DRN-4999488

The complaint

Mr S 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.

In October 2023, Mr S saw on social media that a friend of his had made money by investing in cryptocurrency. From there, he approached someone I'll refer to as "the scammer", who claimed to work for an investment company which I'll refer to as "R". The scammer seemed professional and knowledgeable and explained that Mr S would be given an online trading account and that he would be his account manager. He said Mr S would get a week of free trading on the platform, and that he would take 10% of his profits as commission.

Mr S checked the Financial Conduct Authority ("FCA") website to see if there were any warnings or red flags about R. He was reassured by his friend's social media posts, which included screenshots of his investments and how well he was doing, and there was no negative information about R online.

Mr S made an initial payment and was given log in details for an account on the trading platform, which showed the fluctuating exchange rates of various currencies, profits, losses, etc. The scammer asked him to first purchase cryptocurrency through cryptocurrency exchange companies, and then load it onto an online wallet. Mr S moved funds to his NatWest account from an account he held with an EMI I'll refer to as "W", and between 13 October 2023 and 13 November 2023, he made twenty payments to the scam totalling £22,843 (nineteen faster payments and one debit card payment).

Mr S remained in contact with the scammer via WhatsApp and monitored his investment on the trading platform. On 22 October 2023, he decided he wanted to make a withdrawal and was told he'd have to transfer funds into the account to demonstrate activity, so between 22 October 2023 and 30 October 2023, he processed four additional payments totalling £2,820. He was then told his funds had been stolen and he needed to pay a further £5,000, so between 1 November 2023 and 3 November 2023, he made three further payments.

Mr S realised he'd been scammed when he still didn't receive any money, he learned his friend's social media account had been hacked, and he found negative reviews online about R. He complained to this service with the assistance of a representative arguing that Monzo didn't provide effective warnings before he made the payments, and it should have intervened because he was making high-value payments to a new payee with links to cryptocurrency. He said he made the payments from his Monzo account because he was having difficult using his Wise account, but he wasn't told what to say to Monzo and if it had contacted him, he'd have done more checks.

His representative said the account was mostly used for low value payments and Monzo should have stopped all payments over £1,000. Further, on 24 October 2023, Mr S received £1 ,000 into the account and within 24 hours, he transferred £1 ,000 and £500 to the scam, which should have been cause for concern. They said he was making high value payments to new payees and the increased activity on the account should have been concerning.

Specifically, the representative said Monzo should have intervened on 13 October 2023 when Mr S paid £1,300 to the scam. They said it should have asked Mr S why he was making the payment, where the money was going after the cryptocurrency exchanges, whether he'd researched the investment company, whether he'd been predicted unrealistic returns, and whether he'd made any withdrawals, and had it done so it would have detected the scam.

Monzo said that no warnings were provided and even if it had intervened, based on the answers he gave when he took out a loan for £15,000, Mr S would've been dishonest, and it wouldn't have detected the scam. It said that as long as Mr S received the cryptocurrency into his digital wallet, there would be no reason not to execute the payment orders. It also said the payments weren't covered under the Contingent Reimbursement Model ("CRM") Code because he was paying an account in his own name, and it didn't have the right to intervene in line with the Phillip v Barclays, and its express current account terms.

Our investigator thought Monzo should have intervened on 21 October 2023 when Mr S made several payments totalling £12,850 to high-risk cryptocurrency merchants. He said it should have asked him how he came across the investment, whether there was a third party involved and if so whether the third party was regulated by the FCA, what returns he'd been promised, whether he was aware of the risks involved with cryptocurrency and using unregulated companies, and whether he understood that finding investment opportunities on social media isn't common practice for genuine investors.

He noted Monzo had said Mr S would have been dishonest, but he commented that the loan was taken out after the scam when he was taking steps to mitigate his financial situation, and he didn't think this meant he'd have been dishonest if had Monzo intervened. He noted that Mr S thought the investment was genuine, he hadn't found any adverse information about R, and there was no evidence that he'd been coached to lie, so he was satisfied he'd have disclosed how he came across R, the returns he expected to make and the fact he'd being asked to make an onwards payment from the cryptocurrency exchange, which would have been enough information for Monzo to detect the scam.

He explained that by 21 October 2023, Mr S was beginning to have concerns because he was having to pay to withdraw his profits, so it's likely he'd have weighed up the risks and done more checks, which would've shown the negative reviews claiming R was operating a scam. So, he recommended that Monzo should refund the money Mr S lost from 21 October 2023 onwards.

However, he thought the settlement should be reduced by 50% for contributory negligence because if he'd done some due diligence before making the payments, he'd have seen negative reviews about R which pre-dated the payments. Further, the WhatsApp messages with the scammer show was aware of the requirements of having an FCA certificate and had actually checked whether R was regulated, even though he was ultimately unconcerned that it wasn't.

Both parties asked for the complaint to be reviewed by an Ombudsman. Monzo argued that the payments were made to Mr S's own cryptocurrency wallet and no fraud occurred from his Monzo account, so the payments weren't covered under the CRM Code. It said there was no suspicion of fraud because all payments were legitimate, so it didn't have the right to

intervene in line with the Phillip v Barclays, and its express current account terms. And as long as Mr S received the cryptocurrency into his digital wallet, there would be no factual reason for refusing to execute the payment order.

Mr S's representative accepted he could have done more due diligence, but they suggested Monzo should have intervened on 13 October 2023, 19 October 2023, or 20 October 2023.

My provisional findings

I explained the Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. Monzo has said the CRM code didn't apply in this case because Mr S was paying accounts in his own name, and I was satisfied that's fair.

There's no dispute that this was a scam, but although Mr S 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.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr S'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 25 April 2023 terms and conditions gave it rights to block payments where it suspects criminal activity on the account.

So, the starting position at law is 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 fraud.
• It had a contractual right to delay payments to make enquiries where it suspected fraud.
• It could therefore refuse payments, or make enquiries, where it suspected fraud, but it was not under a contractual duty to do either of those things.

Whilst the current account terms did not oblige Monzo to make fraud checks, I didn't 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 was 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.

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 genuine cryptocurrency exchange companies. However, Monzo ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have intervened to warn Mr S 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 Mr S 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 S normally ran his account, and I thought they were. The first four payments were to legitimate cryptocurrency exchange companies, and they were for relatively low values, so there would have been no reason for Monzo to intervene. However, on 20 October 2023, Mr S made five payments in one day to the same high-risk cryptocurrency merchant and the cumulative total for the payments was £4,500, which was unusual for the account. Because of this, I thought Monzo ought to have presented a tailored written warning when Mr S made the ninth payment (which was the fifth payment that day).

I thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case and on the balance of probabilities, I thought it would have.

I explained I would expect a written warning to have covered off some of the key features of cryptocurrency-related investment scams, including the fact victims are usually targeted via social media or email, and fake online trading platforms can appear professional and legitimate. There were some key hallmarks of common cryptocurrency investment scams present in this case, such as Mr S having found the investment through social media, the involvement of a 'broker', and being asked to make an onwards payment from the cryptocurrency exchange, so I think the warning would have resonated with Mr S.

He hadn't yet been asked to make additional payments to access his investment, but I hadn't seen any evidence that he was asked, or agreed to, disregard any warnings, that he'd expressed mistrust of Monzo or financial firms in general, or that his relationship with the scammer was so close that Monzo would have found it difficult to counter through a warning.

I noted that Mr S did go on to lie in a loan application, but I didn't think this is indicative of how he'd have responded to a relevant and effective warning from Monzo in the early stages of the scam. And, I hadn't seen any evidence that he was given warnings by another bank.

Therefore, on the balance of probabilities, had Monzo provided Mr S with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from fraud, I said I believed he would have paused and looked more closely into R before proceeding. Had he done so he might have seen the negative reviews online or had a

conversation with his friend which might have alerted him to the fact his friend's social media account had been hacked, and the scam could've been uncovered.

Because I was satisfied that Monzo's failure to intervene represented a missed opportunity to prevent Mr S's loss, I was minded to direct that it should refund the money he lost from the ninth payment onwards (the fifth payment on 20 October 2023).

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence.

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 S to have believed what he was told by the scammer in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

He hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He wouldn't have known the returns were unrealistic or how to check the information he'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he trusted the scammer, he believed the trading platform was genuine, and he thought his friend had made money from the investment.

However, Mr S came across this opportunity on his friend's social media page and made the payments without ever discussing it with the friend, meeting the scammer or conducting reasonable due diligence. I thought the unexpected request for fees when he asked to make a withdrawal should have raised concerns, and I noted he wasn't given any invoices or promotional material, which he should reasonably have expected from a genuine investment.

Our investigator had explained that there were negative reviews about R which pre-dated the payments and so some basic checks might have uncovered the scam, just as a conversation with his friend would have shown his social media account had been hacked. So, I was minded to direct that the settlement should be reduced by 50% for contributory negligence.

Recovery

Mr S has described that he paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I was satisfied there was no prospect of a successful recovery.

Compensation

The main cause for the upset was the scammer who persuaded Mr S to part with his funds. I hadn't found any errors or delays to Monzo's investigation, so I didn't think he was entitled to any compensation.

Developments

Both parties have accepted my provisional findings.

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.

Because both parties have accepted my provisional findings, the findings in my final decision will be the same.

My final decision

My final decision is that I'm minded to direct that Monzo Payments Ltd should:

- refund Mr S the money he lost from the ninth payment onwards.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 8 January 2025.

Carolyn Bonnell
Ombudsman