

The complaint

Miss H complains Monzo Bank Ltd (“Monzo”) didn’t reimburse the money she lost when she was the victim of an ‘authorised push payment’ (“APP”) impersonation scam.

What happened

Both parties are aware of the circumstances of the complaint, so I won’t repeat them all here. But briefly, Miss H was the victim of an impersonation scam.

Miss H received a friend request on a well-known social media website. Miss H thought it was her friend’s mother and accepted. Unbeknown to Miss H it wasn’t her friend’s mother and was in fact a scammer. Miss H was tricked into believing that her friend’s mother had been successful in obtaining money – a grant – from a foundation and that Miss H could also apply. Miss H ultimately made three transfers, totalling £1,253.16, in the belief that she would receive a grant of £50,000.

Miss H had her doubts about what she was doing when she made the payments – but ultimately discovered it was a scam when she spoke to her friend the next day.

Miss H reported the matter to Monzo and to see if it could recover any of her funds.

Monzo logged the details and investigated the matter. Monzo contacted the beneficiary bank (the bank where the funds were sent to) to see if any funds remained that could be recovered. Ultimately £16.63 was recovered and returned to Miss H.

Monzo also considered whether Miss H should be reimbursed for her remaining loss. Monzo considered this in line with the ‘Lending Standards Board Contingent Reimbursement Model’ (the “CRM Code”). Monzo isn’t a signatory of the CRM Code but has explained that it is committed to applying the principles set out in it.

The CRM Code requires firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances. Monzo said one or more of those exceptions applies in this case. It said it gave a scam warning and that Miss H made the payments without having a reasonable basis for believing that: the payee was the person the customer was expecting to pay, the payment was for genuine goods or services, and/or that the person or business with whom they transacted with was legitimate.

Unhappy, Miss H referred the matter to our service. One of our Investigators looked into Miss H’s complaint and thought it ought to be upheld in part. In short, while they agreed that Miss H didn’t have a reasonable basis of belief when making the payments, she felt the second and third payments Miss H made were unusual and out of character and Monzo could have done more under the CRM Code to prevent Miss H from financial harm.

Our Investigator concluded both parties were therefore liable and considered reimbursement of 50% of the funds for the second and third payment would be fair.

Monzo disagreed with the Investigator's opinion and maintained its position. As the matter hasn't been resolved, I have been asked to make a final decision on the outcome of Miss H's complaint.

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.

As I've said above, the CRM Code requires payment service providers to reimburse customers who have been the victims of authorised push payment (APP) scams, in all but limited circumstances. If Monzo declines to reimburse its customer in full, it is for Monzo to establish that its customer failed to meet the requisite level of care under one, or more, of the listed exceptions set out in the CRM Code itself. Those exceptions are:

- where in all the circumstances, the customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay, the payment was for genuine goods or services, and/or that the person or business with whom they transacted with was legitimate; or
- the customer ignored an 'effective warning' by failing to take appropriate steps in response to that warning.

There are further exceptions within the CRM, but none of these are applicable here.

After having carefully considered all of Miss H's testimony around what happened, Monzo's submissions and our investigator's opinion, I agree that shared responsibility for the loss is a fair outcome in the individual circumstances of this case. I'll explain why.

Did Miss H 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 Miss H serious cause for concern that something simply wasn't right.

Miss H was in essence being offered £50,000 for a fee of £1,250. The likelihood of what was being promised was just far too good to be true. From reviewing the messages and Miss H's testimony she clearly had concerns at the time also. Miss H has advised that she searched on the internet and saw negative information regarding the supposed foundation, and it being targeted by scammers. Miss H also explained she didn't get any answers about the grant when she asked. Miss H also queried the beneficiary account name when she received a confirmation of payee 'no match' and was told to skip past it. Miss H had also tried contacting her friend who didn't answer.

To my mind, Miss H was more than reasonably aware that things weren't quite right. And Miss H simply shouldn't have proceeded until she had spoken to her friend or her friend's mother as this would have brought the scam to light. There were enough warning signs that meant Miss H should have been far more careful and carried out a check with her friend before proceeding with any payment.

Overall, I don't find that Miss H had a reasonable basis of belief when making the payments. So I think Monzo has correctly identified that under the CRM Code an exception to full reimbursement applies.

Did Monzo do enough?

Good industry practice requires that regulated firms such as Monzo engage in the monitoring of customer accounts to be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. And under the CRM Code, where it identifies a risk of a customer falling victim to an APP scam, it is required to provide that customer with an “effective warning”.

Monzo provided a warning initially when Miss H set up the new payee and made a transfer of £253.16 at 19:51 on 03 June 2022. Given the value of the payment, I don’t think the CRM Code required that Monzo display an ‘effective warning’ as part of the payment process. And I’m not persuaded it would’ve had any grounds for intervening to question that transfer with Miss H before allowing it to be processed. That said, Miss H acknowledged seeing Monzo’s warning and explained that it did make her think that she may be at risk.

So I think Monzo, while not required to give an effective warning under the CRM Code for the transfer of £253.16, did more than what was required of it in the circumstances of this specific payment.

However, Miss H went on to make a further two transfers of £500 each at 21:08 and 22:35. I don’t think Monzo did enough here. As explained, Monzo has to be on the lookout for suspicious or out of character transactions in order to try and identify the risk of a customer falling victim to an APP scam. Here, taking into account Miss H’s account usage based on the statements provided, I consider the activity was unusual. Miss H rarely made faster payments; I can see she made three faster payments in the six months prior to the scam. And I’m mindful that the faster payments she did make were to an existing payee.

To my mind, I consider it is reasonable to suggest that Miss H, in setting up a new payee and making a payment, and then making a further payment to the same payee around an hour later can be considered as unusual activity. I think Monzo ought to reasonably have identified that Miss H was potentially at risk when she made a second, larger payment to the same payee as the risk of financial harm had increased. And in this instance, I consider it ought to have led to Monzo providing an effective warning as set out by the CRM Code for the second and third payments. I’m not satisfied that its low friction warning provided initially was sufficient or that Monzo has demonstrated an effective warning was subsequently provided in relation to the second and third payments.

So I don’t consider, for the second and third payment, that it is fair for Monzo to rely on the exception that Miss H ignored an effective warning to decline full reimbursement.

With all of this in mind, while I am sorry that Miss H fell victim to a scam, I don’t find that she had a reasonable basis for believing the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate. So I consider an exception to full reimbursement applies under the CRM Code.

But I also find that Monzo didn’t meet its obligations under the CRM Code as it didn’t provide an effective warning when I consider it should have done for the second and third payments.

Overall I consider a fair outcome in this case would be for Monzo to reimburse Miss H 50% of the second and third payments – with Miss H sharing some responsibility for the loss also.

My final decision

For the reasons outlined above, I’ve decided it is fair and reasonable to uphold Miss H’s complaint about Monzo Bank Ltd in part. I therefore require Monzo Bank Ltd to pay Miss H:

- 50% of payments two and three (less any sums from these amounts that have already been recovered and returned); and,
- 8% simple interest per year on that amount calculated from the date Monzo Bank Ltd originally declined Miss H's claim under the CRM Code until the date of settlement.

I direct Monzo Bank Ltd to pay compensation, as set out above, within 28 days of receiving notification of Miss H's acceptance of my final decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss H to accept or reject my decision before 29 December 2022.

Matthew Horner
Ombudsman