DRN-4722223

The complaint

Ms A complains that Monzo Bank Ltd hasn't refunded her after she fell victim to a scam.

What happened

The background to this complaint is well known to all parties and so I'll not go into extensive detail here.

Ms A was looking for employment opportunities. She was contacted on WhatsApp by someone claiming to work for a marketing company. This was in fact a scammer, though Ms A didn't realise at the time.

The scammer said Ms A could work for their marketing company, with the job involving submitting reviews online for different products. This is what has generally come to be known as a job or task scam. The premise was that Ms A would receive commission for the reviews, likes, and associated tasks that she performed.

Ms A was told she'd need to fund a cryptocurrency account with an initial deposit so that she could gain access to the tasks and to be paid her commission. Convinced all was above board Ms A set up cryptocurrency accounts at the scammer's instruction. She went on to fund these from her Monzo account.

Over the course of two days there were six small payments (all under £50) sent to a crypto wallet, all of which were returned to Ms A's Monzo account. Two days later she started to make payments to a different wallet. But this time the payments were for a much higher amount. She sent the following payments, the first to one wallet, the other three to a separate one:

- £843 on 15 September 2023
- £1,796.58 on 16 September 2023
- £3,169.14 on 16 September 2023
- £2,332.53 on 16 September 2023

Ms A then sent this money onto the scammer, believing she was funding a different account linked to her new job. She'd made each payment as she was being told her account balance was depleting and needed topping up in order to retain access to new tasks and so that she could be paid.

Ms A realised something was wrong when the scammer kept asking for money and she found she had no access to her supposed earnings. She reported what happened to Monzo and it said it wouldn't refund her loss.

Ms A brought her complaint to our service where one of our investigators recommended it be upheld. He said that Monzo ought to have identified that Ms A was at risk of financial harm

through fraud given the nature and frequency of payments being made. He said there was an identifiable and actionable risk at the point Ms A made the payment of £3,169.14 on 16 September 2023.

He felt the scam could have been avoided if Monzo had asked appropriate questions and given appropriate warnings. And so he recommended Monzo refund 50% of Ms A's loss from that point, minus a payment of £133.32 which Ms A received back from the scammer.

The refund was reduced to 50% because he also took account of Ms A's actions and considered whether they were reasonable in the circumstances. He said there were features of the scam that ought to have caused Ms A to question what she was doing and to reconsider whether it was a legitimate job.

Ms A accepted the outcome, but Monzo didn't. It maintained the same position and said it shouldn't be responsible for Ms A's losses. Its objections can be summarised as:

- The payments weren't particularly unusual and didn't present as an identifiable scam risk and so there was no valid argument that it ought to have intervened;

- The loss didn't occur on the Monzo account. Instead, Ms A's losses occurred when she sent the money on from the crypto wallets which were in her name and which she was in control of.

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.

I'm upholding the complaint and for broadly the same reasons as our investigator.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Ms A's account is that she is responsible for payments she authorised herself. And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, 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 terms and conditions gave it rights (but not obligations) to block payments if it suspected criminal activity on a customer's account or if it were protecting them from fraud. The terms and conditions explain if Monzo 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.

Whilst the current account terms may 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

[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)

[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."

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 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 this payment), 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 Ms A's payments?

I'm satisfied the transactions being made by Ms A had become sufficiently unusual, and presented an identifiable scam risk, by the time the £3,169.14 payment on 16 September 2023 was instructed.

Many of the preceding transactions had been low value. But, by the time the highlighted

payment was made, the spending had quickly ramped up. This payment instruction represented an escalation to over £5,000 of spending in just two days. It was also being sent to the third new crypto wallet provider within a few days.

Monzo has contended that this is normal behaviour for an average person engaged in crypto trading. But I'm not persuaded that is the case. Or, at the very least, I'm satisfied it is also very much reflective of the behaviour of someone caught up in a cryptocurrency connected scam and, more specifically, a job/task scam.

It then follows that Monzo ought fairly and reasonably have identified this risk and questioned Ms A about what was going on. This is in line with the relevant considerations I've set out above and it's important to take careful note of the requirements of the Consumer Duty, referenced in the footnote of page 3 of this final decision.

The Consumer Duty Finalised Guidance FG 22/5, published by the FCA, gives an example of a bank's obligation to avoid foreseeable harm to customers. It states, as an example of foreseeable harm:

"*consumers becoming victim to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.*"

As it stands, I've seen no evidence of any suitable warnings provided to Ms A. And it is clear that Monzo didn't stop any payments to question them, which I find would have been the proportionate, fair and reasonable action to take in the circumstances of this case.

The intervention from Monzo ought to have involved dynamic questioning to help identify the type of scam she was falling victim to. By September 2023 Monzo ought fairly and reasonably 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 the proper flow of dynamic questioning, I'm persuaded it's more likely than not Ms A 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 Ms A from proceeding. There's no evidence to suggest she wouldn't have been honest with Monzo or wouldn't have heeded its warnings.

It is the case that Ms A'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. And so it is fair and reasonable it bears responsibility for her loss.

Did Ms A act reasonably in the circumstances?

Our investigator recommended Ms A's refund be set at 50% of her losses from the £3,169.14 payment onward. The refund was recommended at that level having taken account of Ms A's own actions, finding that she ought to have recognised all was not as it seemed.

Ms A has accepted this position and Monzo doesn't disagree with it either. And so there is no further dispute to address here. I'll only confirm that I also agree this is the correct finding.

Putting things right

If Ms A accepts this decision Monzo should:

- Refund 50% of Ms A's loss from and including the payment of £3,169.14 on 16 September 2023, minus the £133.32 she received back from the scammer.

- Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

My final decision

I uphold this complaint against Monzo Bank Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 27 June 2024.

Ben Murray
Ombudsman