DRN-4447060

The complaint

Ms M complains that Monzo Bank Ltd didn't do enough to protect her from the financial harm caused by an investment 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.

Ms M was the victim of an employment scam. She had seen a job opportunity on social media and was contacted on WhatsApp by someone claiming to work for a company I'll refer to as "T". The scammer told her to purchase cryptocurrency which would be used to top up an account to then pay for tasks.

Ms M was added to a WhatsApp group with other employees who shared their positive experiences and earnings. Throughout the day she was given multiple tasks to do and had to top-up the account with cryptocurrency if they weren't completed.

The broker asked her to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. Between 2 December 2022 and 18 December 2022, she made fourteen payments to individuals totalling £19,792.83 from her Monzo account. And during the scam period she received two credits totalling £419.71.

She realised she'd been scammed when the negative balance on the account kept increasing and she was unable to withdraw any funds. When she complained to Monzo, she said it had failed to provide any warnings when she made the payments and that she was unhappy with its decision to close her account when she reported the scam to it. She also complained about the time it had taken to review her scam claim.

Monzo accepted there were delays in the time it took to respond to the scam claim and offered £100 for the impact this had. It said it reached out to the bank where the money was sent but it was only able to partially recover the funds and the transactions didn't qualify for a refund under the Contingent Reimbursement Model (CRM) code. It also said it was unable to raise a chargeback request because once the money had reached the merchant, the service had been provided.

Finally, it said the decision to close the account was in line with the T&Cs of the account. It explained it had given him two months' notice on 12 January 2023, and the account was closed on the advised date.

Ms M complained to this service and our investigator thought the complaint should be upheld. He said £100 compensation was fair. And the first payment of £19.92 on 2 December 2022 was a low value payment to an individual, so Monzo didn't need to intervene. But he noted Ms M made a payment of £80.82 to a cryptocurrency exchange company I'll refer to as "B" on 3 December 2022 and as Monzo stopped all outbound

payments to B from 24 November 2022, he was satisfied that the transaction should have been flagged.

He said Monzo should have contacted Miss M to discuss the payment and had it done so, he was satisfied she would have been honest and told it she was buying cryptocurrency to send to a third-party wallet to buy tasks for an employment opportunity. With this information, he was satisfied Monzo would have identified that Ms M was being scammed and provided relevant warnings, which would have stopped her from making any further payments.

Our investigator said Monzo should refund the money Ms M lost from the second payment onwards, but he thought the settlement should be reduced by 50% for contributory negligence because Ms M should have been concerned about the fact she was making payments to multiple payees.

Monzo has asked for the complaint to be reviewed by an Ombudsman. It has argued that there's no way to know if Ms M would have disclosed what was happening, so there is no way to say for certain that the scam would have been uncovered.

It has said its fraud systems determined that Ms M was at a low chance of being a victim of fraud, so an intervention would have been inappropriate. It maintains it wasn't involved in any scam payments and has argued there's no legislation or code of practice requiring it to intervene in transactions.

Finally, it has argued that in *Phillip v Barclays* the court have upheld that they expect banks to carry out customers wishes and it's inappropriate for it to decline to do so.

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 Ms M says she'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 Ms M received the cryptocurrency she paid for, and I'm satisfied that's fair.

There's no dispute that this was a scam, but although Ms M didn't intend her money to go to scammers, she 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 Ms Ms's account is that he 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 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

I've thought about whether Monzo could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity, but 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 Ms M when she 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 Ms M 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 Ms M

normally ran her account and because of the low value of the first payment, I don't think it was. But as our investigator explained, Monzo stopped all outbound payments to B from 24 November 2022, so it should have flagged the payment that Ms M made to B on 3 December 2022.

Monzo ought to have contacted Ms M and asked her why she was making a payment to B and as there's no evidence she was coached to lie I'm satisfied she'd have told it she was making payments in cryptocurrency for an employment opportunity that she'd learned about on social media. With this information, I'm satisfied there were enough red flags present for Monzo to have identified that Ms M was being scammed and I would expect it to have warned her that she was probably falling victim to a scam and to have discussed with her the nature of the checks she'd undertaken and to give some advice on additional due diligence.

I haven't seen any evidence that Ms M was keen to take risks and I think that if she'd had any inkling this might be a scam she would have decided not to go ahead with the payments. Because of this, I think Monzo missed an opportunity to intervene in circumstances when to do so might have prevented Ms M's loss. Consequently, I'm minded to direct it to refund the money Ms M lost from the second payment onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and I haven't seen any evidence that Ms M did any due diligence before making payments to T. Having considered the circumstances of this scam, I'm satisfied it was sophisticated, but I think it was unreasonable for her not to have questioned why she was being asked to make payments in cryptocurrency for a job in respect of which he hadn't received any employment documents. Because of this, I think the settlement should be reduced by 50% for contributory negligence.

Compensation

Monzo has explained that its service level agreement gives it 35 days to investigate complex cases and that it didn't investigate the claim within this timeframe. It accepted this caused Ms M inconvenience and offered her £100 compensation for that. I've considered the circumstances and I'm satisfied £100 compensation is fair and that it addresses the impact on Ms M of Monzo's failings.

Recovery

As Ms M received the cryptocurrency she paid for, I'm satisfied there was no prospect of a successful recovery.

My final decision

My final decision is that Monzo Bank Ltd should:

- refund the money Ms M lost from the second payment onwards less any credits she 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 Ms M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 27 February 2024.

Carolyn Bonnell
Ombudsman