

The complaint

Mrs J complains that Metro Bank Plc (Metro) won't provide her with a refund after she became victim of a cryptocurrency investment recovery scam. Mrs J is represented in this complaint, but I'll refer to her as it's her complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In and around August 2024, Mrs J believed she had been the victim of a stocks and shares investment scam with Company W. Mrs J thought her investment with them was worth £16,266 but she couldn't withdraw this due to a 20% tax demand and then the trading platform was subsequently taken down. Mrs J explains that in the following months she remained stressed and anxious.

In and around November 2024, Mrs J saw a government advert on social media for (fake) Company F who claimed it could recover lost investment funds.

Mrs J contacted Company F and the scammer, who I'll refer to as X, said they could recover the investment money she thought might possibly be sitting in a crypto wallet.

Mrs J was informed her funds had been traced and through successful crypto trading, in a volatile period, had grown to £81,401. Mrs J was told she needed to pay an upfront release fee and was led to believe this could be taken from her lost funds.

After checking their website, which she thought looked legitimate, Mrs J agreed to use Company F's services.

Mrs J gave X her identity and bank account information and unbeknown to her X used this information to apply for a loan with her Bank S.

Bank S informed Mrs J that they had approved a loan for her and gave her a key code to release the funds into a bank account of her choosing. Mrs J hadn't applied for a loan and was concerned about a possible data breach. She mentioned this to X who, under the guise of assisting her, asked to see a copy of the letter and told her to disregard it. But by viewing the letter he got access to the key code. X then used this code to activate and release the £20,000 loan into Mrs J's Bank N account.

X convinced Mrs J he was arranging to send her part of her £81,401 lost funds, and he also sent her a fake letter from the crypto exchange company stating that the £81,401 would be deposited into her Metro account. When Mrs J saw this in her Bank N account, she thought it was part of her lost funds enabling her to pay the full release fee.

Having transferred funds from Bank N, which she didn't realise was the Bank S loan in her name, Mrs J made the following payments to her crypto account with Company C and then on to the scammers:

Payment Number	Date	Payment Type	Beneficiary	Amount
1	12/11/24	Faster	Mrs J's account with Firm C (clearance bank	£20

		Payment	for Company C)	
2	26/11/24	Faster Payment	Mrs J's account with Firm C (clearance bank for Company C)	£100
3	26/11/24	Faster Payment	Mrs J's account with Firm C (clearance bank for Company C)	£19,800
Total				£19,920

Mrs J realised it was a scam once the scammer started asking for more money. As she used the loan and paid the scammer from her Metro account, she now has to repay Bank S £27,900 (due to interest on a five-year loan).

Mrs J complained to Metro seeking a refund of £19,800 plus interest. She said Metro failed to pick up on out of character payments and had they done so the fraud would've been prevented.

Metro rejected her claim. They said the APP Scam Reimbursement Rules didn't apply.

Mrs J escalated her complaint to our service. Our investigator said Metro should've intervened, that this would've likely unravelled the scam but due to contributory negligence from Mrs J both parties were liable for 50% of a loss of £19,920.

Mrs J thought this was a fair outcome, but Metro disagreed and said they '*fundamentally disagree with the opinion that we should be held liable for the loss in these types of cases*'.

As Metro disagree this complaint has been passed to me to look at.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, my decision is to partially uphold this complaint. And I'll explain why.

I should first say that:

- From reviewing file submissions, I'm satisfied that Mrs J has been the victim of a cruel scam.
- I'm very sorry to hear that Mrs J has been the victim of this cruel scam and lost a significant amount of money here.
- My role is to independently evaluate the evidence provided by both parties. So, where evidence is incomplete, inconsistent or contradictory, as some of it is here, I must reach my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence and wider circumstances.
- I'm satisfied that the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply to the payments Mrs J authorised to another account under her control.
- The Payment Services Regulations 2017 (PSR) and FCA's Consumer Duty are relevant here.

PSR

Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mrs J made the payments here, so they are considered authorised.

However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions. So, I consider Metro should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023 Metro had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Metro was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud.

Metro was also required to support vulnerable customers. Although I recognise Mrs J's vulnerability after the first scam, I can't see any evidence that she'd made Metro aware of this.

With the above PSR and Consumer Duty in mind, I first considered:

Whether Metro should've identified that Mrs J was at risk of financial harm and put in place proportionate interventions

Although this complaint isn't about Mrs J's losses prior to November 2024, I noted that she opened her Metro account in August 2024 and indicated it was to be a safe account. So, I was surprised to find that Metro was unable to confirm that they didn't either issue Mrs J with a safe account scam warning (which wouldn't have been relevant here) and / or put in place an interaction to probe her account opening reason which appears to be for the investment scam.

Metro also couldn't provide evidence of any interventions, either automated or human (with a fraud and scam agent):

- Between August and November 2024, despite:
 - Mrs J regularly transferring money into her account and then straight out again, with payments ranging from approximately £1,000 to £4,000.

- Metro being able to see that she was sending money to a company that traded in crypto.
- For Payment number 3 on 26 November 2024, which:
 - Was for a high amount (much higher than any previous payments) of £19,800.
 - Was also preceded by a same day transfer.
 - Metro could again see, was being sent to a crypto exchange (Company C).

And I can't see that Metro did any analysis of Mrs J's account, questioned any of her transfers and immediate payments, considered providing fraud / scam warnings or provided sufficient evidence to persuade me they intervened or that the payments weren't unusual, and it wasn't proportionate for them to intervene.

If a bank doesn't question payments like these that have risk factors, then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, there was a heightened risk and a potential multi stage scam indicator.

I think Metro should've provided automated warnings, relevant to high-risk crypto investment transactions, on her initial payments, followed by human interventions. This is because they should be fully aware of different scams, what they look like and what they involve such as the payment journeys that they can take. Also, crypto investment scams were very well known to banks in 2024. So, even though Mrs J was transferring funds to a crypto account in her name, Metro ought to have been on the lookout for unusual transactions and patterns.

I think human interventions to warn, probe, detect and protect Mrs J from financial harm should've occurred on:

- 26 September 2024:
 - When there was a clear pattern of increasing same day credit transfers followed by crypto payments that exceeded £5,000.
- 26 November 2024:
 - When Mrs J made the payment for £19,800.

Having established there were clear intervention trigger points, I then considered whether:

An effective human intervention would've more likely than not prevented the loss Mrs J incurred upon payment 3

I considered causation. Put simply, whether Metro's failure to warn and intervene upon this payment caused Mrs J's loss. To do this, I reflected on whether any such interventions would've made any difference.

I considered what would've likely happened if a Metro fraud and scam agent asked the following type of open questions that banks frequently ask:

- Payment purpose.
- Checks and research completed.
- Expected returns and ability to withdraw.
- Third parties, brokers or recovery agents advising of fees.
- Third party communications including requests to deceive the bank.

Having read Mrs J's submissions, reviewed and questioned her dialogue with the scammer, in which I can't see any evidence of coaching, I have no reason to think she wouldn't have given honest answers to these type of questions.

I think Mrs J would've explained the earlier August 2024 scam, Company W's advert relating to cryptocurrency recovery, the promised return (which was too good to be true) and the £20,000 credit (which she didn't know was a loan). And an agent would've immediately been highly suspicious and discussed checks including with the FCA, Companies House and on-line presence and the scam would've very quickly unravelled.

Metro do provide automated warnings, but they can't evidence that they've implemented them here. The warnings ask / state the following before a customer confirms and proceeds:

- *'Are you investing in an FCA registered firm, if not STOP!'*
- *'Always use the contact details from the FCA site'.*
- *'If the returns seem too good to be true it probably is'.*
- *'Don't make a payment unless you know your money is going to the right place'.*
- *'Read more about scams' – And here they provide a link*
- *'Call us if you have questions'.*

It is difficult to know, but I think Mrs J, who appeared anxious in her conversation with X, may have taken notice of these warnings, conducted more thorough checks and may have called Metro, sought advice and not made payment 1 and 2. So, I 'm in agreement with our investigator that Metro's liability should include payment 1 and 2.

I then considered whether it would've been fair and reasonable for Metro to accept full liability.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions. With this in mind, I considered whether Mrs J did enough to protect herself from the scam. Although I recognise how convincing these cruel scammers are and the impact on Mrs J, I think she should've been more diligent:

- Completing more thorough research on Company F.
- Researching recovery services for which there are many on-line warnings about scams and scammers promising unrealistic recoveries and often requiring upfront fees.
- Requiring proof of how her funds had been found and were recoverable.
- Following up on her concerns with Bank S over the loan application.
- Reading and enquiring about Bank S's letter that said the loan was ready for release.

Considering the above, I'm satisfied that there was contributory negligence from Mrs J

Putting things right

In a situation where both the customer and the business are equally at fault, I think it is only fair and reasonable for liability to be shared from the point – which I consider to be payment number 1 – the payments to the scammer should've been stopped.

So, I'm therefore partially upholding this complaint, and I require Metro Bank Plc to:

- Refund Mrs J £9,960 (50% of £19,920).

- Plus pay simple interest at 8% per annum from the date of the payments to the date of settlement.

My final decision

For the reasons mentioned above, my final decision is to partially uphold this complaint, and I require Metro Bank Plc to:

- Refund Mrs J £9,960 (50% of £19,920).
- Plus pay simple interest at 8% per annum from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs J to accept or reject my decision before 1 November 2025.

Paul Douglas
Ombudsman