DRN-3979971

The complaint

Miss K says Monzo Bank Ltd ("Monzo"), didn't do enough to help when she fell victim to a an 'authorised push payment' ("APP") investment scam. She says Monzo 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, Miss K fell victim to a cryptocurrency investment scam. Miss K says she was invited to be part of a group about making money on an instant messaging service. Miss K was shown that she could make good returns. She was promised returns of 15% and was also told that if she deposited $1,000, she could make daily profits of $200.

Miss K made two payments to a third party and then subsequently made four payments to a cryptocurrency account in her own name, and then from there, on to what she thought was a company that would invest for her.

The payments Miss K made were as follows:

Date	***Time***	***Type of transfer***	***Amount***
23/01/2022	7.38pm	Faster payment to third party	£1,400
23/01/2022	10.23pm	Faster payment to third party	£100
31/01/2022	6.59pm	Faster payment to own cryptocurrency account	£1,040
31/01/2022	8.37pm	Faster payment to own cryptocurrency account	£743.50
01/02/2022	5.02pm	Faster payment to own cryptocurrency account	£900
02/02/2022	5.29pm	Faster payment to own cryptocurrency account	£350
		Total	***£4,533.50***

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

Miss K reported the matter to Monzo on 29 March 2023. Monzo also reached out to the beneficiary bank (the bank where payments 1 and 2 were sent to) to see if any funds remained that could be recovered. Unfortunately Monzo received a response advising that no funds remained. Monzo also didn't consider it was liable for the losses Miss K incurred.

Unhappy, Miss K 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 Monzo adheres to the principles of, was applicable to the first two payments Miss K made – as they were faster payments made to a third party.

The CRM Code is a voluntary code which requires Firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances.

While these two payments were covered by the CRM Code, our Investigator considered Monzo had fairly applied an exception to reimbursement – namely that Miss K didn't have a reasonable basis of belief when making the payments. And given the value of payments one and two they didn't think Monzo needed to provide an 'effective warning' as part of the payment process.

For the remaining four payments Miss K made, as these were made were to an account in her own name at the cryptocurrency exchange provider our Investigator considered they weren't covered by the CRM Code as the CRM Code requires consumers to pay 'another person'.

And in relation to these four payments, our Investigator didn't think Monzo ought to have done more to identify the payments as potentially fraudulent in the circumstances. They didn't consider Monzo ought to have had a cause for concern that Miss K 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 transfers.

With regards to the recovery of any funds, our Investigator considered that Monzo had acted in a timely manner and provided evidence to show it had contacted the beneficiary bank but unfortunately no funds remained that could be recovered.

Miss K 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.

Having thought carefully about Monzo' actions, I'm not upholding Miss K's complaint. I do appreciate how disappointing this will be for her. Miss K was a victim of a cruel scam. But in weighing everything up, I don't think I can fairly say Monzo should reimburse her under the CRM Code or otherwise. I'll explain why.

There's no dispute that Miss K authorised the payments that are the subject of this complaint, even though she did so as a result of being deceived by a fraudster. Broadly speaking, under the account terms and conditions and the Payment Service Regulations 2017, she would normally be liable for it. But that isn't the end of the story.

Payments 1 and 2

Where a customer has been the victim of a scam it may be appropriate for the bank to reimburse the customer, even though payments have been properly authorised. Of particular relevance to the question of what is fair and reasonable in this case is the CRM Code.

Payments 1 and 2 are covered by the CRM Code – as Miss K made a payment via faster payment, in sterling and the payments were to 'another person' with the beneficiary account being a UK domiciled account.

The CRM Code requires Firms to reimburse customers who have been the victims of APP scams like this, in all but a limited number of circumstances. If a Firm chooses not to reimburse a customer, it is for the Firm to establish that one of the listed exceptions to reimbursement as set out in the CRM Code apply.

Under the CRM Code, a Sending Firm (in this case Monzo) may choose not to reimburse a customer if it can establish that*:

- The customer made 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
  - the person or business with whom they transacted was legitimate.
- The customer ignored what the CRM Code refers to as an “Effective Warning” by failing to take appropriate action in response to such an effective warning

*_Further exceptions outlined in the CRM Code do not apply to this case._

In this case, I think Monzo has been able to establish that it may choose not to reimburse Miss K under the terms of the CRM Code. I’m persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies.

Taking into account all of the circumstances of this case, including the characteristics and complexity of the scam, I don’t think Miss K 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.

In order to determine whether this exception to reimbursement applies, I must ask if Miss K made the payments she did whilst having a reasonable basis for belief that all was genuine. Having carefully reviewed everything I’m afraid I don’t find that’s the case. I’ll explain why.

Miss K was invited to be a part of a group on an instant messaging service which was about making money. But having reviewed this aspect and the messages Miss K has provided, I find there was enough going on that reasonably should have given Miss K cause for concern that things weren’t right and there were enough warning signs that meant Miss K should have carried out further checks before proceeding with any payments. I say this because Miss K didn’t know anyone within the group and Miss K was told that she could make profits of 15% and also $200 a day if she deposited $1,000. This type of return is wholly unrealistic, and it appears Miss K simply accepted what she was being told at face value when reasonably it should have caused concern.

There were other factors that should have reasonably caused Miss K to question things also. Miss K made the first two payments to a third-party account and not into the name of a company or a business account for example. Miss K has explained that she was told it was the ‘sons’ account and that this was the procedure and she felt reassured that it was a family company. However I don’t find this plausible. Legitimate companies or investment firms don’t operate in this manner and Miss K should have been concerned or questioned what she was being asked to do here.

Overall, there was enough going on that should have given Miss K more than a cause for concern. To my mind it is reasonable to suggest that this should have led to Miss K questioning the legitimacy of it all and what she was being told and the returns she was being promised. So I think Monzo have acted fairly in choosing to decline reimbursing Miss K under the CRM Code under the grounds that an exception to reimbursement applies.

Good industry practice requires that regulated firms such as Monzo engage in the monitoring of customer accounts and 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 identified a risk of a customer falling victim to an APP scam, it was required to provide that customer with an "effective warning".

We now know, with the benefit of hindsight, that Miss K was falling victim to a scam. But based on the information that was available to it at the time, I don't consider Monzo would've had any reasonable basis for coming to that conclusion. I say this because the payments wouldn't have appeared out of character or unusual. The payments weren't particularly large or remarkable. So 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 the payments with Miss K before allowing them to be processed.

I have also considered Miss K's circumstances at the time of making the payments and I thank her for being open with our service in this regard. However upon reviewing this aspect, I'm not persuaded Miss K was 'vulnerable' under the CRM Code which would allow for an automatic refund of payments 1 and 2. To my mind Miss K ought reasonably to have been able to protect herself from becoming a victim to this type of APP scam at the time. As explained above, it seems Miss K simply took what she was being told at face value whereas the returns she was being promised ought to have raised concerns. I think it is reasonable to say that Miss K wasn't vulnerable to an extent whereby she couldn't have questioned what she was being told.

Payments 3 - 6

Before I go on to explain my findings in relation to payments 3 - 6, I want to clarify for Miss K's benefit why the CRM Code isn't applicable in her case and what the relevant law and regulations were at the time.

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 transfers Miss K made from her Monzo account to the cryptocurrency exchange provider were to an account in her own name, they aren't covered by or within the scope of the CRM Code. This is because Miss K 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 Miss K authorised all the transfers that are in dispute. And under the Payment Service Regulations 2017 (which are the relevant regulations in place here) that means Miss K is responsible for them. That remains the case even though Miss K 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 Monzo have certain obligations to protect customers from fraud.

What does this mean for Miss K?

In this case, I need to decide whether Monzo acted fairly and reasonably in its dealings with Miss K when she made the four transfers, 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 four transfers Miss K made would (or should) have alerted Monzo that Miss K was potentially at risk of financial harm, to an extent whereby it should have carried out some additional checks before processing the payments. So I don't consider Monzo are liable for the losses Miss K 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 payments or the amounts that ought to have alerted Monzo to the possibility Miss K was being scammed or was at risk of financial harm. All things considered; I think it was reasonable that the payments didn't flag as suspicious – and I can't say Monzo acted unfairly here.

Recovery of the funds

I have also considered whether Monzo did all it could to try and recover the money Miss K lost.

For payments 1 and 2, Monzo was limited in terms of what it could do here; it could only ask the Receiving Firm to return any money that remained in the recipient account. It needed to make enquiries quickly for the best chance of recovery. The evidence I've seen persuades me Monzo did act quickly. Unfortunately, it is common for fraudsters to withdraw or move the money on as quickly as possible. While Miss K, after realising she was the victim of a scam, reported the matter – it was on 29 March 2023, nearly two months after she had made the payments. And unfortunately, no funds remained that could be recovered, so there was nothing more Monzo could do.

For payments 3 - 6 given Miss K 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 Monzo could do to help Miss K recover her funds.

Summary

I'm sorry Miss K lost her money in this way. But for the reasons explained, I find:

- for payments 1 and 2, Miss K didn't have a reasonable basis for believing the payments were for genuine goods or services; and/or the person or business with whom she transacted was legitimate. So I consider it was fair and reasonable for Monzo to decline to reimburse her for her losses under the CRM Code. And, given the value of the payments, Monzo wasn't required to provide an 'effective warning' as part of the payment process.

- for the remaining four payments Miss K made, Monzo wouldn't have been alerted to the fact Miss K was potentially at risk of financial harm, to an extent whereby it should have carried out some additional checks before processing the payments – so isn't liable for the losses she incurred.
- Monzo acted in a timely manner in attempting to recover any funds from the beneficiary bank for payments 1 and 2 but unfortunately none remained. And there was nothing it could do to recover the remaining payments Miss K made as they had already been moved on to the scammer from her cryptocurrency 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 Miss K to accept or reject my decision before 26 July 2023.

Matthew Horner
Ombudsman