

The complaint

Miss I complains that Monzo Bank Ltd won't refund her the money she lost after she fell victim to an Authorised Push Payment (APP) scam.

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 or around May 2023, Miss I was contacted unexpectedly about a job opportunity. She was told the job involved completing tasks, for which she would earn commission. Believing everything to be genuine Miss I proceeded, but unknown to her at the time, she had been contacted by fraudsters. The fraudsters then persuaded Miss I to pay her own money in order to proceed with the work.

Miss I was instructed to convert her money into USDT. She did this through payments to cryptocurrency exchanges and also sent money to individuals who were selling cryptocurrency through 'peer-to-peer' exchange platforms. Once her money had been converted into cryptocurrency it was then sent to accounts controlled by the fraudsters.

Detailed below are the payments Miss I sent from her Monzo account as part of the scam;

Date	Payee	Method of payment used	Amount
29/05/2023	Payee 1	Faster payment outwards	£150.00
31/05/2023	Payee 2	Faster payment outwards	£250.00
31/05/2023	Payee 2	Faster payment outwards	£100.00
01/06/2023	Payee 1	Faster payment outwards	£1,400
01/06/2023	Payee 1	Faster payment outwards	£3,000
01/06/2023	Payee 1	Faster payment outwards	£4,150
06/06/2023	Payee 3	Credit from payee 3	-£40.00
29/06/2023	Payee 3	Faster payment outwards	£40.00
29/06/2023	Payee 4	Faster payment outwards	£1,700
29/06/2023	Payee 4	Faster payment outwards	£2,300
01/07/2023	Payee 5	Faster payment outwards	£2,758
01/07/2023	Payee 6	Faster payment outwards	£1,140
01/07/2023	Payee 7	Faster payment outwards	£242.00
03/07/2023	Payee 8	Faster payment outwards	£2,500
03/07/2023	Payee 8	Faster payment outwards	£1,630
04/07/2023	Payee 8	Faster payment outwards	£3,410

05/07/2023	Payee 8	Faster payment outwards	£3,580
		Total:	£28,310

Miss I realised she'd been scammed when a further payment she was trying to make was held by Monzo. It contacted Miss I to discuss the payment and it came to light that she was making the payments as the result of a scam.

Miss I used money from her savings, borrowed money from friends and took out loans with another bank to fund the payments, which she is now having to pay back.

Miss I raised a fraud claim with Monzo, but it didn't agree to reimburse her.

Unhappy with Monzo's response, Miss I brought her complaint to this service. One of our Investigators 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 Miss I made the payment for £4,150 on 1 June 2023. It was our Investigator's view that had Monzo intervened, at this point, and warned Miss I, it would have made a difference and she wouldn't have gone ahead with this payment, or the ones that followed.

But our Investigator also thought Miss I should bear some responsibility for her loss. In summary this was because our Investigator thought there was enough going on that ought to have led Miss I to have had some doubts. Overall, our Investigator thought Monzo should refund Miss I 50% of the payments, from the point she made the payment for £4,150 onwards, along with interest. Our Investigator added that where Monzo had provided screen shots of Miss I's crypto currency account, showing she had some USDT remaining in her account, at the time the scam was uncovered (that being 613.92 USDT), it would be reasonable for this amount to be deducted.

Through her representatives, Miss I accepted our Investigator's view. But Monzo disagreed; in summary it didn't think it should be liable as the loss was not from Miss I's Monzo account, but from Miss I's cryptocurrency accounts/wallets.

As 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 Miss I authorised the payments she made to the scammers. And the starting position is that banks ought to follow the instructions given by their customers in order 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 Miss I is responsible for payments she 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 April 2023 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*

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.

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 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 of the Contingent Reimbursement Model (CRM Code). This sets out both standards for firms and situations where signatory firms will reimburse consumers. The CRM Code does not cover all APP’s 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:

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.”

- 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 Miss I's payments?

To decide this, I've reviewed the activity on Miss I'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 Monzo 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.

Having considered the first five payments of the scam, on balance, I can't fairly say they were so unusual or suspicious in comparison to her usual activity, that they ought to have alerted Monzo that Miss I may have been at risk of financial harm. The payments weren't so dissimilar in value to other payments that Miss I had made previously and I don't think they ought to have stood out.

However, there were elements here of a pattern starting to emerge – with payments made in quick succession, to multiple new payees, some of which were identifiably related to cryptocurrency. So when, on 1 June 2023, Miss I attempted to make a further payment for £4,150, I'm persuaded Monzo ought reasonably to have had some concerns and made further enquiries before allowing the payment to be processed. I say this because, by this point, it was the third payment on the same day, to a third new payee within the space of just four days, with the amount and frequency escalating – and Monzo will be aware that multiple escalating payments being made in quick succession can be indicative of financial harm. By the time she was making the payment of £4,150, Miss I would have cumulatively paid over £8,000 within a short period of time on the same day.

As mentioned above, the sequence here included payments which were identifiably linked to cryptocurrency, and while there can be legitimate payments made for the purchase of cryptocurrency, payments such as this can be indicative of a higher degree of risk of fraud. There doesn't appear to have been these sorts of payments being made from Miss I's account previously and, on balance, I think the payments were becoming out of character compared to the typical sort of spending associated with Miss I's account.

For the reasons explained, I'm persuaded Monzo ought to have stepped in at this point. The intervention from Monzo ought to have involved questioning to help identify the purpose of the payment and type of scam Miss I may have been at risk of. At the time these payments were made Monzo ought fairly and reasonably to have been aware of cryptocurrency scams and, more specifically, job/task scams that often rely on the use of cryptocurrency wallets.

Had such an intervention occurred, with proportionate questioning, I'm persuaded it's more likely than not Miss I would have explained to Monzo what she was doing and why. That would then have clearly revealed the scam to Monzo who could in turn have prevented Miss I from proceeding. I think this is supported by what happened when Monzo did go on to stop a later payment that Miss I attempted on 6 July 2023. Here Monzo contacted Miss I, on 8 July 2023, to discuss the payment and the scam came to light. I think it's a reasonable conclusion to reach that had this intervention from Monzo come sooner, as for the reasons I've explained above I think it ought to have done, then the scam would have come to light sooner than it did.

I'm persuaded it is the case that, from the point of this payment for £4,150, Miss I'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 Miss I'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.

I'm mindful that Monzo has argued that even after its intervention Miss I went on to make a further payment to the fraudster. But I think it's important to note that, after its intervention, Miss I didn't make any further payments to the fraudsters from her Monzo account after it had intervened. Rather, the payment was made from an account she held with another provider.

I'm not persuaded it automatically follows that just because Miss I went on to make one further payment, it means Monzo is discharged from its responsibilities to be on the lookout and to protect its customers from the risk of financial harm. Alongside this, it is arguable that had Monzo's intervention come sooner, as I think it ought to have done, Miss I would likely have been less invested in the scam, than she became, and so would have been less likely to have made such desperate attempts to try and recover her money.

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

Did Miss I act reasonably in the circumstances?

I've also thought about whether Miss I did enough to protect herself from the scam, and, having thought carefully about this, I don't think she did. I think she ought reasonably to have had concerns about the legitimacy of the job offered given the requirement to send funds to acquire the salary she'd supposedly earned. I also think receiving an unsolicited job offer – unrelated to her usual field of work – via a mobile messaging service app should've been seen as unusual to Miss I, and so should have led to her looking more deeply into this job she was being offered - particularly so, when she was then asked to start making payments.

I'm also persuaded, in the circumstances of this case, Miss I ought to have had her doubts and been concerned where the fraudsters told her they had received her application for the job, but she knew she hadn't applied. Because of this, I think it would be fair and reasonable to make a 50% reduction in the award based on contributory negligence in the circumstances of this case.

Recovering Miss I's money from the recipient accounts

I've also thought about whether Monzo could have done more to attempt to recover the payments after Miss I reported the fraud. However, as part of the scam, the funds were forwarded on to the fraudsters from the crypto exchanges to which they were sent. So 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 Miss I £11,705 (being 50% of £23,410 - the sum of the payments made from the £4,150 payment sent on 1 June 2023 onwards, less a credit of £40 received from payee 3)
- Pay 8% simple interest per year on this amount, calculated from the date of loss until the date of settlement, minus any applicable tax.

Monzo has provided evidence to show that Miss I held a balance of 613.92 USDT in her cryptocurrency account at the time the scam came to light. It is fair and reasonable that Monzo also deduct the sterling equivalent of this USDT amount from the £11,705 ahead of refunding Miss I.

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 Miss I to accept or reject my decision before 30 January 2025.

Stephen Wise
Ombudsman