

## The complaint

Mr S complains that Monzo Bank Ltd ("Monzo") has failed to refund money he lost to a romance scam in 2021.

## What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Mr S fell victim to a romance scam after he met someone through a dating app, ("D") who he then believed he was in a relationship with.

After talking for around six-eight weeks, the scammer convinced Mr S to send money for various reasons, including solicitor's costs and tax payments for the sale of D's company in Egypt. Between 27 August 2021 and 23 November 2021, the following transactions took place from Mr S's Monzo account:

Date	Amount	Payee	Payment Type	Covered by CRM?
27 August 2021	£5,000	Helene	Faster Payment	Yes
27 August 2021	£2,000	JV Beat Ltd	Faster Payment	Yes
28 August 2021	£8,000	JV Beat Ltd	Faster Payment	Yes
29 August 2021	£7,000	Mr S	Faster Payment	No (me to me payment)
4 October 2021	£150	Kam	Faster Payment	Yes
8 October 2021	£7,700	Coinbase	Faster Payment	No (me to me payment)
21 October 2021	£1,200	Coinbase	Faster Payment	No (me to me payment)
31 October 2021	£500	Coinbase	Faster Payment	No (me to me payment)
2 November 2021	£5,000	Donna Ltd	Credit	
2 November 2021	£5,500	Coinbase	Faster Payment	No (me to me payment)
3 November 2021	£2	Coinbase	Credit	

4 November 2021	£5,000	Coinbase	Credit	
4 November 2021	£5,000	Trading Account Limited	Faster Payment	Yes
8 November 2021	£100	Donna Ltd	Credit	
8 November 2021	£102	Binance	Card payment	No
12 November 2021	£5,000	Donna Ltd	Credit	
12 November 2021	£5,000	Binance	Card payment	No
12 November 2021	£5,000	Binance	Credit	
12 November 2021	£5,000	Binance	Card payment	No
15 November 2021	£500	Donna Ltd	Credit	
15 November 2021	£700	Binance	Card payment	No
22 November 2021	£2	Donna Ltd	Faster Payment	No (me to me payment)
22 November 2021	£10	Donna Ltd	Faster Payment	No (me to me payment)
23 November 2021	£633	Donna Ltd	Faster Payment	No (me to me payment)

Mr S had opened several crypto and electronic money accounts under D's instruction (of which the scammer had access to). Mr S was both paying money into these accounts for D and also receiving payments from other parties. He realised he'd been scammed after the police raided his home in November 2022 for fraud/money laundering as a result of the payments he'd been receiving, where it came to light that D had been scamming him and others.

Mr S reported the scam to Monzo, but it said it wouldn't be refunding the money he'd lost. In terms of the payments that weren't covered by the Contingent Reimbursement Model (CRM Code), it didn't consider it was liable for these payments as the money was sent to accounts that Mr S had control of. For the payments that were covered under the Code, it didn't think he had a reasonable basis for believing they were genuine, and also said that he'd prevented it from giving an Effective Warning, so he wouldn't be eligible for any reimbursement. Unhappy with this, Mr S referred the matter to our service.

Our investigator also didn't uphold Mr S's complaint. She didn't think Monzo would be liable to repay any of the payments made that weren't covered under the CRM Code. And for those that were, she thought that Monzo had acted reasonably by relying on the exceptions to reimbursement. Mr S disagreed, so the matter has been escalated to me to determine.

### **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, I've decided not to uphold it. I'll explain why.

It's not in dispute Mr S was scammed here, and I'm sorry about the impact this whole experience has had on him. It's also not disputed that he authorised the payments he made to the scammer. The payments were requested by him using his legitimate security credentials provided by Monzo, and the starting position is that banks ought to follow the instructions given by their customers in order for legitimate payments to be made as instructed.

#### **Payments not covered by the CRM Code**

As part of the scam, there are several payments that Mr S made to an account that was either in his own name (such as the crypto wallets he opened), or that he had opened and had control of (such as the Wise/Revolut accounts in the name of Donna Ltd). As I've set out in the transaction table above, these payments do not fall within the scope of the CRM Code, which only applies to scam payments made to 'another person'. As these payments were effectively made to Mr S himself before being transferred on again to the scammer, they cannot be said to have been paid to another person from his Monzo account and therefore are not covered by the CRM Code. Similarly, any debit card payments Mr S made from his account are also not covered by the Code, which only extends to authorised push payments.

However, I've considered whether Monzo would be liable to refund any the payments Mr S made in line with its expectations to fairly and reasonably be monitoring accounts for fraud, as there are some situations in which a bank should reasonably have had a closer look at the circumstances surrounding a particular transfer. For example, if it was particularly out of character.

I acknowledge that some of the payments Mr S made to either Coinbase, or Binance would have arguably been unusual or suspicious enough to warrant further enquiries being made by Monzo. However, even if Monzo *had* intervened in any of these payments to ask further questions, I'm not persuaded it would have likely stopped Mr S from proceeding or have ultimately prevented his loss.

I say this because Mr S was not upfront or honest with Monzo when he was questioned about earlier payments he'd made as part of the same scam. I can see, for example, that when Mr S was asked to choose a reason for the payments, he selected 'Safe account' on multiple occasions, rather than choosing an option that was applicable to the circumstances of the transaction.

Monzo also questioned Mr S in relation to the payments he made on 27 August 2021. Mr S told Monzo that he had received some funds from an inheritance and that he was making payments to family members who were entitled to part of the inheritance. He didn't at any point mention that he was paying someone he'd never met in person in order to cover the costs of them selling their business overseas. I appreciate Mr S was being told what to say and do by the scammer at each stage, who was assisting him with the payments via remote

access to his laptop, which is why he may have given it false information on 27 August 2021. But it indicates that Monzo would not have been able to get clear and honest answers if it had probed further into any of the payments he was making.

So, overall, even if Monzo *could* have carried out further checks on any of the payments Mr S made and asked more probing questions, I'm not persuaded this would have likely revealed he was falling for a scam or ultimately prevented his loss. Therefore, I don't think Monzo's failure to look more closely into these payments can be considered the proximate cause of Mr S's loss in these circumstances, as it seems likely he would've continued to provide false information in order to make the payments. As such, I don't consider it would be fair and reasonable to hold Monzo liable for any of the payments outside of the CRM Code.

I also don't think there was anything more Monzo could've done to recover the money lost through any of the payments not covered by the CRM Code. In terms of the debit card payments made to Binance, a chargeback claim would've had little prospect of succeeding given Mr S would've received the asset he had paid for (i.e. the cryptocurrency). Similarly, for the faster payments, there would've been no prospect of recovering the money from the receiving accounts either, given we know these accounts were controlled by Mr S and that the funds had already been taken by the scammer by the time the fraud had been reported.

#### Payments covered by the CRM Code

In terms of the remaining faster payments Mr S made from his Monzo account, these were made to 'another person' and so would fall within the scope of the CRM Code (indicated in the transaction table above).

Monzo isn't a signatory to the CRM Code – which requires a firm to reimburse a customer who has been the victim of an APP scam like this one in all but a limited number of circumstances – but it has agreed to abide by its principles.

Under the provisions of the CRM Code, both the bank and its customer have obligations. If it can be shown that the customer has met their requisite level of care, then they will receive full reimbursement. If the customer has not done this, then it is for the firm to show that it has met its obligations under the Code, one of which is the provision of an Effective Warning when the firm identifies an APP scam risk in a payment journey. If a firm has not met its obligations then it, subject to any liability by the bank which received the money, will be liable for 50% of the customer's loss.

In this case, Monzo argues that exceptions to reimbursement under the Code apply as Mr S did not enable it to provide an Effective Warning, and it also does not consider he had a reasonable basis for believing that the recipient of the funds was legitimate, such that he therefore did not meet his requisite level of care. In such circumstances, Monzo would not need to reimburse any of the payments Mr S made to the scammer, so I've considered whether it has fairly relied on these exceptions.

#### Did Mr S have a reasonable basis for belief when making the payments?

Having reviewed this aspect, I'm satisfied there was enough going on from the outset that should have given Mr S serious cause for concern that something simply wasn't right:

- Mr S was under the belief that he was sending money to D to assist with the sale of her business. However, he sent payments to multiple third-party accounts, including different companies, rather than paying any money directly to D to. Mr S said he questioned D about this and says he was told it was easier for her to send and receive funds that way.

But I don't think this was a plausible enough explanation as to why he was having to send funds to multiple third-party accounts in order to help her pay taxes, and it's not clear how D was supposed to have been able to receive the money this way either. Mr S was also told by D that her solicitor was only taking payment in cryptocurrency from now on, which ought to have seemed particularly implausible.

- Mr S had never met D in person or even spoken to her over the phone before he started sending money to her. She claimed to be deaf, to avoid talking to Mr S over the phone, yet she was supposedly still able to deal with multiple parties in the selling of her business. Overall, I'm not persuaded Mr S had enough cause to believe that D was a genuine person.

I appreciate that Mr S was under the spell of the scammer and believed they were in love, which is seemingly why he was willing to follow her instructions. But overall, with all the red flags that were present here, I don't consider that Mr S had a reasonable basis for believing the person he was paying was legitimate. So, I think Monzo has correctly identified that this exception to reimbursement under the Code applies.

#### *Did Monzo meet the standards expected of a firm under the CRM Code?*

Even though I don't think Mr S had a reasonable basis for belief when making the payments, he would still be entitled to a refund of 50% of the money he lost if Monzo didn't meet the standards it has agreed to adhere to under the CRM Code

The CRM code says that, where a firm identifies APP scam risks, it should provide "Effective Warnings" to their customers. It sets out that an Effective Warning should enable a customer to understand what actions they need to take to address a risk and the consequences of not doing so. And it says that, as a minimum, an Effective Warning should be understandable, clear, impactful, timely and specific.

It isn't in dispute that an APP scam risk was identified here for some of the Faster Payments, given that Monzo required Mr S to disclose the reason for the payments so it could provide a scam warning. But on at least three different occasions, Mr S selected "Safe Account" as the reason for him making the payments. This then generated a warning that was specific to safe account scams rather than the particular scam he was falling victim to.

I understand that D was assisting Mr S with making the payments via remote access software, so it seems likely he would've selected this option under the instruction of the scammer, as no part of the scam he's described involved transferring money to any safe accounts. But what is clear is that Monzo has effectively been prevented from providing Mr S with an Effective Warning because he didn't choose an accurate reason. I acknowledge that Monzo shouldn't have theoretically let the payment proceed if it thought Mr S was sending it to a safe account, as this would ordinarily indicate that he was in the process of being scammed. So, I would've expected Monzo to contact Mr S in such circumstances to determine whether he was in fact transferring money to a safe account, or if he had chosen this option by mistake.

As I've set out above, Monzo did get in contact with Mr S about the first two Faster Payments he was making from the account. But after asking him to expand further upon the reason for the payments, he gave a misleading answer and explained he was paying an inheritance to his family members. So, Monzo would've then been reassured that he was not falling victim to a safe account scam.

Therefore, while Monzo may not have provided an Effective Warning in line with the standards expected of firms, I don't think it would be fair and reasonable to ask it to

reimburse 50% of the CRM covered faster payments (that represented an APP scam risk), as Monzo was prevented from being able to give such a warning.

I've also considered whether Mr S would be considered as having been vulnerable at the time he made the payments, as I understand he has been suffering with mental health issues for quite some time. I'm sorry to hear about the issues Mr S has been experiencing; I don't doubt that he has been through a very difficult time, and I accept that this may have had some impact on him at the time. However, I've not seen enough persuasive evidence to demonstrate that this would have prevented him from being able to protect himself from falling victim to this type of scam. So, I'm not persuaded he can reasonably be considered as 'vulnerable' under the CRM Code.

As a result, I don't think Monzo has acted unfairly by declining to reimburse any of the payments Mr S made that are covered under the CRM Code. I also don't think there would've been much Monzo could have done to recover the money either. I say this because the payments in question were made between August and November 2021, yet the fraud wasn't reported until a year later in November 2022. So, while it's not clear if Monzo took sufficient action to try and recover the money, I'm not persuaded it would've had any reasonable prospect of doing so given the time that had passed since the transactions took place.

I appreciate this will likely come as a disappointment to Mr S, and I'm sorry he's fallen victim to such a cruel scam. However, I'm not persuaded Monzo can fairly or reasonably be held liable for any of his loss in these circumstances.

### **My final decision**

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 5 February 2024.

Jack Ferris  
**Ombudsman**