

The complaint

Mr S complains that Monzo Bank Ltd won't refund him the money he lost after he fell victim to an Authorised Push Payment ("APP") scam.

In bringing his complaint to this service Mr S is represented, but for ease of reading I will refer to Mr S throughout this decision.

What happened

The background to this complaint is well known to both parties so I won't repeat it all in detail here. But in summary, I understand it to be as follows.

In February 2023, Mr S' wife was contacted by an individual about a job opportunity. Mr S thought this was also a good opportunity for himself to earn some extra income, so he registered his interest and was contacted by a representative of the company. The job involved completing tasks, for which he would earn commission. Believing everything to be genuine Mr S proceeded, but unknown to him at the time, he was communicating with fraudsters. The fraudsters persuaded Mr S to pay his own money to proceed with the work.

Mr S was instructed to open an account with a cryptocurrency platform. He sent money directly to the cryptocurrency platform, or to individuals who were selling cryptocurrency through 'peer-to-peer' exchange platforms. Once his money had been converted into cryptocurrency and sent to his wallet, he was then instructed to send it to accounts controlled by the fraudsters.

Detailed below are the payments Mr S sent from his Monzo account as part of the scam;

Payment	Date	Type of transaction	Amount
1	20.02.2023	Faster payment to Payee 1	£4,000
2	20.02.2023	Faster payment to Payee 2	£2,200
3	20.02.2023	Faster payment to Payee 3	£500
4	24.02.2023	Faster payment to Payee 4	£100
5	24.02.2023	Faster payment to Payee 4	£900
6	24.02.2023	Faster payment to Payee 4	£1,500
7	28.02.2023	Faster payment to Payee 5	£4,000
8	28.02.2023	Faster payment to Cryptocurrency Wallet	£900
	01.03.2023	Return of Payment 7	+ £4,000
	01.03.2023	Return of Payment 8	+ £900
9	01.03.2023	Faster payment to Payee 6	£10
10	01.03.2023	Faster payment to Payee 6	£990
		Total Loss	£10,200

Mr S has said as he had run out of money after making the third payment, he borrowed money from a friend to help him fund the payments from this point.

On 20 February 2023, Mr S reported the second payment in the table above to Monzo, as the cryptocurrency seller he was dealing with had told him that the payment hadn't been received. Mr S thought it may have been a scam (although at this point Mr S didn't suspect it may have been a job related scam). Mr S told Monzo that the payment related to cryptocurrency and was for a currency purchase. But later that day Mr S went back to Monzo and told them it wasn't fraud related and was a bank issue – with the evidence indicating that Mr S did receive, and subsequently move on, the cryptocurrency related to this specific payment.

Mr S said that he'd initially been able to withdraw a small amount back into his cryptocurrency wallet, but the fraudsters persuaded him not to take it back into his bank account, telling him that he could use the money to top up his account for the tasks he needed to complete. But he realised he'd been scammed when the fraudsters told him that he was unable to make withdrawals and was continually told that more payments were needed.

Mr S raised a fraud claim with Monzo, but it didn't agree to reimburse him. In summary, Monzo said it couldn't refund the money lost because the payments weren't lost from Mr S' Monzo account, rather they went to another account (a cryptocurrency account), before then being sent on to the fraudster. So, the loss wasn't from Mr S's Monzo account.

Monzo added that it had provided Mr S with warnings when the payments were made, and it had followed his instructions when making the payments. Monzo added that it had contacted the beneficiary banks (the banks to which the payments were made) but was unable to recover any of the money lost.

Unhappy with Monzo's response, Mr S brought his complaint to this service. One of our Investigator's looked into things and thought the complaint should be upheld in part. In summary, our Investigator thought Monzo ought to have intervened at the point Mr S made the second payment to the fraudster, the payment for £2,200 on 20 February 2023. It was our Investigator's view that had Monzo intervened, at this point, and warned Mr S, it would have made a difference, and he wouldn't have gone ahead with this payment, or the ones that followed.

But our Investigator also thought Mr S should bear some responsibility for his loss. In summary this was because our Investigator thought there was enough going on that ought to have caused Mr S some concern. Overall, our Investigator thought Monzo should refund Mr S 50% of the payments, from the point he made the payment for £2,200 onwards, along with some interest.

Through his representatives, Mr S accepted our Investigator's view. But Monzo disagreed; in summary it said;

- It is hypothetical to say that Mr S would have likely told Monzo that he was sending money to pay for tasks.
- The payments made were proportional to what Mr S had previously told Monzo his annual earnings were.
- The payments were within Mr S' daily limits and Monzo doesn't have the capacity to stop all payments of this nature/value.
- If Mr S had observed the warnings it had provided it may have helped him realise he was being scammed.

As an agreement couldn't be reached, the case has been 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.

It isn't in dispute that Mr S authorised the payments he made to the fraudster. And the starting position is that banks ought to follow the instructions given by their customers for legitimate payments to be made. There are though some circumstances in which a bank may still be reasonably expected to reimburse a customer for payments made as part of a scam.

My fellow Ombudsmen and I have referenced the relevant rules, codes of practice and good industry practice at the time in many previous decisions, both to Monzo and published on our website. But as a reminder, I'll set them out again here.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of the account is that Mr S is responsible for payments he authorised. And, as the Supreme Court has reiterated in *Philipp v Barclays Bank UK PLC*, which Monzo has referred to in its submissions, banks generally have a contractual duty to make payments in compliance with the customer's instructions. 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 consumer's instructions where it reasonably believed the payment instruction was the result of 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, Monzo's December 2021 terms and conditions gave it rights (but not obligations) to:

- Block payments if it suspects criminal activity on a customer's account. It explains if it blocks a payment it will let its customer know as soon as possible, using one of its usual channels (via its app, email, phone or by post).

So, the starting position at law 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 criminal activity.
- It could therefore block payments, or make enquiries, where it suspected criminal activity, but it was not under a contractual duty to do either of those things.

It is not clear from this set of terms and conditions whether suspecting a payment may relate to fraud (including authorised push payment fraud) is encompassed within Monzo's definition of criminal activity. But in any event, whilst the current account terms did not oblige Monzo to

make fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded Monzo from making fraud checks before making a payment.

And, whilst Monzo was not required or obliged under the contract to make 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 made additional checks, before processing payments in some circumstances – as in practice all banks, including Monzo, do.

I am mindful in reaching my conclusions about what Monzo ought fairly and reasonably to have done, that:

- FCA regulated banks are required to conduct their “business with due skill, care and diligence” (FCA Principle for Businesses 2) and to “pay due regard to the interests of its customers” (Principle 6)¹.
- Banks have a longstanding regulatory duty *“to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime”* (SYSC 3.2.6R of the Financial Conduct Authority Handbook, which has applied since 2001).
- Over the years, the FSA, and its successor the FCA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.²
- Regulated banks are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).
- The October 2017, BSI Code, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent

¹ Since 31 July 2023 under the FCA’s new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

² For example, both the FSA’s Financial Crime Guide at 4.2.5G and the FCA’s 2015 “Financial crime: a guide for firms” gave examples of good practice in relation to investment fraud saying:

“A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.

A bank contacts customers if it suspects a payment is being made to an investment fraudster.

A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.”

transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code, but in my view the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now.

- Monzo has agreed to abide by the principles CRM Code. This sets out both standards for firms and situations where signatory firms will reimburse consumers. The CRM Code does not cover all authorised push payments (APP) in every circumstances (and it does not apply to the circumstances of these payments), but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a fair articulation of what I consider to be good industry practice generally for payment service providers carrying out any APP transactions.

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Monzo should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.
- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Monzo have fairly and reasonably made further enquiries before it processed Mr S' payments?

To decide this, I've reviewed the activity on Mr S' account statements, from which the payments were made, for the months leading up to the scam. This is often a finely balanced matter, and I agree with Monzo that it has a difficult balance to strike in how it configures its systems to detect unusual activity or activity that might otherwise indicate a higher than usual risk of fraud. There is a delicate balance to be struck. There are many millions of payments made each day and it would not be possible or reasonable to expect a bank to check each one.

With this in mind, having considered the first payment of the scam, while it is finely balanced as it was a payment to a new payee and was the largest payment Mr S had made from the account, when compared to the months leading up to the scam, I can't fairly say that it would have appeared as so unusual or suspicious that it ought to have alerted Monzo more than it did, that Mr S may have been at risk of financial harm. In providing online warnings, I think

Monzo's response was proportionate, and I wouldn't reasonably have expected its intervention to have gone any further than this.

However, when shortly after making this payment (within 20 minutes) Mr S attempted to make a further payment for £2,200, I'm persuaded there was enough going on that Monzo ought reasonably to have had some concerns and reached out to Mr S, for example through its in-app chat function or by way of a phone call, to make enquiries before allowing the payment to be processed.

I say this because, by this point, this was the second payment to two different payees, within the space of a short period of time for amounts that were larger than Mr S' typical spend. It meant, accumulatively, Mr S was sending over £6,000 within the space of twenty minutes. Overall, the payments here represented a sharp uplift in value, when compared to other payments Mr S had typically made from this account. Alongside this, Monzo would also have been aware – from Mr S contacting Monzo himself about this payment for £2,200, that the payment was intended for the purchase of cryptocurrency. While there can be legitimate payments made for the purchase of cryptocurrency, payments such as this can be indicative of a higher degree of fraud risk.

I appreciate that Monzo have referred to Mr S' annual income. However, I'm not persuaded that this in and of itself detracts from a clear departure from how Mr S typically ran his account, which was most often for low value day to day spending.

Given the above, I'm persuaded Monzo ought to have intervened at the point the payment for £2,200 was being made, on 20 February 2023, and asked a series of questions in order to try and establish the actual scam risk. Of course, I can't know for sure what would have happened had Monzo intervened further on these payments. So I have to base my findings on the balance of probabilities – that is, what I think is more likely than not to have happened, taking into account what I know. Had such an intervention occurred, with proportionate questioning, I'm persuaded it's more likely than not Mr S would have explained to Monzo what he was doing and why, and it would have come to light that Mr S was making payments to individuals for the purchase of cryptocurrency wallets in order to facilitate payments for employment purposes.

From what I've seen Mr S wasn't provided with a cover story. So, I think he'd have been honest about the reason for the payment and explained that he was buying cryptocurrency for the purpose of a job. I'm satisfied that his response is likely to have been concerning given that Mr S thought he was buying cryptocurrency to release tasks to make an additional income. So, I believe that if Monzo had asked the kind of questions it ought to have asked, the scam would have been uncovered and Mr S's loss from this point on could have been prevented.

I'm persuaded that it is the case that, from the point of this payment for £2,200, Mr S' loss was both reasonably foreseeable to Monzo and that it could have been prevented, even though the funds were ultimately lost from the cryptocurrency wallets.

Monzo has argued that the payments from Mr S' Monzo account were made to other accounts before being sent to the fraudsters, so it cannot be considered the point of loss and so it cannot be held liable. But as Monzo ought to be aware, and as has been set out in previous decisions from this service to Monzo, the potential for multi-stage scams ought to have been well known to it at the time. And as a matter of good practice Monzo should fairly and reasonably have been on the look-out for payments presenting an additional scam risk, including those involving multi-stage scams.

And so given the circumstances, I'm persuaded it is fair and reasonable that Monzo, at least in part, bears some responsibility for Mr S' loss.

Did Mr S act reasonably in the circumstances?

Mr S has already accepted the Investigator's opinion that any refund provided should be reduced to account for his own actions as part of the scam, and as I agree with this point, I won't dwell on it, except to say that I think there were a number of things that ought to have led Mr S to proceed with more caution than he did.

While I accept Mr S believed that these payments were being made in connection with a legitimate employment opportunity, I'm not persuaded that belief was a reasonable one. From what I've seen, there was no formalisation of the arrangement between him and the employer – for example, there was no written contract and indeed no clear setting out of the terms of his employment.

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. I also think the level of salary and commission being offered seemed inflated, considering the nature of the work that was being carried out.

Overall, I think it's fair and reasonable for Monzo to make a 50% deduction from the redress payable to him.

Recovering Mr S' money

I've also thought about whether Monzo could have done more to attempt to recover the payments after Mr S reported the fraud.

Monzo did reach out to the beneficiary accounts but was unfortunately unable to recover any of the money Mr S sadly lost. In any event as part of the scam here, Mr S bought cryptocurrency from legitimate sellers, before forwarding it on to fraudsters from his cryptocurrency account. So once Mr S had done that, which it seems he did as soon as the money reached his cryptocurrency wallet, there was then no money to recover.

Putting things right

For the reasons given above, I uphold this complaint in part and direct Monzo Bank Ltd to:

- Refund Mr S £3,100 (being 50% of £6,200 - the sum of the payments made from the payment of £2,200 sent on 20 February 2023 onwards, excluding the payments where the funds were returned to Mr S)
- Pay 8% simple interest per year on the amount being refunded from payments 2 and 3 in the table above only, calculated from the date of loss until the date of settlement, minus any applicable tax*

*Remaining payments were funded by funds Mr S received from a friend, so I'm not persuaded it would be fair or reasonable for Monzo to pay Mr S interest on the remaining payments.

My final decision

For the reasons given above my final decision is that I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 14 August 2025.

Stephen Wise
Ombudsman