DRN-4530031

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 company, 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 S came across an advert for an investment opportunity with a company I'll refer to as "X" while he was on social media. He was interested because he'd heard friends speaking about their investments and had also heard discussions about similar investments on TV. He googled the company and saw positive reviews on its website and on Trust Pilot, and as he thought it was a genuine opportunity he left his name, mobile number and email address on the online contact form. The following day, he received a call from someone claiming to a broker, who I'll refer to as "the scammer".

The scammer was friendly and professional and told Mr S that X had been operating for about five years and that he could make an initial deposit of £180. He told Mr S to download AnyDesk remote access software to his device and then used it to show him how to open accounts with X and a cryptocurrency exchange company I'll refer to as "F". He also asked him to send a picture of himself holding ID and proof of his address, and to set up secure log-in details for the apps which would allow him to log-in to his account.

The scammer said he would make all the trades Mr S's behalf and that he would take a commission. He told Mr S him to first purchase cryptocurrency through F and then load it onto an online wallet. Between 7 February 2022 and 1 March 2022, he made four transfers to F totalling £15,050 from his Monzo account. On 11 February 2022, he was able to withdraw £178.21 from his trading account, which reassured him the investment was genuine. He was also able to log into the trading platform to check his profits.

By the time the investment had grown to £82,000, Mr S decided he decided he wanted to make a withdrawal, but the scammer made various excuses as to why he shouldn't and he eventually realised he'd been scammed. He complained to Monzo with the assistance of a representative who said it had allowed him to send £15,050 to a new payee linked to cryptocurrency in seven days with no intervention.

But Monzo refused to refund any of the money he'd lost. It said it was unable to provide a refund because the fraudulent payments were sent from the cryptocurrency exchange and it was the onwards payments that had resulted in the loss.

It said it has designated pages on its website for scam education and Mr S didn't take sufficient steps to verify the legitimacy of the investment or to research the investment company. It said the promise of immediate profits was unrealistic and he'd heard about the investment via social media, which should have raised concerns. It said he didn't complete

reasonable due diligence because he didn't meet the third party or a representative of S in person or question the true identity of the scammer.

Mr S wasn't satisfied and so he complained to this service with the assistance of a representative. He explained he hadn't previously invested in cryptocurrency, so he struggled to conduct due diligence. And he had thought the investment was genuine because he couldn't see any negative reviews about S. He said he wanted Monzo to refund the money he'd lost and to pay him compensation and legal costs.

His representative argued that both payments were unusual when compared with Mr S's usual spending habits and he was paying a brand new payee, which was a cryptocurrency merchant. They explained that in November 2021, December of 2021 and January 2022, there were no payments over £100 and on the day he made the payment of £5,000, Mr S transferred in £10,000 from an external bank account, which represented a drastic change in the operation of the account. Similarly, on 1 March 2022, Mr S deposited two transactions of £5,000 each from his external account and immediately transferred £10,000 out to the scam.

They said Monzo should have contacted Mr S to ask him who he was paying, whether he'd been asked to download AnyDesk, whether he'd responded to any adverts on social media, whether he'd been cold called, whether someone had invested on his behalf, whether he'd been allowed to withdraw and funds from the platform, whether he had access to the account he was paying, whether anyone he knew had invested in the company before, whether he'd checked the Financial Conduct Authority ("FCA") website and whether he'd done other research. And with the answers Mr S would have given, it should have provided a scam warning and advice on additional due diligence, which would have prevented him from making any further payments.

Our investigator recommended that the complaint should be upheld. He explained the initial payments were low-value payments which matched the typical spending pattern on the account, so he didn't think Monzo needed to intervene when he made the first two payments. And he didn't think the £5,000 payment was unusual because on 22 April 2021 and 12 August 2021, £2,000 and £3,800 were transferred in and out of the account on the same day, the payee wasn't new and Mr S had received credits from F. So he didn't think Monzo needed to intervene.

However, he thought it should have intervened when Mr S paid £10,000 to F on 1 March 2022 because there wasn't a history of similar payments on the account. And by the time he made the payment, there was increase in activity on the account and the payment drained the account. He explained that Monzo ought to have identified the payment as unusual and suspicious, and contacted Mr S to question him about the payment.

Had it done so, our investigator was satisfied Mr S would have told Monzo he was investing in cryptocurrency and that he was being advised by someone who worked for a company he'd seen advertised on social media. With this information, even though he was paying a legitimate cryptocurrency merchant, Monzo should have provided a tailored scam warning which would have led Mr S to the discovery of an FCA warning from October 2021, which confirmed X was a scam. Because of this our investigator recommended that Monzo should refund Mr S the money he lost on 1 March 2022.

He explained that even though this was a sophisticated scam and Mr S wouldn't necessarily have known to search the FCA website, if he'd done some more thorough research, he would have seen a number of negative reviews which predated the disputed payments, so he thought the settlement should be reduced by 50% for contributory negligence.

Mr S has indicated that he accepts our investigator's view, but Monzo has asked for the complaint to be reviewed by an Ombudsman. It has explained the payments weren't considered suspicious or unusual because Mr S was authorising payments to a legitimate cryptocurrency exchange. And changes or increased spending to merchants of this nature aren't unusual considering the wider context of cryptocurrency as a market based product, whereby it's common for consumers to adjust their spending depending on the market.

It maintains the loss occurred when Mr S sent the funds to a third party from his cryptocurrency account and that they were "me-to-me" transactions, so he was in full control of the funds when they were received into the cryptocurrency wallet. It has argued that banks aren't expected to assess fraud that doesn't happen within their remit, and it isn't responsible for onward loss of cryptocurrency that was legitimately purchased.

It has argued that it has the right balance in its approach to reduce APP scams and the suggested intervention would have meant it was interrupting a legitimate payment journey which, contradicts regulators expectations, as set out in PSRs. It has also argued that in *Phillip v Barclays*, the regulator and the court have upheld that they expect banks to carry out customers wishes.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons.

The 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 an account in his own name, and I'm satisfied that's fair.

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 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 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).

• 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

Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Monzo ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need 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've 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 think they were. All the payments were to a legitimate cryptocurrency exchange and the first two payments were for small amounts, so Monzo didn't need to intervene. The third payment was for £5,000 on 24 February 2022 and while I note the representative's comments that there were no similar payments in the three months prior to this payment, there were payments for £2,000 and £3,800 on 22 April 2021 and 12 August 2021, therefore I don't think the payment was unusual so I don't think Monzo missed an opportunity to intervene.

However, I agree with our investigator that by the time Mr S made the £10,000 payment on 1 March 2022, the spending was unusual. And even though at this point Mr S had made several payments to F, the payments into the account immediately before the payment meant that there was a pattern of spending which should have been concerning. So I think Monzo missed an opportunity to intervene.

It should have contacted Mr S to ask him why he was making the payments, whether there was a third party involved and if so how he met the third party, whether he'd been told to download remote access software to his device, whether he'd been allowed to make small

withdrawals, whether he'd been promised unrealistic returns and whether he'd been told to make an onwards payment from the cryptocurrency exchange. There's no evidence that Mr S had been coached to lie and so I'm satisfied he would have told Monzo he'd seen an advert for X on social media and that he was being advised by a broker who had told him to download AnyDesk. I think he'd have also disclosed that he been allowed to make a small withdrawal from the trading platform and told to make an onwards payment from F.

With this information, Monzo would have been able to advise Mr S that there were red flags present indicating that he was probably being scammed. It could have given him a tailored scam warning and provided advice on additional due diligence. There's no evidence that Mr S was keen to take risks and so I'm satisfied he'd have listened to Monzo and subsequently found the FCA warning from October 2021, confirming the investment was a scam. Because of this I'm satisfied Monzo failed to intervene in circumstances which could have prevented his loss and that it should refund the money he lost on 1 March 2022.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. Mr S wasn't an experienced investor and so we wouldn't expect him to have known to check the FCA website for warnings. He hadn't invested in cryptocurrency before and he has said he didn't see any negative reviews. But there were negative reviews online about X which predated the disputed payments and if he'd done some basic internet research before going ahead, I'm satisfied he might have realised the investment was a scam. So, I agree that the settlement should be reduced by 50% for contributory negligence.

My final decision

My final decision is that Monzo Bank Ltd should:

- refund £10,000.
- 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 Bank 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 20 February 2024.

Carolyn Bonnell
Ombudsman