DRN-6002914

The complaint

Ms D is unhappy that Metro Bank PLC has declined to reimburse her after she lost money to an investment scam.

Ms D is represented in this matter, but for ease of reading I will refer to Ms D throughout this decision.

What happened

The background to this complaint is well known to all parties, so I will not set it out in detail here. In summary, Ms D says she was interested in investing to create a second income stream. She came across an advertisement on a social media platform promoting the services of an investment company. Interested in the opportunity, she completed an enquiry form. Shortly afterwards, Ms D was contacted by someone who discussed investment options with her.

Ms D now knows that the individual she spoke to was a fraudster and not a representative of a legitimate investment firm. The fraudster encouraged Ms D to open an account with a cryptocurrency exchange. She did so and made the following payments from her Metro account:

no	date	Payment type	payee	amount
1	18.01.24	faster payment	cryptocurrency exchange	£1,400
	25.01.24	faster payment - returned	cryptocurrency exchange	£10,000
	25.01.24	faster payment - returned	cryptocurrency exchange	£10,000
	26.01.24	faster payment - returned	cryptocurrency exchange	£10,000
2	26.01.24	faster payment	cryptocurrency exchange	£5,000
3	26.01.24	faster payment	cryptocurrency exchange	£5,000
	29.01.24	credit	cryptocurrency exchange	£149.65
4	29.01.24	faster payment	cryptocurrency exchange	£21,000
5	30.01.24	faster payment	cryptocurrency exchange	£7,000
6	30.01.24	faster payment	cryptocurrency exchange	£10
7	31.01.24	faster payment	cryptocurrency exchange	£1,400
	21.03.24	faster payment	cryptocurrency exchange	£20,000

	22.04.24	faster payment - returned	cryptocurrency exchange	£20,000
8	22.04.24	faster payment	cryptocurrency exchange	£20,000
			Net loss	**£80,660.35**

It appears that the funds were then transferred on to a 'trading account' under the control of the scammers.

Ms D realised she had been scammed when she was unable to access her trading account.

Ms D reported the scam to Metro, it declined to refund the money she had lost to this scam. Ms D wasn't happy with Metro's response and referred her complaint to this service.

An investigator looked into the complaint and upheld it in part. The investigator said they were of the view that Metro should have done more to prevent this scam and, had it done so, it could've prevented Ms D's losses. However, they also considered that Ms D should bear some responsibility for her losses.

The investigator recommended that Metro refund 50% of the losses Ms D had suffered from the first payment of £1,400 on 18 January 2024.

Ms D accepted the investigator's view. Metro did not accept our investigator's view. It said, in summary, that it felt its intervention had been adequate and noted Ms D seemed confident when she spoke to its representative and had confirmed she understood she was making a payment to buy cryptocurrency and the payment was to a wallet under her control.

As Metro did not accept our investigator's view, the complaint has been passed to me for a final decision.

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.

In doing so, I'm required to take into account relevant: law and regulations; regulators' rules; guidance and standards; codes of practice; and where appropriate, what I consider to have been good industry practice at the time. Having done so, I have reached the same view as our investigator, and for much the same reasons. I'll explain why.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (PSRs) and the terms and conditions of the customer's account. And I have taken this into account when deciding what's fair and reasonable in this case.

However, taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Metro should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.

- Have had systems in place to look out 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 decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

It is not in dispute that Metro intervened in this case. The evidence provided shows that Metro contacted Ms D before it processed the first payment on 18 January 2024 of £1,400. I think it was reasonable for Metro to intervene before processing this payment.

I have carefully listened to this call and the subsequent conversations Ms D had with Metro. Like our investigator, I don't think Metro took adequate steps to establish why Ms D was sending money to a cryptocurrency exchange, so soon after she had opened her account with it.

In the conversation the representative explained he was calling from Metro's fraud department. The conversation was rushed, taking just over 3 minutes, including the security questions. The representative explained that the payment had been flagged on Metro's system as a '*potential scam payment*'. He said the beneficiary was a cryptocurrency exchange and noted that Metro had received scam claims against the beneficiary in the past. In light of the information Metro had - and that it knew Ms D had only recently opened her account with it - I think the representative should have done more to determine whether the payment was legitimate or whether Ms D might be falling victim to a scam.

Rather than asking questions to establish Ms D's knowledge of cryptocurrency investing, the representative said, '*I assume you are quite knowledgeable about how cryptocurrency works and the risks associated with them'*. He then asked if Ms D had made payments to the beneficiary previously and when Ms D said she had, he said *'…so you are fully aware of them and had no issues in the past.'* I think the lack of curiosity shown by the representative, together with the rushed nature of the call meant that Metro's intervention did not have the impact it should have had on Ms D. I think the call gives the impression that the representative was speaking to Ms D as a formality, rather than a legitimate attempt to disrupt a potential scam.

(I note that the WhatsApp chat Ms D had with the scammers shows she had been instructed to open an account with Metro as her existing bank had refused to process payments to the cryptocurrency exchange.)

I am of the view that if Metro had questioned Ms D more robustly, when it spoke to her about this payment, and discussed why she was making a payment to buy cryptocurrency, so soon after she had opened her account with it, the scam could have been uncovered at this point. I say this because I think it would have become apparent to Metro if it had questioned Ms D in more depth about investing in cryptocurrency that she only had limited knowledge in the area.

Metro would then have been able to discuss with Ms D the characteristics of an investment scam such as unrealistic returns and that 'investors' are often put under time pressure to invest quickly and that the cryptocurrency would not be under her control once it was transferred on. I think this would have led Ms D to tell Metro that she was in fact transferring the cryptocurrency onto an 'investment company' and the scam could have been uncovered at this point.

Like our investigator I don't think Metro's intervention was sufficiently robust. I am also mindful that it appears none of the subsequent payments Ms D made to the same beneficiary triggered Metro's fraud detection systems, despite the frequency and value of the payments increasing. Increasing value and frequency of payments being one of the hallmarks of a scam. I think Metro should have intervened again when Ms D sent a second payment for £5,000 on 26 January 2025.

This payment was the fifth attempted payment to the beneficiary in just over a week (Ms D had made three unsuccessful attempts to transfer £10,000 earlier that day and the previous day and had spoken to Metro about the attempted transfers), the value of the payment Ms D was making was significantly larger than her previous payment and the payments were being made from a recently opened account.

That said, having very carefully considered this matter, like our investigator, I think Ms D should bear some responsibility for her losses. In reaching this view, I've taken into account what the law says about contributory negligence while keeping in mind that I must decide this case based on what I consider to be fair and reasonable in all the circumstances.

Having done so, I'm satisfied that it is fair and reasonable for Ms D to bear some responsibility for her losses here, despite the apparent shortcomings of the calls Ms D had with Metro.

I say this as I am mindful that Ms D did not carry out checks on the company before investing with it. Likewise, it appears she did not query why the scammer had told her to open an account with Metro to make payments from, when her own bank would not permit payments to the beneficiary. I also note that in the chat Ms D had with the scammer she noted that Metro had told her *'…they have numerous scam claims against [name of cryptocurrency exchange].'* This suggests that, despite the rushed nature of Metro's intervention, Ms D had noted Metro's concern about the payment she was making.

To be clear, I don't wish to blame Ms D for being the victim of a scam. But in assessing whether Metro acted fairly, I must also consider whether Ms D took less care to protect herself than I would reasonably expect. I can see how Ms D was taken in by the scammer. The scammer posed as an investment adviser and showed Ms D what she felt was a credible-looking fake investment platform where she could see her supposed investments' performances.

On the other hand, I think there were times where Ms D didn't act as I'd reasonably expect. Namely, while I recognise how Ms D was enticed by this scam, as I have set out above I think there were some dubious and suspicious signs that I think she ought reasonably to have acted on. In view of this I think it is fair for Metro to refund 50% from the first payment on 18 January 2024, to take account of Ms D's contributory negligence.

Recovery

I've also considered whether Metro did enough to recover the money Ms D lost in this scam.

In this case, Metro wasn't able to recover any of the money lost in this scam, as by the time Ms D made it aware she had been scammed the money had already been transferred to the scammers and could not be recovered.

Putting things right

In order to put matters right Metro Bank PLC should pay Ms D:

- 50% of the money she lost from the first payment on 18 January 2025 of £1,400;

- less the £149.65 that was transferred to Ms D's account on 29 January 2024; and

- pay 8% simple interest per year on these sums calculated to run from the date the payments left Ms D's account until the date the settlement is paid.

My final decision

For the reasons I've explained above, I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms D to accept or reject my decision before 6 February 2026.

Suzannah Stuart
Ombudsman