Take Five to Stop Fraud

April Partner Pack

What's in the toolkit?

Our monthly partner packs have a range of resources to help you support Take Five:

- Key messages and advice
- Assets
- Template social media posts

How can you help?

There are a range of ways to get involved and support consumers, this might include:

- Posting on social media
- Including information in newsletters
- Sharing with internal colleagues

This month, we're focusing on:

1. Investment fraud
2. Payment in advance fraud
3. Spoofing

We will be sharing content across our channels throughout the month. You can re-post and share our content or post your own content using the key messages and template posts below. If you need any support in using this partner pack, please contact us at: takefive@ukfinance.org.uk.

Download your April assets now

Advice this month:

1. Investment fraud

Investment fraud is when you're convinced to move your money into a fictitious fund to pay for what later turns out to be a fake investment. In the first half of 2023, £57.2 million was lost to investment scams.[1]

Investment scams can include markets such as gold, property, carbon, cryptocurrencies such as Bitcoin or even wine. Criminals often set up fake websites claiming to be legitimate investment firms.

After a small initial investment, you may receive a payment or see "returns" – criminals do this to convince you to invest more. They may even use fake celebrity endorsements.

What to look out for:

- Adverts on your social media feeds, sometimes celebrity endorsed, offering high returns on investments
- Unexpected contact by phone, email, message or social media about an investment opportunity
- People offering a high return on your investment with apparently little or no risk
- 'Exclusive' investment opportunities
- People who pressure you into making a decision with no time for consideration

You can check if an investment or pension opportunity you've been offered could potentially be a scam by taking the FCA's ScamSmart investment checker or play their 'Scam or Smart' quiz.

[1] UK Finance Half Year Fraud Report 2023

2. Payment in advance

Payment in advance fraud, also known as an 'advance fee' fraud, is where you're convinced to pay an upfront fee in order to receive something in return.

This might be a loan, a job application, a prize or high-value goods. Whether it's tickets for Coachella or the FA Cup Final, a recruitment offer, or even a loan, always ask yourself why you're being asked to pay for an upfront fee for goods or services.

How to protect yourself:

- Avoid giving out your personal or financial information on cold calls or unexpected emails.
- Always do your research to check if it's legitimate.
- Buy tickets through a genuine seller or re-seller.
- If you've won a competition on lottery that you didn't enter, it's most likely a scam. in this scenario.
- If you've applied for a loan, call the loan provider back on a number or email you know to be true.

Payment in advance scams were the second most common form of Authorised Push Payment (APP) scam in the first half of 2023.[2]

3. Spoofing

Spoofing is a tactic criminals use to make it look like you're being contacted from a genuine organisation. They can disguise their phone number or caller ID to look like a legitimate organisation, in the hope that you click on a link in a text or email.

These scams might include: fake passwords resets, failed deliveries, lotteries, banking messages.

Follow the Take Five advice and avoid clicking on these links. Always log in to your account separately to update any information or make payments.

---

[2] UK Finance Half Year Fraud Report 2023

Template social media posts

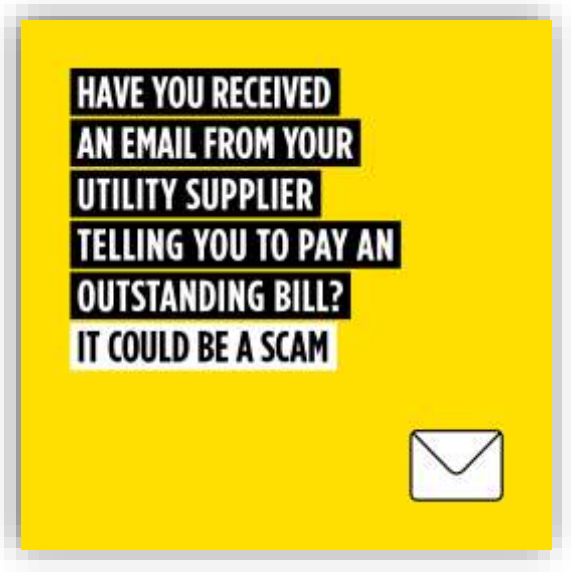
Platform	Copy	
Facebook, Instagram, LinkedIn (asset 1)	Criminals offering you investment opportunities go to great lengths to appear legitimate. They might have bogus registration numbers, authorisation documents and personal testimonies about their offer. They may even give you access to portals so you can manage your 'portfolio'. You can check if an investment opportunity you've been offered could potentially be a scam by taking the @FCA's Scam or Smart test. https://www.fca.org.uk/consumers/play-scam-or-smart #TakeFive #StopChallengeProtect✋👍👊	
Twitter (asset 1)	Criminals offering you investments work hard to appear legitimate. They might have bogus registration numbers, authorisation documents and personal testimonies about their offer. Check if an investment opportunity is a scam by taking the @FCA's ScamSmart test: https://www.fca.org.uk/consumers/play-scam-or-smart	

Facebook, Instagram, LinkedIn (asset 2)	Criminals create fake online adverts offering high returns through cryptocurrency investing or mining. These ads may look official, including celebrity endorsements or personal testimonies. Most cryptocurrencies aren't regulated by the FCA which means they're not protected by the UK's Financial Services Compensation Scheme. If you are scammed it is unlikely you will recover any of your money. Remember: - Never invest if someone is putting pressure on you – no legitimate organisation or person will try to rush or panic you. - Even if your family or friends are investing, it doesn't mean it's genuine. If you think you have been scammed, contact your bank immediately and report it to Action Fraud. #TakeFive #StopChallengeProtect✋☝👊	

Twitter (asset 2)	Beware of crypto fraud. Never invest if you are being put under pressure. Even if your friends are investing, it doesn't mean it's genuine. Think you have been scammed? Contact your bank immediately and report to @actionfrauduk. #TakeFive	
Facebook, Instagram, LinkedIn (asset 3)	You've just won the lottery! Or have you? If you receive a message like this, #TakeFive and ask yourself: Did you buy a lottery ticket? Why is someone asking you to pay a fee to access the prize? Payment in advance scams are where criminals ask for upfront fees for goods and services that never materialise. If you think you've been scammed, contact your bank immediately and report it to Action Fraud. #StopChallengeProtect	

Twitter (3)	Have you really just won the lottery? If you receive a message like this, #TakeFive and ask yourself if it could it be fake? If someone is asking you to pay a fee to claim a prize, this could be a payment in advance scam. #StopChallengeProtect	
Facebook, Instagram, LinkedIn (asset 4)	Been asked to pay an upfront fee to receive a delivery, get a loan or claim a prize? Always #TakeFive and ask yourself - could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. Report suspicious emails by forwarding them to report@phishing.gov.uk. If you have visited a website you think is suspicious you can report it to the National Cyber Security Centre using their online reporting form. #TakeFive #StopChallengeProtect	

Twitter (4)	Been asked to pay an upfront fee to receive a delivery, get a loan or claim a prize? Could it be fake? Report suspicious emails to report@phishing.gov.uk. If you have visited a website, you think is suspicious you can report it to @NCSC. #TakeFive	
Facebook, Instagram, LinkedIn (asset 5)	What to do when you receive a call you weren't expecting: ⚠STOP: Only share personal or financial information to services you have consented to and are expecting to be contacted by. ⚠CHALLENGE: Could it be fake? Don't give anyone remote access to your computer following a cold call. It's ok to say 'no'. ⚠PROTECT: If you've transferred money to another account for 'safe keeping', contact your bank immediately and report it to Action Fraud. #TakeFive	

Twitter (5)	Received an unexpected call? ⚠ STOP: Only give info to services you have consented to and expect contact from ⚠ CHALLENGE: Could it be fake? It's ok to say 'no' ⚠ PROTECT: If you've transferred money to a 'safe account', contact your bank **immediately** #TakeFive	
Facebook, Instagram, LinkedIn (asset 6)	Watch out for 'spoofing' scams 👀 Criminals use this tactic to make it look like you're being contacted by a genuine organisation. Avoid clicking links in emails, and instead log in to your account separately to update your information or make payments. #TakeFive #StopChallengeProtect	
Twitter (6)	Watch out for 'spoofing' scams 👀 Criminals can make it look like you're being contacted from a genuine organisation. Avoid clicking these links, and instead log into your account separately to update your information/make payments. #TakeFive #StopChallengeProtect	