

## Complaint

Miss V is unhappy that Monzo Bank Ltd didn't reimburse her after she told it she'd fallen victim to a scam.

## Background

In late September 2023, Miss V was contacted by a recruiter. They claimed to hire for a company I'll refer to as F. Miss V was not looking for a job. However, her CV was on several recruitment websites, so she says she didn't find the contact unusual. The recruiter persuaded her to take the job, which involved completing tasks on an online platform maintained by the employer. She was told that the commitment in terms of hours was flexible and she could work remotely and so, from Miss V's perspective, it was a simple way to earn extra income. Unfortunately, this wasn't a genuine job opportunity. Miss V had been contacted by fraudsters. Miss V looked up F online and it seemed like a legitimate company. It subsequently turned out that fraudsters had imitated F to appear genuine.

Miss V was told she would complete tasks on F's platform and that she'd earn commission for the work she completed. She was also added to a WhatsApp group with other participants. I understand she did receive some very small returns that she was able to withdraw from the platform at the outset. However, after a while, her account balance went negative. She was told that, due to the way the platform operated, she needed to deposit funds if she wanted to continue earning. Miss V did so in the anticipation of earning them back.

She used her Monzo account to make these payments:

1	17 September 2023	£31
2	17 September 2023	£5
3	20 September 2023	£130
4	28 September 2023	£200
5	28 September 2023	£870
6	29 September 2023	£2,370
7	1 October 2023	£2,000
8	1 October 2023	£4,305
9	1 October 2023	£300
10	2 October 2023	£2,900

These funds went to an e-wallet on a cryptocurrency exchange in Miss V's name. They were converted to cryptocurrency and then she transferred them into the control of the fraudsters. As I understand it, she did so in the sincere belief that this was the correct mechanism for

“funding” her account on the employer’s platform.

She later realised that the job opportunity hadn’t been a legitimate one and that she’d fallen victim to a scam. She contacted Monzo, but it declined to refund her. She wasn’t happy with that and so she brought her complaint to this service. An Investigator upheld the complaint in part, concluding that Monzo should’ve intervened at payment 8. If it had done so, the Investigator was persuaded that Miss V’s subsequent losses would’ve been prevented. However, she also thought it was fair and reasonable for Miss V to bear some responsibility for her own losses by way of contributory negligence. She said it was fair and reasonable for Monzo to make a 50% deduction from any redress due to Miss V.

Miss V accepted the decision. Monzo disagreed. As a result, the complaint has been passed to me for a final decision.

## Findings

I’ve considered all the available evidence and arguments to decide what’s fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations 2017 and the terms and conditions of the customer’s account. Monzo has agreed to follow the terms of the Lending Standards Board’s Contingent Reimbursement Model (CRM) Code. However, the Code doesn’t cover these payments.

They were used to purchase cryptocurrency. As a result of the transactions, Miss V did take ownership of the underlying cryptoassets, albeit briefly. In other words, the transactions that left her Monzo account were legitimate purchases of cryptocurrency. In summary, the CRM Code requires that she *“transferred funds to another person for what [she] believed were legitimate purposes but which were in fact fraudulent.”* The fact that she later transferred the cryptocurrency to a blockchain address controlled by the fraudster doesn’t mean that these initial payments weren’t for legitimate purposes.

Although the CRM Code doesn’t apply to these transactions, good industry practice required that Monzo be on the lookout for payments that were out of character or unusual to the extent that they might have indicated a fraud risk. On spotting such a payment, I’d expect it to intervene in a manner proportionate to the risk identified.

The Investigator thought Monzo should’ve acted in connection with payment 8 in the table above and I’d agree with that conclusion. In itself, the payment was fairly large, it came immediately after a payment of £2,000, was to a high-risk payee and significantly depleted the balance on Miss V’s account. These factors taken together indicated a greater than normal risk of fraud. Monzo shouldn’t have processed that payment without first making enquiries with Miss V to satisfy itself that she wasn’t at risk of financial harm due to fraud.

I’ve considered Monzo’s comments regarding Regulation 82 of the Payment Services Regulations 2017. This regulation sets out what steps a payment service provider (PSP) should take when it chooses not to process a customer’s payment and the information it should make available to that customer. It doesn’t set any limits or restrictions on how a PSP might exercise its discretion to decline to make a payment. Overall, I’m not persuaded it’s relevant to the outcome here.

I have also taken into account the Supreme Court’s decision in *Philipp v Barclays Bank UK PLC [2023] UKSC 25*. In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks when making payments. Among other things, it said,

in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, the bank must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- The express terms of the current account contract may modify or alter that position. For example, in *Philipp*, the contract permitted Barclays not to follow its customer's instructions where it reasonably believed the payment instruction was the result of authorised push payment ("APP") fraud, but the court said having the right to decline to carry out an instruction was not the same as being under a duty to do so.

In this case, the terms and conditions applicable to Miss V's Monzo account conferred on it rights (but not obligations) to:

1. Block payments where it suspects criminal activity on the account, or to protect the customer from fraud.
2. Refuse to make a payment if it suspects the customer is a victim of fraud. Not make a payment if it reasonably believes the payment may be connected to a scam, fraud, or other criminal activity.

The starting position at law, therefore, was that:

- Monzo was under an implied duty at law to make payments promptly.
- It had a contractual right not to make payments where it suspected fraud.
- It had a contractual right to delay payments to make enquiries where it suspected fraud.
- It could therefore refuse payments, or make enquiries, where it suspected fraud, but it was not under a contractual duty to do either of those things.

Whilst the current account terms did not oblige Monzo to undertake fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded it from doing so before making a payment.

Whilst Monzo was not required or obliged under the contract to undertake checks, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good practice at the time, it should *fairly and reasonably* have been on the look-out for the possibility of APP fraud and have taken additional steps, or carried out additional checks, before processing payments in some circumstances – as in practice all banks, including Monzo, do.

In this case, for the reasons I have explained I am satisfied it should have intervened at payment 8. It should have contacted Miss V to establish the circumstances surrounding that payment. Having established that she was making payments in connection with an employment opportunity, it should then have gone on to warn her appropriately that such opportunities are likely to be fraudulent.

There's no good reason to think Miss V wouldn't have responded to the bank's queries openly and honestly. I've seen the communications between her and the scammer. There's nothing there that suggests she was told that she'd need to mislead the bank if it asked her questions about the payments. This was a commonly occurring scam type at the point Miss V made this payment, so I don't think it would've been particularly difficult for the bank to have uncovered what was going on and explained things to her.

I've also considered whether it would be fair and reasonable for her to bear some responsibility for her own losses here. In doing so, I've considered what the law says about contributory negligence but kept in mind that I must decide this complaint based on what I consider to be fair and reasonable in all the circumstances. I've considered the evidence carefully and, while I accept Miss V did genuinely believe that these payments were being made in connection with a legitimate employment opportunity, I'm not persuaded that belief was a reasonable one. There was no formalisation of the arrangement between her and the employer – for example, there was no written contract or even a set of terms and conditions.

In addition to that, the arrangement was an inversion of the normal employer-employee relationship. In most circumstances, people expect to be paid by their employer, rather than the other way around. As far as I can see, there wasn't really any attempt to explain this uncommon arrangement and Miss V doesn't appear to have asked about it. I think she ought to have proceeded only with great caution. Overall, I think it's fair and reasonable for Monzo to make a 50% deduction from the redress payable to her.

I've also taken into account that the loss she suffered didn't occur from the Monzo account. She did genuinely make purchases of cryptocurrency and took ownership of the underlying assets. It was only when she transferred that cryptocurrency on to the fraudster that she sustained any loss. Nonetheless, Monzo ought to have been aware of the risk of multi-stage scams involving cryptocurrency. Such scams have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency have continued to increase since. Overall, I am satisfied that Monzo could have prevented the losses she suffered if it had acted as I've found it should've done.

For completeness, I've also considered whether Monzo did everything it should've done once it became aware that a scam had taken place. But given that these payments were in relation to genuine purchases of cryptocurrency, any recovery of funds wouldn't have been possible.

### **Final decision**

For the reasons I've explained above, I uphold this complaint in part.

If Miss V accepts my final decision, Monzo Bank Ltd needs to refund 50% of payments 8, 9 and 10 in the table above. It should also add 8% simple interest per annum to those sums calculated to run

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss V to accept or reject my decision before 17 January 2025.

James Kimmitt  
**Ombudsman**