DRN-5136948

The complaint

Mr B complains that Metro Bank PLC ("Metro") hasn't refunded the £19,989.66 he lost as the result of a job scam.

What happened

Between 10 February 2023 and 4 April 2023 Mr B made 12 faster payments totalling £19,989.66

Transaction #	Date	Payee	Debit	Credit
1	10/02/23	Cryptocurrency S	£585	
2	10/02/23	Cryptocurrency S	£305	
3	10/02/23	Cryptocurrency S	£500	
4	10/02/23	Cryptocurrency S	£250	
	12/02/23	Metro called Mr B		
5	24/02/23	Cryptocurrency S	£3,200	
6	24/03/23	Cryptocurrency S	£6,300	
	24/03/23	Cryptocurrency S (bounced back)		£6,300
7	24/03/23	Cryptocurrency S	£6,300	
	27/03/23	Cryptocurrency S (bounced back)		£6,300
	27/03/23	Mr B called Metro		
8	27/03/23	Cryptocurrency S	£3,000	
	28/03/23	Cryptocurrency S (bounced back)		£3,000
9	27/03/23	Cryptocurrency B	£3,299.72	
10	28/03/23	Cryptocurrency B	£2,798.19	
11	28/03/23	Cryptocurrency B	£798.30	
12	30/03/23	Cryptocurrency B	£2,488.55	
13	03/04/23	Cryptocurrency B	£3,002.91	
14	04/04/23	Cryptocurrency B	£761.99	

Our investigation upheld the complaint in part. He thought Metro ought to have been concerned by the time Mr B made the payment of £3,299.72 on 27 March 2023 and should refund this and the transactions that followed. However, he also considered Mr B should share in the responsibility for these losses so he considered the refund should be reduced by 50%.

Mr B accepted the view. Metro didn't agree. It said these are payments made to the consumer's own account, and it is not reasonable to ask the bank to refund these. Mr B was not truthful and as he hadn't been forthcoming when previously questioned there no evidence to suggest any further intervention would have prompted him to be honest.

As the case could not be resolved informally, it has been passed to me for a 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.

I'm sorry to hear about this cruel scam and the impact it has had on Mr B.

When considering what is fair and reasonable, I'm also required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

Having done so, I've reached the same outcome as the investigator, broadly for the same reasons.

The starting position in law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, where the customer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though they authorised the payment.

The payments in this case are not covered by the Lending Standard Board's Contingent Reimbursement Model (CRM) Code or the new Faster Payment Scheme Reimbursement (FPS) Reimbursement Rules. The latter came into force after the payments were made, but in any event both schemes only apply to certain types of payment made, in pounds sterling, between accounts based in the U.K and to an account not in the consumer's own name.

That said, a bank still has wider obligations and a duty to protect its customers, as far as is reasonably possible, against the risk of financial harm from fraud and scams.

Taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in March 2023 that Metro should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms 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, or provided additional warnings, before processing a payment.
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

In the six months before the scam, the account was generally used to receive and transfer funds. Whilst Mr B made payments to various payees regularly, the transactions on the account were of relatively low value. There was one transaction to a (non-cryptocurrency) account in his own name in January 2023 for £3,890. But other than that, the usual day to

day activity was for low value payments.

I am also mindful that banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

I think the initial payments were still relatively low in value. In my view, there was nothing about the payments that ought reasonably to have led Metro to have any concerns at this point.

That said, Metro was concerned *as it did intervene* on 12 March 2023 and spoke to Mr B. It was clear from this call it was specifically concerned about scams – despite the money going to an account in his own name. The caller handler asked Mr B about payments three and four and asked him if it was for an investment. Mr B confirmed it was and that he'd been investing in the company for four years. Although the call handler didn't probe further or give any warnings – I think at this stage, Metro could only be reasonably expected to have warned about investment scams given what Mr B disclosed and what it could see about the destination of the payments.

Similarly for the payment on 24 March 2023, given the amount and knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, Metro ought to have provided a warning (whether automated or in some other form) that addressed the key risks and features of the most common cryptocurrency scams at the time – cryptocurrency investment scams.

But Mr B wasn't sending payments in connection with an investment opportunity. So, I'm not convinced that a warning relating to cryptocurrency investment scams would have resonated with Mr B and the circumstances he found himself in. I think it's likely that Mr B would have seen a warning about investment scams involving cryptocurrency and disregarded it, as he wasn't making an investment, and he'd likely have proceeded with the £3,200 payment.

However, by the time Mr B made the £3,299.72 payment on 27 March 2023, there had been three returned large transactions from S, during which time Mr B had also called Metro to find out why the payments were being returned. I think there was an opportunity here for Metro to delve deeper into why Mr B was making increasingly large transactions towards cryptocurrency (which at the same time were being returned); to make sure he wasn't at risk of financial harm from fraud.

I've thought about whether Mr B would have maintained he was investing. In doing so I've carefully considered the call on 12 March 2023. Whilst I concluded earlier - that I didn't think Metro needed to do anymore at that point, by 27 March 2023 I think it needed to do much more probing and questioning given the more concerning pattern of transactions that had emerged.

Listening to the call of 12 March 2023 (and reading the instant messages between Mr and the scammer), it doesn't seem to me that Mr B had a cover story prepared or that he was being coached about what to say. He simply acknowledged the call handler's own conclusion (that this was an investment) and divulged that he'd used the cryptocurrency provider for a number of years. On balance, I think if Metro had asked more open and probing questions it would have quickly established Mr B wasn't making payments in relation to an investment but rather to a job opportunity. And if it had warned him about the key features of such a scam, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money, I think this would have given the perspective Mr B needed and he would more likely than not have concluded that the scheme was not genuine. In those circumstances I think, he's likely to have decided not to go ahead with the £3,299.72 payment and those transactions that followed, had such a warning been given.

I've thought about whether Mr B should bear any responsibility for his loss connected to the £3,299.72 payment onwards. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Mr B's own actions and responsibility for the losses he has suffered.

I'm not going to go in detail here, as Mr B accepted the investigator's conclusions but for completeness; I agree. I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible looking job platform. And Mr B did ask for a link to the company's website. But the scam appears to have had some features that made its plausibility questionable - certainly by the time of the payment I'm upholding from. I think that on some level Mr B ought reasonably to have questioned whether the activity he was tasked with carrying out (which does not appear to be unduly time-consuming or difficult) was capable of generating the returns promised.

I recognise that the scam operates on a cruel mechanism – always making the victim believe that a further (seemingly final) top up to clear the negative balance will allow them to get back what they've put in along with profits made. But I think Mr B should have become increasingly aware of this risk before making the payments I am asking Metro to refund.

So, given the above, I think it fair that he should bear some responsibility for his losses. I've concluded, on balance, that it would be fair to reduce the amount Metro pays Mr B in relation to £3,299.72 payment onwards because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

The payments were made to a cryptocurrency account in Mr B's own name. Mr B sent that cryptocurrency to the fraudsters. So, Metro would not have been able to recover the funds.

Putting things right

In order to put things right for Mr B, Metro Bank PLC should

Refund Mr B 50% of transactions 9 -14.

Because Mr B has been deprived of this money, I consider it fair that Metro Bank PLC add 8% simple interest to the above from the date of the transactions to the date of settlement.

If Metro Bank PLC is legally required to deduct tax from the interest it should send Mr B a tax deduction certificate so he can claim it back from HMRC if appropriate.

My final decision

My final decision is that I uphold this complaint in part, and I require Metro Bank PLC to put things right for Mr B as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 27 August 2025.

Kathryn Milne
Ombudsman