

The complaint

Miss S is unhappy that Monzo Bank Ltd won't refund money she lost as a result of a scam.

What happened

Miss S thought that she'd been contacted by a celebrity (that I'll call C) on a popular social media website. They exchanged messages for several weeks, but each attempt at a video call ended after a few seconds (albeit after Miss S was convinced she'd heard C talking). C offered to send Miss S everything she needed to visit him including a visa, plane ticket, and clothes. C said Miss S would need to pay shipping and customs costs of over \$1,000. Miss S made four bank transfers using her Monzo account towards these costs.

Later, C said Miss S would also need to pay £2,900 because the package had been held at customs. Miss S seems to have been concerned enough at this point to report the matter as a scam to Monzo, but later she appears to have decided to continue to make payments. She couldn't afford to pay the whole amount – so, on the suggestion of the fraudster, she made a series of payments using her debit card to a cryptocurrency provider.

Further requests followed: another £10,000 to release the package and then £5,000 in late payment fees. Miss S said that she couldn't afford to pay these amounts but she made a series of smaller payments after borrowing money from various sources.

When a final request for money came - £500 for delivery, Miss S became suspicious. She contacted the delivery company which was being impersonated and it confirmed it had no package for her.

Miss S initially reported the matter to Monzo soon after the first four payments (all of which were faster payments to another Monzo account). It has agreed to adhere to the principles of the Lending Standards Board Contingent Reimbursement Model ("CRM Code") which requires firms to reimburse victims of APP scams in all but a limited number of circumstances. The CRM Code only covers those first four payments Miss S made (and not the subsequent card payments).

Monzo said it wouldn't refund Miss S as she hadn't taken the necessary steps to protect herself under the CRM Code.

Miss S then appears to have become involved with the fraudsters again, as, in October 2021, she reported the additional transactions, all made to a cryptocurrency exchange. Monzo additionally said that it couldn't be expected to reimburse those transactions as they'd been carried out by Miss S.

Miss S made some payments from another account she holds at a different financial business. That business decided to refund the money she lost as a gesture of goodwill.

The complaint about Monzo was referred to our service but our investigator didn't uphold it. They thought that the scam was implausible and didn't think Monzo ought to have recognised the risk that Miss S might be the victim of a scam.

Miss S, through her representatives, disagreed, arguing:

- C had interacted with her posts on social media and she'd interacted with C's actual mother.
- She'd had a brief video call with the fraudster and was adamant that she'd heard the real C.
- She's received various pieces of legitimate looking paperwork.
- Some of the information that the fraudster provided was consistent with genuine information about C.

As no agreement could be reached, the case was 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.

The starting position under the relevant regulations is that Miss S is responsible for payments she's authorised herself. But I've also considered whether Monzo should refund Miss S under the provisions of the CRM Code and whether it breached its longstanding obligations to be on the lookout for out of character and unusual transactions that might have indicated that Miss S was at risk of financial harm from fraud.

As set out above, the CRM Code only covers the first four payments Miss S made (the rest were card payments, which are excluded under the CRM Code). I've decided Monzo can fairly rely on one of the exceptions to reimbursement set out in the CRM Code, namely that Miss S made the payments without a reasonable basis for believing that the recipient was legitimate and who she was expecting to pay.

As set out by Miss S' representatives, she was a big fan of C. It's clear that she wanted to believe that she was genuinely being contacted by him. I think that desire caused her to continue to engage with the fraudsters despite clear warning signs, many of which she recognised herself. I also have to note that Miss S hasn't been able to provide much of the correspondence with C. That has made it more difficult for me to assess the plausibility of those communications.

I've summarised my reasons for reaching that decision below:

- The premise of the scam: that a celebrity would send her a package in the mail containing expensive items, but she'd need to pay for various charges, was implausible. Miss S seem to have recognised this but proceeded regardless.
- Miss S knew that she could verify the fraudster's claims by contacting the shipping company to check whether it held a package for her (as she did later). But she didn't do this before sending the first four payments.
- Miss S appears to have questioned and been suspicious of the fraudsters throughout. She appears to have had concerns about the fees, the social media profile, the language used in some correspondence and the email addresses used.
- While Miss S may be convinced she'd heard C's real voice over a video call, she ought to have recognised both that it was unusual that C wasn't able to communicate clearly with her and the possibility that such a brief interaction could be faked.
- While Miss S may have had some limited interactions with C or persons connected to him, those interactions did nothing to confirm what the fraudster told her was true.

- The personal information associated with C that the fraudsters utilised appears to have all been in the public domain.

As Miss S' representatives state, she simply didn't want to believe that she wasn't speaking to the real C. That belief appears to have been based largely on hope, so I don't think that Miss S held a reasonable basis for belief in making the payments and I think Monzo can fairly rely on that exception to reimbursement set out in the Code.

I've also considered whether Monzo ought to have recognised that Miss S might be at risk of financial harm from fraud. The payments covered by the CRM Code were all for amounts of less than £500 and although they took place over the course of two days I don't think a concerning pattern had yet developed. So I don't think that Monzo should have been alert to a potential scam risk when processing them and I don't think it was obligated to provide a warning under the CRM Code.

The rest of the payments were card payments to cryptocurrency exchanges. They took place over almost three months and many were for less than £100. There was a single payment of £1,000, which I think stood out somewhat against Miss S' normal account activity. I also note that she doesn't seem to have purchased cryptocurrency before. But, there doesn't seem to be a concerning pattern of transactions here (which is unsurprising given the somewhat unusual nature of the scam) and I must take into account the difficult balancing act Monzo has between not unduly inconveniencing customers making genuine payments (of which there would be a hugely significant number of this size) and trying to prevent fraud.

I've also thought about whether Monzo should have been extra vigilant, given that Miss S had recently reported having been scammed (and retracted and reinstated the allegation once). But, the transactions that followed the initial faster payments were very different in nature and weren't obviously linked to those earlier payments. I also think Monzo would have been reasonably sure that Miss S wasn't going to send any more money to the fraudsters, given the conversations they'd had with her in June and July 2021. Overall, I don't think that the payments that took place were sufficiently unusual or suspicious in nature that Monzo made a mistake by processing the payments without contacting Miss S.

Finally, I've thought about Monzo's efforts to recover Miss S' funds. I understand that the card payments were used to purchase cryptocurrency which was then sent to the fraudster. As such, those payments would not be recoverable. In relation to the faster payments, all of them went to another Monzo account, but it told our service that the money had been removed by the time Miss S initially reported the matter to it on 9 June 2021. So I think Monzo acted reasonably in trying to recover her money.

While I'm sympathetic to Miss S, I don't find that Monzo are responsible for her loss.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 31 May 2023.

Rich Drury
Ombudsman