DRN-4582939

The complaint

Mrs C is unhappy 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

I issued my provisional decision on this complaint on 10 January 2024. The background and circumstances of the case and the reasons why I was minded to uphold the complaint in part were set out in that decision. I have reproduced the provisional decision in italics below:

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.

Mrs C fell victim to a task-based employment scam in November 2022. She was contacted through a social media messaging platform by someone pretending to be from a well-known employment agency. Mrs C responded to the message and was then contacted by an individual, claiming to be working for a marketing consultancy company. But unknown to her at the time she was dealing with fraudsters.

Mrs C has said she'd previously loaded her CV onto a library and thought the contact was as the result of that. Due to health issues and the need to look after her children, Mrs C had been looking for a remote role, which would enable her to work from home. The fraudster explained to Mrs C what the role entailed and offered her a job, that would enable her to work remotely. The role involved completing online tasks that would generate star ratings for various products.

The fraudster told Mrs C that she would be paid in cryptocurrency for completing these tasks online and she would receive commission and a weekly salary. Mrs C has said she researched the company the fraudster claimed to be from and could see it was registered on Companies House and had a social media presence.

Believing everything to be genuine, Mrs C agreed to proceed. Shortly after she was told that she needed to set up a wallet with a cryptocurrency platform and that the fraudster was willing to teach her how to use it. She went through some training and set up a cryptocurrency account with a legitimate platform at the scammer's instruction. She was shown how to purchase cryptocurrency using the peer to peer ("P2P") network, as she was told this was a better way to buy it.

Mrs C was initially told that she needed to deposit small amounts, via the P2P process in order to complete tasks. She's said at one point she did receive a small amount back into her cryptocurrency wallet, but this was then paid back to the fraudsters. But the purchases Mrs C was having to make as part of her job became increasingly expensive and she continued to purchase cryptocurrency, through P2P, which she then went on to transfer to the fraudster from her cryptocurrency wallet. She was under the impression that she was topping up the balance in her 'work wallet', but the payments were in fact going to wallets the fraudsters controlled.

Eventually Mrs C told the scammer that she wasn't able to afford any more top up payments, at which point the fraudsters told her there would be further consequences if she didn't pay.

In total Mrs M made 24 payments from her Monzo account, totalling £51,320, which were made up of several international payments and the remainder being faster payments towards P2P purchases of cryptocurrency. Mrs C has told us she funded these payments through transfers into her Monzo account from an account her husband held. A breakdown of these payments is listed below;

19/11/2022	*£60*	*Faster Payment (through P2P network)*
21/11/2022	*£70*	*Faster Payment (through P2P network)*
21/11/2022	*£120*	*International Payment*
23/11/2022	*£40*	*Faster Payment (through P2P network)*
23/11/2022	*£470*	*Faster Payment (through P2P network)*
23/11/2022	*£1,800*	*International Payment*
23/11/2022	*£4,500*	*Faster Payment (through P2P network)*
24/11/2022	*£5,000*	*Faster Payment (through P2P network)*
24/11/2022	*£1,000*	*International Payment*
24/11/2022	*£2,000*	*Faster Payment (through P2P network)*
25/11/2022	*£5,000*	*Faster Payment (through P2P network)*
25/11/2022	*£2,800*	*International Payment*
25/11/2022	*£2,000*	*Faster Payment (through P2P network)*
26/11/2022	*£3,000*	*International Payment*
26/11/2022	*£2,700*	*International Payment*
26/11/2022	*£3,100*	*Faster Payment (through P2P network)*
26/11/2022	*£2,000*	*Faster Payment (through P2P network)*
26/11/2022	*£2,000*	*International Payment*
26/11/2022	*£300*	*Faster Payment (through P2P network)*
27/11/2022	*£4,182*	*Faster Payment (through P2P network)*
27/11/2022	*£2,778*	*Faster Payment (through P2P network)*
27/11/2022	*£2,000*	*Faster Payment (through P2P network)*
27/11/2022	*£1,000*	*Faster Payment (through P2P network)*
27/11/2022	*£3,400*	*Faster Payment (through P2P network)*

Mrs C raised the matter with Monzo. It has committed to follow the Lending Standards Board Contingent Reimbursement Model (CRM) Code (although it isn't a signatory) which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams like this in all but a limited number of circumstances. Monzo looked into Mrs C's complaint and concluded it had no responsibility to refund her loss. In summary this was because it didn't think Mrs C had carried out any due diligence for a deal that it considered too good to be true. It added that International payments weren't covered by the CRM code and that it had no control over the onward transfer of cryptocurrency from Mrs C's cryptocurrency account. So overall, it didn't consider it could be held liable for the payments.

Monzo added that it had provided warnings to Mrs C. This included freezing Mrs C's account, at the time she made her final payment (for £3,400). It contacted her via its online chat functions and asked Mrs C some questions about the payment. Mrs C told Monzo the transaction was for family and friends and the payment was then allowed to be progressed. Monzo also tried to recover Mrs C's money from the beneficiary bank (the bank to which the money was sent), but unfortunately no funds remained.

Unhappy with Monzo's response, Mrs C brought her complaint to this service. One of our Investigator's looked into things, but didn't think the complaint should be upheld. In summary our Investigator didn't consider the payments made would be covered by the CRM code. Our Investigator did however think that Monzo ought to have intervened at the time Mrs C

attempted to make her payment for £5,000, on 24 November 2022. As he thought this payment would have appeared unusual when compared to her typical activity.

However, it was our Investigator's view that even if Monzo had questioned Mrs C about this payment, it didn't think it would have changed the outcome. He thought this because when Monzo had asked Mrs C about her final payment, she had told it that it was for family and friends. It was unclear to our Investigator why Mrs C had told the bank this, when she thought this was a legitimate job opportunity. But in any event, he considered if the bank had questioned her further she would have been able to tell it that she had successfully purchased cryptocurrency, which he considers would have reassured Monzo.

Mrs C didn't agree with our Investigators view. As agreement couldn't be reached the complaint has been passed to me for a final decision.

What I've provisionally 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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

To begin with, Monzo has a primary obligation to carry out the payment instructions its customers give it. As a starting point, a customer will therefore be assumed to be liable for payments they have instructed to be made. There is no dispute that Mrs C authorised these payments, albeit having been deceived into believing she was sending them for the purpose of a job opportunity. On the face of it, she is therefore liable for the resultant losses.

The CRM Code can provide additional protection for the victims of APP scams such as this was. However, international payments are not within the scope of the CRM Code and nor would the other payments Mrs C made be, as ultimately she has made the transactions to fraudsters from a cryptocurrency wallet she held, which isn't a faster payment between GBP accounts, which is a requirement of the code. So I cannot fairly apply the terms of the CRM code to any of the payments Mrs C has made.

However, there are circumstances where it might be appropriate for Monzo to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud. I've therefore considered whether the instructions given by Mrs C (either individually or collectively) were unusual enough to have expected additional checks to have been carried out before the payments were processed.

To decide this, I've reviewed the activity on Mrs C'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 six 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 C may have been at risk of financial harm. The payments weren't dissimilar in value to other payments that Mrs C had made previously and I don't think they ought to have stood out.

However, I'm minded to say that a pattern has started to emerge and at the point, on 23 November 2022, when Mrs C is attempting to make a payment of £4,500, Monzo ought to

have had some concerns and made further enquiries before allowing it to be processed. I say this because, by that point, it was the sixth new payee within the space of just a few days, in a series of payments that were increasingly escalating in value. Monzo will be aware that multiple escalating payments being made in quick succession can often be indicative of financial harm.

Alongside this the sequence included payments to international accounts and the amounts being sent were also becoming out of character for the typical sort of spending associated with Mrs C's account. By the time she was making the payment of £4,500, she would have cumulatively paid nearly £8,000, within just a few days to several new payees and to international accounts. However, Mrs C's account statements show that she rarely makes payments for anything over and above £1,000, and when she has done, it appears to have been transfers between her and her husband's account.

It follows that I think Monzo should've spoken with Mrs C, about the payment for £4,500, before processing it. Had Monzo done so and asked proportionate questions, I've no reason to think Mrs C wouldn't have been candid about the detail behind the payments – that being for a job involving completing tasks, in which she would get paid in crypto, and that she had to make payments to increase her wallet balance.

Given Monzo's familiarity of scams, including those involving completing tasks such as this, I think this would've been a red flag. And so, at this point, I think Monzo ought to have highlighted to Mrs C that there was a significant risk of it being a scam and encouraged her to not make any further payments. I've no reason to doubt that Mrs C wouldn't have acted on such advice. I think it's reasonable to assume, that had she been given a clear warning that it was very likely she was being scammed, Mrs C would've most likely not proceeded with making the £4,500 payment to the scammers, nor the subsequent payments she made. I therefore think Monzo's lack of intervention led to Mrs C suffering the loss from this point.

In saying that, I'm very mindful that when Monzo asked Mrs C, through its chat function, who the payment was to (when it froze her account at the point of her making the final payment for £3,400), she answered the transaction was for 'friends and family'. However, I'm not persuaded its more likely than not Mrs C answered in this way, in order to mislead the bank in anyway. Monzo didn't provide Mrs C sufficient context at the time of asking, that I think would have enabled her to reasonably understand the importance of her providing accurate and specific answers to what it was asking. It simply told Mrs C "we know this is a pain, as a regulated bank we have to run checks on accounts from time to time". In the absence of any such context or follow up questions and without any mention at all about the risks surrounding fraud and scams, it's understandable the gravity of the question she was being asked didn't resonate with Mrs C at the time.

Overall, for reasons already explained, I'm minded to say that there was enough going on earlier in the scam, for Monzo's intervention to fairly and reasonably have gone further than it did. So I'm persuaded that it was, at least in part, responsible for some of Mrs C's loss.

I've also thought about whether Mrs C did enough to protect herself from the scam, and I don't think she did. While I understand Mrs C was trusting of the fraudster, I think it would've been reasonable for her to have had concerns about the legitimacy of the job offered. This is because I consider the concept of running tasks to drive ratings for products or services she hadn't used or purchased, being paid in crypto and having to deposit funds in order to acquire earnings doesn't seem genuine, and so should've prompted concerns.

I've considered that Mrs C has said she did receive a small return into her wallet. But I don't think a legitimate company would require somebody to make any upfront payments, but

Mrs C has proceeded to pay money over anyway without completing sufficient independent checks, and I don't think that was reasonable.

I'm also mindful of the fact Mrs C had to initially make payments to accounts that were not in the name of the company she believed she was working with. I don't think the explanation given around having to purchase cryptocurrency through a third-party network rings true of how a legitimate company would typically run. Alongside this, I think Mrs C ought reasonably to have had concerns about the strong additional income she was being offered to complete basic tasks. I think the level of income, seemed improbable to the point of being too good to be true.

I'm mindful that any of these individual factors in isolation may not have been enough to have prevented Mrs C from proceeding. But considering the specific circumstances of this case and the factors in the round, on balance, I think that there was enough going on and sufficient red flags that Mrs C ought reasonably to have taken further steps to protect herself. So, I think it would be fair and reasonable to make a 50% reduction in the award I'm intending to make, based on contributory negligence in the circumstances of this complaint.

Finally, I've considered whether Monzo did all it could to try and recover the money Mrs C lost, once she had reported the scam to it. From the evidence I've seen, Monzo did contact the receiving bank when the matter was raised, but unfortunately the receiving bank reported that no funds remained. So, I think Monzo has done what it could reasonably have been expected to and I don't think it has missed an opportunity to recover the money Mrs C has sadly lost.

Putting things right

For the reasons I've explained, I'm minded to uphold this complaint in part and to ask Monzo Bank Ltd to;

- *Refund Mrs C 50% of the money she lost from the point she made the payment for £4,500 on 23 November 2022 – being £24,380 (being 50% of £48,760), from the date of the payments to the date of settlement.*

In my provisional decision I asked both parties to send me any further evidence or arguments that they wanted me to consider by 25 January 2024.

Mrs C responded and accepted my provisional decision and had nothing further to add.

Monzo confirmed it had received my provisional decision but didn't agree with it. In summary, it said it wasn't obliged to make fraud checks, although it was something that it routinely did. Monzo referred to the approach outlined by the Supreme Court in the case of *Phillip v Barclays.* It added for this case specifically interrupting the payment journey would have been inappropriate as there was no suspicions that fraud was occurring.

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.

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 for Monzo, 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 C's account is that Mrs C is responsible for payments she authorised. And, as the Supreme Court has recently 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 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 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.

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

---

[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."

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 C's payments?

Bearing all of this in mind and as I've already set out in my provisional decision. I think Monzo should've spoken with Mrs C, at the point she was making the payment for £4,500 on 23 November 2022, before it processed it. My position remains that had Monzo done so, as I think it ought to have done, and asked proportionate questions, I've no reason to think Mrs C wouldn't have been candid about the detail behind the payments – that being for a job involving completing tasks, in which she would get paid in crypto, and that she had to make payments to increase her wallet balance.

Monzo ought to have highlighted to Mrs C that there was a significant risk of it being a scam. I've no reason to doubt that Mrs C wouldn't have acted on such advice. I think it's reasonable to assume, that had she been given a clear warning that it was very likely she was being scammed, Mrs C would've most likely not proceeded with making the £4,500 payment to the scammers, nor the subsequent payments she made. I therefore think Monzo's lack of intervention led to Mrs C suffering the loss from this point.

With all of this in mind, I see no reason to depart from the findings within my provisional decision. Overall, for the reasons set out here and in my provisional decision, I remain of the view that this complaint should be upheld in part.

Putting things right

To put matters right Monzo Bank Ltd should now;

- Refund Mrs C 50% of the money she lost from the point she made the payment for £4,500 on 23 November 2022 – being £24,380 (being 50% of £48,760), from the date of the payments to the date of settlement.

My final decision

My final decision is that I uphold this complaint in part and require Monzo Bank Ltd to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 23 February 2024.

Stephen Wise
Ombudsman