DRN-4563421

The complaint

Mr M complains that Monzo Bank Ltd didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr M was the victim of an investment scam. He met someone on social media who I'll refer to as "the scammer". The scammer claimed to work for a company I'll refer to as "R" and told him he could make money by investing in cryptocurrency. They asked him to first purchase cryptocurrency through a cryptocurrency exchange company I'll refer to as "M" and then load it onto an online wallet. Between 20 April 2023 and 25 April 2023, he made fifteen payments to M totalling £13,419 using a debit card connected to his Monzo account.

Mr M contacted Monzo on 26 April 2023 when he realised he'd been scammed, but it refused to refund the money he'd lost. It said the payments were authorised and the loss happened as a result of the onwards payment from M. And there were no chargeback rights because once the money had reached M, the service was considered provided, so it didn't have any grounds to dispute the payment.

It accepted there had been delays in the time it took to provide a response to the scam claim, offering £125 compensation as an apology and for the distress and inconvenience he'd suffered as a result of its failings.

Mr M wasn't satisfied and so he complained to this service. Our investigator felt the complaint should be upheld. She explained Mr M's account was used for low value transactions, except for one transaction for £404.50 on 24 November 2022, so she didn't think the first four payments were unusual. But she thought Monzo should have intervened when Mr M paid £1,800 to M on 22 April 2023 because he had been making significant payments to M for three consecutive days and it was still a new payee. She explained that from January 2023, we would expect Monzo to recognise cryptocurrency transactions carry an elevated risk of fraud or a scam, so it should have intervened.

Had it intervened and questioned Mr M about the payments, our investigator was satisfied he hadn't been coached to lie, so he would have explained he'd found the investment on social media and that there was a third party involved. She said that even though there were no reviews about R, it was based overseas with a UK address for a food court, so if Monzo had provided a meaningful scam warning, he might have realised he was being scammed. Because of this she thought it should refund the money he'd lost from the fifth payment onwards.

However, she explained that Mr M should bear some responsibility for his loss because even though this was a sophisticated scam, there were clear red flags including the suspicious company address, R wasn't regulated by the Financial Conduct Authority ("FCA"), and the

returns were unrealistic.

Finally, she accepted there had been failings in Monzo's handling of the claim but she was satisfied that £125 compensation was fair and reasonable in the circumstances.

Monzo asked for the complaint to be reviewed by an Ombudsman stating the payments were "me-to-me" payments, so no material loss occurred as a result of the payments from Monzo. Instead, the loss occurred when Mr M sent funds from the cryptocurrency wallet. It argued that the upcoming changes to the Payment Services Regulations 2017 ('the Regulations'), and the rules around APP mean banks are not expected to assess fraud that doesn't happen within their remit and it isn't responsible for the onward loss of cryptocurrency when purchased legitimately.

It explained that the payments weren't suspicious or unusual as Mr M was paying a legitimate cryptocurrency merchant and the fact he made a larger than usual payment didn't mean it should have intervened. It argued that in Phillip v Barclays, the regulator and the court have upheld that they expect banks to carry out customers wishes and it's inappropriate for it to decline to do so.

It also argued that there is no evidence that an intervention from Monzo would have prevented Mr M's loss as he ignored warnings from M which were available on its app and website and there's nothing to suggest he wouldn't have ignored similar warnings from Monzo.

My provisional findings

I thought about whether Monzo could have done more to recover Mr M's payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Monzo) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr M).

Mr M's own testimony supported that he used cryptocurrency exchanges to facilitate the transfers to M. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr M's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that Monzo's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

There was no dispute that this was a scam, but although Mr M didn't intend his money to go to scammers, he did authorise the disputed payments. Monzo is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

I explained the starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr M's account is that he is responsible for payments he's authorised himself. 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 if it suspects criminal activity on a customer's account. 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 was 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).

• 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”.

• 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 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 circumstance (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.

Prevention

I thought about whether Monzo could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I’d seen, the payments were made to a genuine cryptocurrency exchange company. However, these payments were part of a wider scam, so I needed to consider whether it ought to have

intervened to warn Mr M when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Monzo to intervene with a view to protecting him from financial harm due to fraud.

The payments didn't flag as suspicious on Monzo's systems. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr M normally ran his account and I thought they were. This is because, even though he was paying a legitimate cryptocurrency exchange, in the months before the start of the scam, the largest payment was for £404.50 on 4 November 2022, so the amounts he was paying to M were unusual. The first 6 payments were relatively low value and I didn't agree with our investigator that Monzo needed to intervene when Mr M paid £1,800 to M on 22 April 2023 because I didn't think it was high enough to have raised concerns. But by the time he made the third payment that day of £3,550, the cumulative total for the day was £5,420, and he had made seven payments to the same high risk cryptocurrency merchant over three consecutive days. I was satisfied this was a pattern of spending which should have raise concerns, so I thought Monzo should have intervened.

Monzo ought to have contacted Mr M either by phone or its live chat facility and asked him why he was making the payment, whether there was a third party involved and if so how he met them, whether he'd been told to download remote access software to his device, whether he'd made any withdrawals and what he'd been promised in terms of returns. And had it done so, there's no evidence he'd been coached to lie and so I thought he'd have said he was being assisted by a broker who worked for R and that he'd found the opportunity online. He'd have also told it he'd been told to make on onwards payment from M and that he'd been told he could make £30,000 profit on his investment.

With this information, I was satisfied Monzo would have had enough information to identify that Mr M was being scammed and so have provided a tailored scam warning, providing some detailed information about how cryptocurrency scams work. There were no warnings about R on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites which would have alerted Mr M to the fact there was a scam. But I hadn't seen any evidence that Mr M was keen to take risks and I thought it was likely he'd have listened to a robust scam warning from Monzo and advice on how to check the investment was genuine and decided not to go ahead with the payments. Because of this I was minded to direct Monzo to refund the money Mr M lost from the seventh payment onwards.

Contributory negligence

Our investigator had said that the settlement should be reduced by 50% for contributory negligence and I agreed that there were some red flags that Mr M missed when he decided to go ahead with the investment. These red flags included the suspicious company address, the fact R wasn't regulated by the FCA and the very high rate of return. But, Mr M had explained that he'd never invested before and so he wouldn't have known about the importance of checking the FCA register. And in recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I didn't think it was unreasonable for Mr M to have believed what he was told by the scammer in terms of the returns he was told were possible.

I accepted he might have been alerted to the fact the investment was a scam if he'd noticed the anomaly with the company address, but I didn't think he should be penalised for not having noticed this detail. And having considered the circumstances of this scam, I was satisfied it was sophisticated and I didn't think it was unreasonable for Mr M to have thought it was genuine. Consequently, whilst there may be cases where a reduction for contributory negligence is appropriate, I didn't think this was one of them.

Compensation

Mr M was told he would by informed of the outcome of his complaint by 2 June 2023, but he didn't receive the final response letter until 18 July 2023. Monzo offered Mr M £125 compensation for this and I was satisfied this fairly reflected the impact of its failings and that it was fair and reasonable.

Developments

Mr M has indicated that he accepts the findings in my provisional decision. But Monzo has argued that the payments went to an account in Mr M's own name with a legitimate cryptocurrency platform and that this wouldn't have raised concerns, so it wouldn't have contacted him via chat or a call. It has also argued that the conclusion that an intervention would have resulted in a different outcome is speculation.

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've considered the additional comments that Monzo has raised, but the findings in my final decision will remain the same as the findings in my provisional decision.

Monzo has stated that the payments weren't concerning because Mr M was paying an account in his own name with a legitimate cryptocurrency platform. But as I've previously stated, by the time he made the third payment on 22 April 2023, the cumulative total for the day was £5,420, and he'd made seven payments to the same high risk cryptocurrency merchant over three consecutive days. So, even though Mr M was paying an account in his own name with a legitimate cryptocurrency platform, I remain satisfied that this was a pattern of spending which should have raised concerns and that Monzo should have intervened.

Monzo has also suggested that my conclusion that an intervention would have resulted in a different outcome is based on speculation. I accept we don't know for sure what would have happened because Monzo didn't actually intervene, but in circumstances where we think a bank or EMI missed an opportunity to intervene, we need to consider what is most likely to have happened had they done so. In this case there were no warnings about R on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites which would have alerted Mr M to the fact there was a scam. But as I haven't seen any evidence that he was keen to take risks, I think it's likely he'd have listened to a robust scam warning from Monzo and advice on how to check the investment was genuine and ultimately decided not to go ahead with the payments. Consequently, I remain satisfied that Monzo's failure to intervene represented a missed opportunity to have prevented Mr M's loss and so it should refund the money he lost from the seventh payment onwards.

My final decision

My final decision is that Monzo Bank Ltd should:

- refund the money Mr M lost from the seventh payment onwards, less any credits received during the scam period.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Monzo Bank Ltd deducts tax in relation to the interest element of this award it should provide Mr M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 2 April 2024.

Carolyn Bonnell
Ombudsman