DRN-4469976

The complaint

Miss P complains that Monzo Bank Ltd (Monzo) is refusing to refund her the amount she lost as the result of a scam.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Miss P came across a trader (X) on Snapchat who appeared to be endorsed by a known public figure. Miss P could see information on the account showing other people had successfully invested, as well as recommendations from other influencers.

X discussed the investment with Miss P. Miss P then setup an account with the legitimate cryptocurrency exchange Crypto.com where she purchased cryptocurrency that she transferred to X with the belief that X would be trading the funds on her behalf.

Miss P made a relatively small initial investment of around £500 which appeared to have grown substantially to around £10,000. However, Miss P was advised she had to make further payments to withdraw the funds, which she did.

Having made the payments as requested by X, X stopped communicating with Miss P and blocked her from Snapchat.

Miss P was then contacted by a second individual who claimed to be able to recover the funds she had lost but Miss P didn't receive any money back.

Miss P made the following payments in relation to the scam:

Date	Payee	Payment Method	Amount
24 December 2022	CRO INTERNET MLT	Debit Card	£0.10
24 December 2022	CRO INTERNET MLT	Debit Card	£514.85
25 December 2022	CRO INTERNET MLT	Debit Card	£1,029.90
26 December 2022	Crypto.com	Debit Card	£257.48
26 December 2022	CRO INTERNET MLT	Debit Card	£2,317.28
29 December 2022	CRO INTERNET MLT	Debit Card	£956.32
30 December 2022	CRO INTERNET MLT	Debit Card	£1,242.06
1 January 2023	CRO INTERNET MLT	Credit	- £0.10

Our Investigator considered Miss P's complaint and thought it should be upheld in part. Miss P agreed but Monzo didn't, so this complaint has been passed to me to decide.

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 has not been disputed that Miss P has fallen victim to a cruel scam. The evidence provided by both Miss P and Monzo sets out what happened. What is in dispute is whether Metro Bank should refund the money Miss P lost due to the scam.

Recovering the payments Miss P made

Miss P made payments into the scam via her debit card. When payments are made by card the only recovery option Monzo has is to request a chargeback.

The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The card scheme operator ultimately helps settle disputes that can't be resolved between the merchant and the cardholder.

Such arbitration is subject to the rules of the scheme, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be considered valid, and potentially succeed. Time limits also apply.

Miss P was dealing with X, which was the individual that instigated the scam. But Miss P didn't make the debit card payments to X directly, she paid a separate cryptocurrency exchange (Crypto.com). This is important because Monzo would only have been able to process chargeback claims against the merchant she paid (Crypto.com), not another party (such as X).

The service provided by Crypto.com would have been to convert or facilitate conversion of Miss P's payments into cryptocurrency. Therefore, Crypto.com provided the service that was requested; that being the purchase of the cryptocurrency.

The fact that the cryptocurrency was later transferred elsewhere – to the scammer – doesn't give rise to a valid chargeback claim against the merchant Miss P paid.

Should Monzo have reasonably prevented the payments Miss P made?

It has been accepted that Miss P authorised the payments that were made from her account with Monzo, albeit on X's instruction. So, the starting point here is that Miss B is responsible.

However, banks and other Payment Services Providers (PSPs) do have a duty to protect against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering.

The question here is whether Monzo should have been aware of the scam and stepped into question Miss P about the payments she was making. And if it had questioned Miss P would it have been able to prevent the scam taking place.

In the six months leading up to the scam Miss P didn't use her account very much and the payments she did make from the account in this time did not individually exceed £200. By the time Miss P made the fifth payment in relation to the scam she had made five payments over just three days to a known cryptocurrency exchange. The value of the fifth payment was also for £2,317.28 which was significantly higher than her usual spend. With this in mind I think it would be reasonable to expect Monzo to step in when Miss P made this payment and question her about it.

I'm unable to see that Miss P was coached on what to say to the bank by X if it intervened, so I think had Monzo asked Miss P some simple questions about what the payment was for

it's likely Miss P would have explained the reason for the payment and how it came about. I think based on the circumstances of the scam, Monzo with its vast experience in crypto scams would have uncovered the scam and prevented Miss P from incurring any further loss.

Monzo is therefore responsible for the amount Miss P lost in relation to the scam from the fifth payment onwards.

Did Miss P contribute to her loss?

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances, I do think it would be fair to reduce compensation by 50% on the basis that Miss P should share blame for what happened. Miss P confirmed no contracts were signed in relation to the investment and everything was conducted over social media. I think this should have caused Miss P concern and she should have carried out more research before making payments in relation to the scam, and the withdrawal of funds from it.

In addition to the points covered above Monzo has said that it is required to carry out its customers payment instructions promptly and that it therefore wouldn't be able to decline a valid payment instruction.

I have, seen a copy of Monzo's terms and conditions applicable to current accounts dated 6 December 2021. Given the point at which I think Monzo should've intervened was 26 December 2022, I will be proceeding on the basis that these were the terms applicable to Miss P's account at the time.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Miss P's account is that she is responsible for payments she's 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 December 2021 terms and conditions gave it rights (but not obligations) to:

- Block payments where it suspects criminal activity on the account. It explains that if it blocks a payment, it will let its customer know as soon as possible, using one of its 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).

[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."

- 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.

I've already set out the reasons why I consider Monzo should have stepped in before processing the fifth payment made in relation to the scam, as well as why I consider such an intervention would have likely prevented any further loss. Monzo hasn't provided any evidence that would alter my conclusions in this regard,

Putting things right

To put things right I require Monzo Bank Ltd to:

- Refund the payments Miss P lost to the scam from the fifth payment she made in relation to the scam for the value of £2,317.28, less a deduction of 50%.
- Pay 8% simple interest per year on this amount from the date of loss until the date of settlement.

My final decision

I uphold this complaint and require Monzo Bank Ltd to put things right by doing what I've explained above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss P to accept

or reject my decision before 12 April 2024.

Terry Woodham
Ombudsman