

The complaint

Mrs A says Metro Bank PLC (“Metro”), didn’t do enough to help when she fell victim to a an ‘authorised push payment’ (“APP”) cryptocurrency investment scam. She says Metro should reimburse her for the money she lost.

What happened

As both parties are familiar with the circumstances of this complaint, I’ve summarised them briefly below.

In summary, Mrs A fell victim to a cryptocurrency investment scam. Mrs A was duped into believing she was liaising with a genuine investment firm and made a payment of £1,500 from her Metro account to a cryptocurrency account in her own name, and then from there, on to what she thought was a company and adviser that would invest for her.

Unfortunately Mrs A had in fact cruelly been duped by fraudsters. Mrs A uncovered that she had fallen victim to a scam when she was unable to withdraw any funds / profits.

Mrs A reported the matter to Metro who ultimately didn’t consider it was liable for the losses she incurred.

Unhappy, Mrs A brought her complaint to our service. Our Investigator reviewed the matter and didn’t recommend the complaint be upheld.

Ultimately the Investigator explained the ‘Contingent Reimbursement Model (‘CRM code’), which Metro is a signatory of, didn’t apply to the payment Mrs A made. They explained the payment was made to an account in her own name at the cryptocurrency exchange provider so wasn’t covered by the CRM Code as the CRM Code requires consumers to pay ‘another person’. So they didn’t consider Metro were liable to reimburse Mrs A because of any obligation under the CRM Code.

Our Investigator also didn’t think Metro ought to have done more to identify the payment as potentially fraudulent in the circumstances. They didn’t consider Metro ought to have had a cause for concern that Mrs A was potentially at risk of financial harm, or that she was falling victim to a scam to an extent that it ought to have intervened and questioned her further about the payment she made.

With regards to the recovery of any funds, as Metro explained that it had received a response from the beneficiary bank advising that no funds remained, the Investigator considered there wasn’t anything further that Metro could do to recover the funds. Mrs A disagreed with the Investigator’s opinion and as the matter hasn’t been resolved, it’s been passed to me to decide.

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 deciding what's fair and reasonable in all the circumstances of a complaint, 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.

I'm aware that I've summarised this complaint and the responses briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here – which is to determine whether Metro are liable to reimburse Mrs A under the CRM Code and whether it should have done more to prevent Mrs A's losses. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as an alternative to the courts.

Having thought carefully about Metro's actions, I'm not upholding Mrs A's complaint. I do appreciate how disappointing this will be for her. Mrs A was a victim of a cruel scam. But in weighing everything up, I don't consider Metro are liable to reimburse her under the CRM Code or otherwise. I'll explain why.

Why the CRM Code isn't applicable

The CRM Code sets out under 'DS1(2) (a)' the scope of what the CRM Code covers in relation to authorised push payment ("APP") fraud. And that is instances where:

“(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or

(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.”

As the payment Mrs A made from her Metro account to the cryptocurrency exchange provider was to an account in her own name, it isn't covered by or within the scope of the CRM Code. This is because Mrs A wasn't paying 'another person'.

The relevant law and regulations in place at the time

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 terms and conditions of the customer's account.

It is agreed by all parties that Mrs A made the payment from her Metro account. So it is the case that Mrs A authorised the payment that is in dispute. And under the Payment Service Regulations 2017 (which are the relevant regulations in place here) that means Mrs A is responsible for it. That remains the case even though Mrs A was the unfortunate victim of a scam.

However there are times when I might expect a bank to question a transaction or payment, even though it may have been properly authorised. Broadly speaking, firms like Metro have certain obligations to protect customers from fraud.

What does this mean for Mrs A?

In this case, I need to decide whether Metro acted fairly and reasonably in its dealings with Mrs A when she made the payment, or whether it should have done more than it did.

I've thought about this carefully. Having done so, I can't fairly say the payment Mrs A made would (or should) have alerted Metro that Mrs A was potentially at risk of financial harm, to an extent whereby it should have carried out some additional checks before processing the payment. So I don't consider Metro are liable for the losses Mrs A incurred. I'll explain why.

I have to be mindful that banks process a high volume of transfers and transactions each day. And a bank has to strike a balance as to when it should possibly intervene on a payment against not holding up or delaying its customer's requests.

Here, I don't consider there is anything unusual or remarkable about the payment or the amount that ought to have alerted Metro to the possibility Mrs A was being scammed or was at risk of financial harm. And I'm also mindful that Metro didn't have a historic relationship with Mrs A as the account had only been opened around 10 days prior to the payment made as a result of the scam. As there wasn't a historic relationship between the parties Metro wouldn't reasonably have been able to determine whether the payment Mrs A was making was unusual or out of character. And while I appreciate £1,500 was a lot of money to Mrs A, given the volume of payments Metro processes, the amount wasn't so significant that I would expect Metro to carry out some additional checks on it.

All things considered; I think it was reasonable that the payment didn't flag as suspicious – and I can't say Metro acted unfairly here.

Recovery of the funds

I have also considered whether Metro did all it could to try and recover the money Mrs A lost. Given Mrs A sent the funds to a cryptocurrency account in her own name – with her money being converted into cryptocurrency and moved on – there wasn't anything further Metro could do to help Mrs A recover her funds.

Summary

While I appreciate Mrs A's been the unfortunate victim of a cruel scam, I think Metro's decision not to refund her in this instance was fair and reasonable in the circumstances.

I say this because I'm satisfied the CRM Code isn't applicable to the payment Mrs A made meaning Metro isn't liable to reimburse her under the CRM Code.

And Metro followed Mrs A's instructions to make the payment and I haven't seen any reason why it shouldn't have done this.

Unfortunately, given the funds Mrs A transferred were exchanged into cryptocurrency and moved on, there wasn't anything further Metro could do to help Mrs A recover her funds as none remained at the receiving account.

My final decision

For the reasons given above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or

reject my decision before 28 December 2023.

A handwritten signature in blue ink, appearing to read 'Matthew Horner', with a stylized flourish at the end.

Matthew Horner
Ombudsman