DRN-4716729

The complaint

Mrs N 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 August 2023, Mrs N came across a job opportunity. She was told the job involved completing tasks, for which she would earn commission. Believing everything to be genuine Mrs N proceeded and, after completing some initial tasks, she was able to withdraw £116.70 to her account. But unknown to her at the time, she had been contacted by fraudsters. The fraudsters then persuaded Mrs N to pay her own money in order to proceed with the work.

Mrs N 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 Mrs N sent and received from her Monzo account as part of the scam;

21 August 2023	payee one	£30.00
22 August 2023	payee two	£91.00
22 August 2023	credit received	£116.70
23 August 2023	payee two	£481
23 August 2023	payee three	£1,360
23 August 2023	payee four	£902
23 August 2023	payee five	£3,263
23 August 2023	payee three	£1,310
31 August 2023	credit received	£30

Mrs N realised she'd been scammed when she was asked to pay increasingly larger sums and she was unable to withdraw her supposed earnings.

Mrs N raised a fraud claim with Monzo, but it didn't agree to reimburse her.
Unhappy with Monzo's response, Mrs N 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 Mrs N made the payment for £3,263 on 23 August 2023. It was our Investigator's view that had Monzo intervened, at this point, and warned Mrs N, it would have made a difference and she wouldn't have gone ahead with this payment, or the one that followed.

But our Investigator also thought Mrs N 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 Mrs N to have some concerns about the legitimacy of the job.

Through her representatives, Mrs N accepted our Investigator's view. But Monzo disagreed; in summary it didn't think it should be liable as the loss was not from Mrs N's Monzo account, but from Mrs N'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 Mrs N 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 Mrs N's account is that Mrs N 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 it's 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

[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."

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 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 Mrs N's payments?

To decide this, I've reviewed the activity on Mrs N'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 Mrs N may have been at risk of financial harm. The payments weren't so dissimilar in value to other payments that Mrs N 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 23 August 2023, Mrs N attempted to make a further payment for £3,263, 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 fourth payment on the same day, to a third new payee (on that day) 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 £3,263, Mrs N would have cumulatively paid over £5,000 within a short period of time on the same day, to multiple new payees.

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 Mrs N's account previously and on balance, I think the payments were becoming out of character compared to the typical sort of spending associated with Mrs N'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 Mrs N 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 Mrs N 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 Mrs N from proceeding. There's no evidence to suggest she wouldn't have been honest with Monzo or wouldn't have heeded its warnings. And I don't think it would have taken much for Monzo, as professional's in these matters, to persuade Mrs N that she was falling victim to a scam.

It is the case that, from the point of this payment for £3,263, Mrs N'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 Mrs N'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 all things considered, I'm persuaded it is fair and reasonable that Monzo, at least in part, bears some responsibility for Mrs N's loss.

Did Mrs N act reasonably in the circumstances?

I've also thought about whether Mrs N 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 Mrs N, and so should have led to her to looking more deeply into this job she was being offered - especially so, when she was then asked to start making payments. Because of this, I think it would be fair and reasonable to make a 50% reduction in the award based on contributary negligence in the circumstances of this case.

Recovering Mrs N's money from the recipient accounts

I've also thought about whether Monzo could have done more to attempt to recover the payments after Mrs N 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 Mrs N £2,271.50 (being 50% of the sum of the final two payments, less the £30 credit received on 31 August 2023).

- Pay 8% simple interest per year on this amount, calculated from the date of loss until the date of settlement, minus any applicable tax.

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 Mrs N to accept or reject my decision before 16 January 2025.

Stephen Wise
Ombudsman