DRN-4597387

The complaint

Mrs A complains that Monzo Bank Ltd didn't do enough to protect her from the financial harm caused by a scam, or to help her recover the money once she'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.

Mrs A was actively looking for work and saw an advert on social media for an opportunity to work for a company I'll refer to as "S". She was contacted by someone I'll refer to as "the scammer" who told her she'd be paid commission to 'optimise' products to increase their marketability online. To purchase the tasks, Mrs A had to deposit cryptocurrency onto S's platform to simulate the purchase of the products. At the end of each set of tasks she would withdraw her commission and the original deposits.

Mrs A communicated with the scammer via WhatsApp. He told her she'd need to complete 70 tasks per day and that she could make 0.7% commission per task, although certain tasks could generate more.

Mrs A googled S and noted it was a genuine company. She was also added to a WhatsApp group with others working for the company. The scammer asked her to purchase USDT cryptocurrency from private individuals and then load it onto an online wallet. Between 14 January 2023 and 16 February 2023, she made sixteen transfers from her Monzo account totalling £19,106. On 16 January 2023, she received a withdrawal for £633.65.

Mrs A was reassured that she was able to make a withdrawal from the platform early on, but she became concerned when her account had a negative balance and the scammer pressured her to take a loan out so she could make a withdrawal. Eventually she was removed from the WhatsApp group and she was unable to reach the scammer, at which point she realised she'd been scammed.

Mrs A complained to Monzo but it refused to refund any of the money she'd lost. It said she wasn't eligible for a refund under the Contingent Reimbursement Model ("CRM") Code and that it had executed the payments in accordance with her instructions. It also said it has page son its website dedicated to scams and that before each payment, Mrs A was presented with a warning which gave her the option to stop and get advice, yet she chose to go ahead.

It also said Mrs A had paid private individuals and not cryptocurrency platforms, and she didn't complete reasonable due diligence, which would have included meeting the scammer and querying why the URL didn't match the name of the company and contained an unusual suffix. It said social media and WhatsApp groups aren't reliable sources of investment advice and she didn't question why she was being asked to make payments in cryptocurrency for a job opportunity.

Mrs A complained to this service with the assistance of a representative. Her representative said Mrs A had never purchased cryptocurrency from her Monzo account. The account was generally used for day to day spending, the largest transaction was for £689.99 and her income is roughly £1,500, so Monzo ought to have been concerned because she made six payments within a 24 hour period totalling £6,730. And by the time she made the payment of £3,300 on 27 January 2023, the amount and pattern of the payments ought to have raised concerns.

They said Monzo should have contacted Mrs A and asked her questions about the payments and had it done so she would have explained she'd recently taken a job that required her to deposit cryptocurrency to purchase tasks. With this information, Monzo would have easily identified that she was being scammed and any further loss would have been prevented.

Our investigator issued two views in which he recommended that the complaint should be upheld. She said the payments weren't covered under the CRM code because they were transfers to genuine P2P sellers.

She explained she didn't think payments 1-8 were unusual considering Mrs A's normal account activity so she thought confirmation of payee pop-ups and written warnings for each of the new payees was proportionate to the risk. However, she noted payment nine on 27 January 2023 was significantly higher in value than the previous payments she'd made from the account and she'd five made payments to new payees that day in quick succession totalling £5,480. She'd also transferred funds into the account and transferred them out again within minutes, which was a pattern of spending which was indicative of fraud. So she thought Monzo had missed an opportunity to intervene.

In the circumstances she thought Monzo ought to have contacted Mrs A and asked her about the purpose of the payments, why she was making multiple payments to new payees and if anyone was asking her to make the payments. Had it done she hasn't seen any evidence that Mrs A had been coached to lie so she thought she would have explained that she was buying cryptocurrency to simulate 'buying' items for a job opportunity, she'd come across the opportunity on social media, she was communicating with S via WhatsApp and she hadn't signed an employment contract. And as there was no reason to think Mrs A was keen to take risks, she was satisfied she would have listened to advice from Monzo that she was being scammed.

Our investigator recommended that Monzo should refund the money Mrs A had lost from that point onwards. But she felt the settlement should be reduced for contributory negligence because Mrs A didn't question why she was being required to make payments in cryptocurrency for a job she was expecting to be paid for, she didn't receive a signed contract and she was being paid in cryptocurrency.

Monzo has asked for the complaint to be reviewed by an Ombudsman. It has argued that Mrs A was purchasing cryptocurrency from private sellers and she received the cryptocurrency as expected. It has argued that the fraud occurred when Mrs A sent the cryptocurrency on to the scammers so liability sits with the cryptocurrency exchange.

Monzo has also explained that in the case of Philipp v Barclays, the regulator and the court upheld that they expect banks to carry out customers wishes and it's inappropriate for it to decline to do so. It has stated it would be unreasonable to require it to intervene in thousands of transactions daily to uncover potential losses in transactions it's not involved in.

It has further explained that APP fraud is included in the definition of criminal activity in its Terms and conditions but in line with the Phillip v Barclays ruling, it didn't have the right to

intervene in legitimate payment journeys and fraud wasn't suspected because fraud wasn't occurring.

Finally it has argued that it's not unusual for customers to use their Monzo accounts to purchase cryptocurrency, so there was nothing so out of the ordinary or suspicious about the payments.

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 Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mrs A says she's fallen victim to, in all but a limited number of circumstances. But the CRM code didn't apply in this case because Mrs A received the cryptocurrency she paid for.

There's no dispute that this was a scam, but although Mrs A didn't intend her money to go to scammers, she did authorise the disputed payments. Mrs A 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 Mrs A'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 6 December 2021 terms and conditions gave it rights to block payments where it suspects criminal activity on the 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 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 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 wasn't 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.

Prevention

I've 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've seen, the payments were made to genuine cryptocurrency sellers. I also note Monzo's comment that it didn't have the right to intervene in legitimate payment journeys, but it 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 Mrs A when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting Mrs A from financial harm due to fraud.

Each time she paid a new payee Mrs A was presented with a warning which gave her the option to stop and get advice. The first nine payments she made to the scam were relatively low value, there were payments of similar value on the account and because she was paying private individuals it wouldn't have been obvious she was buying cryptocurrency, so I'm satisfied the warnings Mrs A would have seen were proportionate to the risk.

But I think the ninth payment ought to have triggered an intervention from Monzo. This is because £3,300 was significantly higher than the previous payments, this was the fifth payment Mrs A had made that day to a new payee and the cumulative total for the day was £5,480, which was unusual for the account. I accept it wouldn't have been obvious that Mrs A was buying cryptocurrency but the nature of the payee isn't the only consideration and I agree with our investigator that this was a pattern of spending which ought reasonably to have raised concerns. So, I think Monzo missed an opportunity to intervene.

Monzo should have contacted Mrs A and asked her why she was making the payments and had it done so, as I haven't seen any evidence that she'd been coached to lie, I think she'd have told it she was buying cryptocurrency from P2P sellers which she intended to use to pay for tasks. I think its likely she'd have also said she'd seen the job advertised on social media, she hadn't signed a contract and she was following instructions from someone who was communicating with her on social media.

At this point, I think it would have been obvious that Mrs A was being scammed and so Monzo should have advised her that there were red flags present which indicated that she was being scammed. I accept that up to this point Mrs A hadn't picked up on the warning signs or done much due diligence but I'm satisfied that with some robust advice and guidance from Monzo, she'd have decided not to make any further payments. Because of this I'm satisfied that Monzo's failure to intervene when she made the ninth payment represented a missed opportunity to have prevented her loss and so it should refund the money she lost from that point onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. I accept this was a sophisticated scam and that Mrs A was reassured by the fact she was able to make a withdrawal from the platform. I also understand that because this was a role which required her to complete tasks online, she might not have thought it was necessary to meet the scammer. And I wouldn't expect her to have noticed inconsistencies with the URL.

But I think Mrs A should have been concerned that she was being asked to make payments in cryptocurrency for a job in respect of which she hadn't been given any employment documents or training. She should also have been concerned that she'd found the opportunity on social media and she was communicating with the scammer via WhatsApp. I think Mrs A should have taken more care to check she was dealing with a legitimate company and I think her failure to do so contributed to her loss. Consequently I'm satisfied the settlement should be reduced by 50% for contributory negligence.

Compensation

I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I don't think Monzo needs to pay any compensation given that I don't think it acted unreasonably when it was made aware of the scam.

My final decision

My final decision is that Monzo Bank Ltd should:

- refund the money Mrs A lost from the ninth payment onwards, less any credits received during the scam period.
- 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 Mrs S with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 11 April 2024.

Carolyn Bonnell
Ombudsman