DRN-4612426

The complaint

Mrs B complains that Monzo Bank Ltd won't refund the money she lost as a result of a job scam.

Mrs B has used a professional representative to bring this complaint to our service and they have made submissions on her behalf. For consistency, I'll refer to Mrs B throughout.

What happened

In early 2023, Mrs B was contacted by a recruitment company (that I'll call O) via a social media messenger service. O was offering Mrs B a flexible and remote job opportunity which only required her to have internet connection. O told Mrs B it was essentially a marketing role. The role involved her 'driving data' to help well-known companies improve their data and reviews. For this, she was expecting to earn a daily commission and a basic weekly salary of £700.

She completed an online virtual training session, in which she was shown how to complete tasks. Mrs B understood she had to pay a deposit to unlock the tasks, which would be refunded with commission once she hit her target. O told Mrs B to open an account with a cryptocurrency exchange (that I'll call B) in order to facilitate the payments. She was told to make payments to individual employees of O, who would in turn fund her B account with cryptocurrency. She would then use the cryptocurrency to fund her O account and complete the tasks. Mrs B was added into a social media messenger group chat with other alleged employees of O who praised O, and shared success stories.

Between 4 to 12 February 2023, Mrs B made a series of payments to unlock tasks totalling £8,600. Mrs B also received credits into her account totalling £4,518.38, which were supposedly returns from O. These transactions can be seen in the below table:

No#	Date	Payee	Amount
1	4/2/23 23:03	Payee 1	-£100
2	6/2/23 14:40	Payee 2	-£100
3	6/2/23 15:19	Payee 3	-£50
4	6/2/23 15:39	Payee 3	-£150
	6/2/23	*Credit from external account 1*	*+£514.54*
5	7/2/23 11:35	Payee 3	-£100
6	8/2/23 10:44	Payee 3	-£400
7	8/2/23 16:47	Payee 3	-£100
8	8/2/23 17:26	Payee 3	-£800
	8/2/23	*Credit from Payee 3*	*+£800*
9	8/2/23 17:52	Payee 4	-£800
10	11/2/23 11:56	Payee 5	-£3,000
	12/2/23	*Credit (Payment 10 recalled)*	*+£3,000*
11	12/2/23 11:59	Payee 4	-£2,500
12	12/2/23 12:26	Payee 6	-£500
	13/2/23	*Credit from external account 2*	*+£203.84*

		Total outstanding loss (debits less credits)	**£4,081.62**

As Mrs B continued to pay for and complete tasks, these became more expensive to unlock. She continued to make payments until she ran out of money. She contacted the other employees in the group chat for financial assistance, but they encouraged her to borrow from friends and family or take out lending. When she asked O if she could make a withdrawal, she was met with requests for further funds until Mrs B realised that she had been scammed.

Monzo says the scam was reported around 14:22 on 26 May 2023. It contacted the firms Mrs B sent her funds to but unfortunately, no funds remained. On 10 July 2023, Monzo declined to refund Mrs B because:

- The payments went to Mrs B's own account with a cryptocurrency exchange, so they were not 'scam' payments. Monzo referred Mrs B to the cryptocurrency exchange instead.
- It executed the payments in line with Mrs B's instructions and it showed Mrs B a warning when she set up the payees.
- The payments wouldn't be covered under the Contingent Reimbursement Model (CRM) Code, which Monzo has agreed to abide by the principles of. The CRM Code sets out that Monzo should refund victims of authorised push payment (APP) scams (like Mrs B), in all but a limited number of circumstances. Monzo said the payments to international accounts would not be covered as the CRM Code doesn't cover international payments. And Mrs B also made payments to individuals for the purchase of cryptocurrency, so as it was the onward transmission of funds that resulted in the loss, these too wouldn't be covered under the CRM Code.
- Mrs B had no reasonable basis for belief as the returns were unrealistic, she didn't sign any contracts or go through anything before starting the role. And she was asked to invest her own money to earn an income, which no legitimate employer would do. It also said social media messenger isn't a reliable source of employment advice.

Unhappy with this outcome, Mrs B referred her complaint to our service. Our Investigator recommended that Monzo refund 50% of the payments Mrs B made from 12 February 2023 onwards, together with 8% simple interest per year on this amount, from 12 February 2023 to the date of the settlement. They thought Monzo ought to have prevented Mrs B's loss from that point, through some basic questioning. But Mrs B also acted with contributory negligence and so she should share equal responsibility for the loss.

Mrs B originally accepted this outcome. However she later rejected it on the basis that she wanted a 50% refund of all of the transactions in dispute, as she thinks they were all unusual for her account.

Monzo disagreed with our Investigator's recommendations too. It said:

- The payments were legitimate and didn't result in a loss as Mrs B paid for goods/services which she received. It can't be expected to assess the risk or be held liable for activity that occurred on an external platform.
- The Investigator's request would require Monzo to intervene on thousands of transactions daily, to uncover potential losses in transactions it isn't involved in, at a rate of a fraction of a percent.
- It didn't deem the payments to be suspicious, so it didn't do more than provide the

standard in-app payment flow warnings.

- There are no regulatory requirements or expectations, rules, codes or best practice that shares the view that Monzo should have intervened, and that the absence of intervention makes it liable for the customer's loss.
- It referenced the upcoming Payment Services Regulator's mandatory reimbursement scheme. It noted this, and rules around APP fraud outline banks aren't expected to assess fraud that doesn't happen within their remit. And banks aren't responsible for onward loss of cryptocurrency when purchased legitimately by them.
- Monzo referred to a recent Supreme Court ruling in Philipp v Barclays Bank UK PLC. It said the starting position of the law is that it's under an implied duty to make payments promptly. And whilst it could refuse payments where it suspects fraud, it's not under a contractual duty to do this. In line with the current account contract, Monzo isn't required or obliged to make fraud checks. It said the ruling upheld that banks should carry out customers' wishes, and it would be inappropriate for Monzo to decline to do this.
- There is no evidence to support or disprove that an intervention from Monzo would have prevented the onward loss. It is an assumption based on conjecture. Whilst Monzo doesn't suggest Mrs B would have been dishonest, it noted it's just as possible she might have said she was purchasing cryptocurrency from private sellers, had she been questioned. This would have satisfied Monzo that Mrs B was making legitimate payments as it's aware the cryptocurrency exchange Mrs B paid has robust measures in place to prevent fraud occurring on the peer-to-peer market.

As no agreement could be reached, this case was passed to me for a decision to be issued.

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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mrs B's account is that Mrs B is responsible for payments she has authorised herself.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks 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 to their customers 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, it 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.

- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. 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 legal duty to do so.

In this case, Monzo's December 2021 (2.2) terms and conditions gave it rights (but not obligations) to:

- Block payments if it suspects criminal activity on a customer's account. It explains if it blocks a payment, it will let its customer know as soon as possible, using one of its usual channels (via its app, email, phone or by post)

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, the basic implied requirement to carry out an instruction promptly did not in any event mean Monzo was required to carry out the payments immediately[1]. Monzo could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Monzo should in February 2023, fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Monzo should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks, like Monzo do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

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)[2].
- 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".*[3].
- Regulated firms 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). I do not suggest that Monzo ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Monzo's obligation to monitor its customer's accounts and scrutinise transactions.
- 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 (regardless of the fact the BSI was withdrawn in 2022).

---

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

[3] For example, both the FSA's Financial Crime Guide at 4.2.5G and the FCA's 2015 "Financial crime: a guide for firms" gave examples of good practice in relation to investment fraud saying:

"A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.

A bank contacts customers if it suspects a payment is being made to an investment fraudster.

A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules."

- 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 circumstances (and it does not apply to the circumstances of these payments), 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.
- Monzo should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name.

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in February 2023 that Monzo should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms 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 Monzo sometimes does);
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Monzo have recognised that Mrs B was at risk of financial harm from fraud?

I've reviewed Mrs B's statements from September 2022, and I note the following:

- Mrs B's account was typically used for low-value day to day spending, normally by way of card payment.
- She made a small number of payments by faster payment out to two payees. One of these, which most of the faster payments were made to, appeared to be Mrs B's own account. The other payee appeared to be a third party's name and I can only see one payment made to this payee.
- Between 4 February and 12 February 2023, Mrs B made 11 faster payments out and 1 international payment, to 6 different recipients. It was not in keeping with Mrs B's typical account usage for her to make so many transactions out to third party payees in such a short space of time.
- The values of the initial payments she made as part of the scam, didn't appear to

stand out in comparison to previous debits on the account.

- In the six months leading up to the scam, she typically spent an average of around £870 per month. In the week she was making the scam payments, these amounted to £8,600. This level of spending was a drastic change and uncharacteristically high for Mrs B.
- On 8 February 2023, Mrs B cleared the majority of the balance in her pot and transferred it into her current account in order to send £3,000 overseas on 11 February 2023. It was also not common for Mrs B to make international payments.

I've considered that Mrs B made 7 payments to payee 3, however these payments spanned multiple days and fluctuated in value. The credit received on 8 February 2023 might have also reasonably alleviated some of the risk attached to the payee. But as the payments continued, and by the £2,500 payment on 12 February 2023, I'm persuaded that Monzo ought fairly and reasonably, to have been concerned that Mrs B was at an enhanced risk of financial harm due to fraud.

Whilst I accept that people's spending habits can change, by 12 February 2023 Mrs B had made 11 payments to 5 payees and had spent £5,600 in 8 days. She'd also cleared the majority of the balance in her savings pot and had made a payment to an international account which is not typical for her. Taking all of these things into account, Monzo should have taken steps to make further enquiries with Mrs B about the recent activity on her accounts.

Whilst Monzo showed Mrs B some generic online warnings when she set up the payees, I'm not persuaded these went far enough in the circumstances. A proportionate intervention in these circumstances, would have been for Monzo to make enquiries with Mrs B, such as via the in-app chat.

What difference would further enquiries have made?

I've thought about whether a proportionate intervention from Monzo would have made a difference in uncovering the scam. In doing so, I've listened to a call between Mrs B and her other bank (Bank H) where she first attempted to pay the fraudster. The call concerned a payment for £100 on 31 January 2023, which Bank H blocked. During this call, Mrs B told Bank H she was trying to send the money to her brother via her sister in law's account. But that she'd found another way and had sent it to her husband instead. Having reviewed Mrs B's statements, it appears this was sent to her Monzo account and four days later, the disputed transactions start from her Monzo account, also beginning with £100.

Mrs B has told our service that the fraudster told her to tell the bank it was for 'friends and family'. However, this was the extent of her cover story. Had Monzo made some basic enquiries with Mrs B, I'm persuaded the scam would have come to light as I don't think Mrs B could have maintained a plausible cover story in response to such questioning. And, by the point at which I think Monzo ought to have intervened, it would no longer be plausible to say the payment was for a friend or family member, given she had made 11 payments to 5 payees in the recent days. So I'd have expected Monzo to ask further questions to uncover the true reason for the payments and warn her that fraudsters will often tell customers to hide the true reason for payments from the bank, and if she had been told to do this, she was being scammed.

Whilst Monzo has said Mrs B could have confirmed she was buying cryptocurrency, I'm not in agreement that this ought to have alleviated the concerns Monzo ought to have had about the payments.

Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions. By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. This left a smaller number of payment service providers that allow customers to use their accounts to purchase cryptocurrency with few restrictions. And could in turn mean customers choose to make peer to peer cryptocurrency purchases – rather than purchasing it directly from a cryptocurrency exchange.

So, by February 2023, firms like Monzo had been aware of the risk of multi-stage scams involving cryptocurrency (that is scams involving funds passing through more than one account controlled by the customer before being passed to a fraudster) for some time. And Monzo, ought fairly and reasonably to have made further enquiries to establish the circumstances behind the purchase of cryptocurrency.

Essentially, Mrs B thought she was making payments in order to receive employment which ought to have been a red flag to Monzo. I'd expect Monzo to have had a meaningful discussion with Mrs B about the common features of job scams such as making payments to gain employment, being paid to complete tasks and not being able to withdraw funds. And had Mrs B been warned that if she proceeded, it would be highly likely she'd lose her funds, I don't believe she would have proceeded to make further payments.

Can Monzo fairly and reasonably be held liable for the loss which occurred on Mrs B's account with B?

I've taken into account that Mrs B received cryptocurrency in receipt of the payments made to her account with B, and sent this on to a fraudster, rather than paying the fraudster directly from Monzo. But when these payments took place, Monzo ought to have been aware of multi-stage scams involving cryptocurrency. Monzo should fairly and reasonably and as a matter of good practice have been on the lookout for payments presenting an additional scam risk. And in this case, I'm satisfied that Monzo should have made further enquiries with Mrs B before processing the £2,500 payment. And had it done this, I think it's more likely than not that the scam would have come to light and Mrs B's loss would have been prevented, for the reasons explained above. So the loss was foreseeable to Monzo, and it can fairly and reasonably be held liable for it.

Did Mrs B act reasonably in the circumstances?

Mrs B has accepted our Investigator's findings that she should share responsibility for her loss. I am in agreement with this point, and largely for the same reasons as our Investigator. It's not in dispute that Mrs B is the victim, and I'm very sorry she lost this money. But taking into account the overall scam and what was being promised, I think she ought to have held some concerns about the job opportunity and the request being made of her. Specifically, I don't find it plausible that she was asked to make payments for cryptocurrency, towards a job opportunity in order to get paid. And I think she ought to have been concerned that she was being told to hide the true reason for the payments from the bank. Whilst I do appreciate there were some more persuasive elements of the scam, such as online training and access to a platform to complete tasks, I find that the causes for concern far outweigh these. And as such, ought to have prompted a more cautious approach from Mrs B. Overall, I think it's fair that Mrs B accept partial responsibility for her loss.

Recovery of funds

I'm not persuaded that there was any reasonable prospect of Monzo being able to successfully recover Mrs B's funds once she reported the scam. I say this because Mrs B used the funds sent from her Monzo account to individual recipients, to purchase cryptocurrency, which she received and sent on to the fraudster. So Monzo was unable to recover this.

The CRM Code

Like the Investigator, I'm persuaded this case doesn't fall under the CRM Code. Mrs B sent the funds to third parties and in return received cryptocurrency, which she sent to a fraudster. Mrs B received the cryptocurrency she paid for. And the subsequent onward transmission of that cryptocurrency from B to the fraudster is not a faster payment between GBP accounts, as it's a transaction in cryptocurrency. The CRM Code only covers faster payments between GBP, UK-based accounts.

My final decision

For the reasons I've explained, my final decision is that I partially uphold this complaint about Monzo Bank Ltd.

If Mrs B accepts my decision, Monzo should:

- Refund 50% of the final two payments Mrs B made (which I calculate to be a refund of £1,500)
- Pay 8% simple interest on the refund, per year, from the date the payments debited her account, until the date the refund is paid, less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 6 September 2024.

Meghan Gilligan
Ombudsman