:
    - £341 million was lost to APP scams in 2023. Over half of these were reported by victims as originating on Meta platforms
    - Telecommunication and email providers were also targeted by fraudsters to carry out a significant amount of APP scams.
    - Meta platforms feature as the top three platforms being targeted by fraudsters to carry out the most common type of APP scam – purchase scams
- Whole system approach needed to tackle APP scams.

Upcoming publications

Transparency and performance data

- Reimbursement update (Q2)
- Call for views on future of data collection and reporting
- Fraud performance data publication (Q4)

Innovation in data sharing

- Call for views to reconsider EFD, understand how solutions in the market have evolved and what (if any) regulatory action is required

APP Scam

Case Study: Deep Fake

Luke Firmin
Head of Financial Crime (UK)

Aluska Wildash
Assistant Manager

forvis mazars

Case Study: Deepfake Voice APP Scam

1

AI Voice Technology

Fraudsters deployed sophisticated AI to clone the CEO's voice with remarkable accuracy.

2

Target Selection

They identified a finance director with payment authority at a multinational tech tech firm.

3

Social Engineering

They researched the executive's speaking speaking patterns and corporate relationships for authenticity.

forvis mazars

The Fraud in Action

1. **Initial Contact**

   CFO received call 7.30 PM from 'CEO' about urgent confidential

2. **Pressure Applied**

   Fraudster insisted on immediate wire transfer to secure the deal.

3. **Transfer Executed**

   £243,000 transferred to fraudulent account after minimal verification.

4. **Discovery**

   Real CEO questioned about transaction in meeting two days later.

forvis mazars

Red Flags

Extreme Urgency

The 'CEO' claimed the deal would collapse collapse without immediate payment.

Unusual Timing

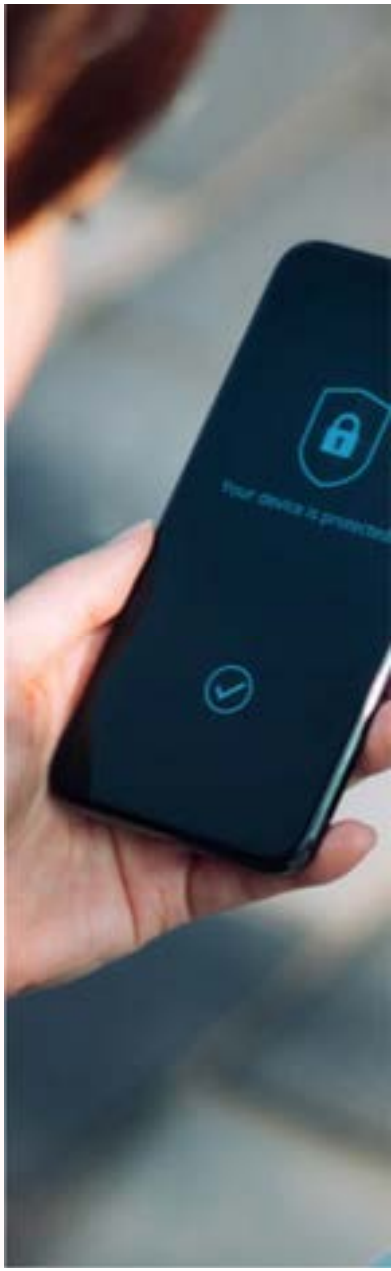
Call came at 7:30 PM when verification resources were limited.

Protocol Breach

Standard dual authorisation procedures were bypassed for the transaction.

Communication Channel

The 'CEO' refused video calls, citing poor internet connection.



forvis mazars

Preventive Measures

Voice Biometrics
Deploy AI solutions to detect synthetic voice manipulations in real-time.

Challenge Questions
Establish personal verification queries known only to executives.

Payment Thresholds
Implement tiered verification based on transfer amount and recipient history.

Simulation Training
Conduct regular fraud scenario drills with realistic deepfake examples.

Encourage skepticism, consulting with internal fraud team and secondary verification.

Protocol Adherence
Follow dual-signature requirements for all large transfers.

Delay Strategy
Implement a mandatory cooling period for unusual high-value transfers.

forvis mazars

Conclusion: Staying Ahead of APP Fraud

Continuous Evolution

Security measures must adapt as quickly as fraudsters' techniques. Today's solutions become tomorrow's vulnerabilities.

Collaborative Approach

Share fraud intelligence across organisations. organisations. No single entity can combat combat these threats alone.

Human Element

Technology solutions must complement complement human vigilance. The strongest strongest defence combines both.

forvis mazars

nationwide

A Building Society's perspective to APP scam reimbursement

Scott Lewis - Fraud and Scams Operations Manager

The wider Fraud and Scams Ecosystem

APP scams prevalence has become significant over the last 6 years with volumes rising significantly across the industry.

This isn't unique to the UK, APP scam prevalence is increasing across the world.

Fraudsters generally don't see the banks as the weak link, they see the consumer as the weak link in the chain. Consumers can often be extremely vulnerable with low financial knowledge, understanding or capability. This makes a bank's job a difficult one because APP victims don't look like a fraudster, their accounts don't look like a first party fraudster, and the transactions they're often making don't look like fraud. Identifying victims can often be difficult.

Implementation of Mandatory Reimbursement

Even prior to the Mandatory reimbursement changes, Nationwide customers were already offered a high level of protection. We were one of around a dozen signatories of the Contingent Reimbursement Model (CRM code). Under the code the starting position was a refund, unless the bank was able to identify the customer hadn't acted reasonably. NBS already refunded 96% of customers fully by volume (PSR APP fraud Data for 2023).

Education and looking after consumers was also an important part of the CRM code and this is something we've carried forward into Mandatory reimbursement. We recognise a key part of reducing APP scams is increasing consumer knowledge of them

Successes of mandatory reimbursement

(PSR Measure 3)

- Consumer protection – Both in terms of claim timescales and reimbursement.
- Better communication between firms leading to fair customer outcomes
- Equal split in responsibility between banks
- More emphasis on preventing mule accounts being opened
- Regular industry roundtables and workshops to ensure approaches are consistent across firms

Challenges going into the future

- The complexity of scams is increasing. This makes prevention difficult and can often take statutory bodies years to unravel if a scam has taken place.

- Operationally the windows for the sending firm and receiving firm to communicate together can be tight, however the Stop the Clock function does support this.

- Still a number of key changes ahead such as the industry switching from UKFs SSI system to a Pay.uk owned replacement.

Practical steps to take if you've been scammed

- Contact your Bank or Building Society as soon as is possible to notify them of the scam

- If the scammer continues to contact you, ignore them.

- If your phone, account details, Card or PIN has been stolen it is important your bank are notified of this as soon as possible.

- If remote access software has been installed on your device, remove this software and install antivirus software. If you're unsure how to do this, you may want to consider giving your device to a specialist.

- Notify Action Fraud or The Police

www.**tenetlaw.**co.uk

APP Fraud | The FOS | Unauthorised fraud

Arun Chauhan

tenet

The FOS and APP interpretation

- Award level | Mandatory reimbursement limit £85,000 | FOS £430,000 (plus interest)
- Reasons to reject a claim (1) Gross Negligence (2) First Party Fraud i.e., acted fraudulently
- 13 months to raise with the PSP | | Timing 6 months from '*deadlock*' letter

FOS case examples

- £478,000 decision in March 2025 | Conveyancing fraud – multiple transactions

- Customer took a call from someone impersonating his bank and the FOS was not persuaded that in these circumstances handing over the OTP was negligent. Full refund.

- Micro-enterprise customer took a call from someone impersonating his bank and it was a safe account scam. Does feel that sharing the OTP was a significant degree of carelessness. Full refund.

Unauthorised transactions

- Payment Services Regulations 2017 | Similar architecture to authorised payment fraud
- Reg 72(3) "*The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service*."
- Reg 73(1)(a) "*ensure that the personalised security credentials are not accessible to persons other than the payment service user to whom the payment instrument has been issued*"
- Reg. 76 (1) Unauthorised transaction = right to refund | Reg 77(3) Gross Negligence or Fraudulent
- Unauthorised transactions on customer accounts. E.G., Sim Swap enabled security codes to be sent to fraudster's phone to load customer card details to fraudster's digital wallet (Apple Pay). PSP ought to have taken better steps to ensure card details sent to their actual customer.

Q&A

icaew.com