DRN-4925417

The complaint

Ms B complains that Monzo Bank Ltd won't reimburse her after she fell victim to a job scam.

Ms B is professionally represented in bringing her complaint to our service. However, for ease of reference, I'll refer to all submissions as being made by Ms B directly.

What happened

Ms B has explained that she was approached by an individual on an instant messaging app purporting to work for a recruitment company and asking whether she was interested in earning extra income. Ms B confirmed she was, and another individual then got in touch with her, explaining more about the job role available. Unfortunately, unknown to Ms B at the time, both these individuals were in fact fraudsters.

Ms B was told the role was to help promote and increase the visibility of online applications (apps). Ms B was told she could earn a daily wage, plus a bonus salary for 'full attendance' and further commission. Ms B agreed to create an account on the fraudulent platform and was walked through the role on a 'practice account' with the fraudster. Ms B was told she needed to review 40 apps in order to be paid and that while most of these were regular apps, some were 'combos', meaning the employee earns ten times the standard commission on those tasks, but also has to first add funds to their account to complete the review. Once Ms B had been through a practice run, she was shown how to set up a cryptocurrency account and begin her own app reviews.

Ms B was told to add funds to her account to begin, which she then had to increase when she became a 'regular member'. Ms B initially made payments towards the scam through another of her bank account providers, but when they froze her account, the fraudster told her to open two other bank accounts, one being with Monzo. Ms B did as instructed and continued making payments through these accounts towards the scam. As Ms B went through the app reviews, she received numerous 'combo' apps, each requiring her to add increasing amounts of cryptocurrency to her account.

However, when her 40 tasks were completed, rather than being able to withdraw her wages as had been suggested by the fraudster, she was told her account had been 'upgraded' - requiring further tasks to be completed before she could make the withdrawal. When these further tasks were completed, she was then told a 'withdrawal fee' of over £35,000 had been applied to her account, followed by a 'latency fee' of £18,000 and then a 'contract fee' of £20,000

In an attempt to meet these demands, Ms B sold her car, took out loans, borrowed from friends, and her family member even sold his car to help her. However, when Ms B had no funds left to send, she realised she had fallen victim to a scam and contacted Monzo to raise a claim. In total, Ms B sent around £100,000 to the fraudster from her Monzo account, in the space of around three weeks. I've included a list of transactions Ms B made towards the scam below:

Date	Payee number	Value

13/07/2023	1	£370.70
13/07/2023	1	£370.70
13/07/2023	2	£319.30
13/07/2023	3	£310
13/07/2023	4	£2,500
13/07/2023	4	£3,500
13/07/2023	4	£2,000
14/07/2023	5	£1,000
14/07/2023	6	£215.60
14/07/2023	7	£549
14/07/2023	8	£233.50
14/07/2023	4	£3,500
14/07/2023	9	£3,500
14/07/2023	4	£3,500
15/07/2023	10	£3,000
17/07/2023	4	£3,500
18/07/2023	4	£3,500
18/07/2023	4	£3,500
18/07/2023	11	£600
18/07/2023	12	£510
18/07/2023	13	£90
19/07/2023	14	£390
19/07/2023	15	£3,000
19/07/2023	Cryptocurrency platform payment	£2,900
21/07/2023	Cryptocurrency platform payment	£2,000
21/07/2023	15	£3,500
21/07/2023	16	£914
21/07/2023	15	£686
24/07/2023	17	£2,500
24/07/2023	17	£2,500
24/07/2023	17	£2,000
24/07/2023	18	£1,700
24/07/2023	18	£500
24/07/2023	17	£500
24/07/2023	17	£300
25/07/2023	19	£789.82
25/07/2023	20	£193.75
26/07/2023	21	£2,200
26/07/2023	22	£564
27/07/2023	23	£2,500
28/07/2023	24	£3,000
28/07/2023	25	£1,882
28/07/2023	26	£1,118
Date	**Payee number**	**Value**
28/07/2023	10	£4,000
28/07/2023	27	£10,000
29/07/2023	28	£4,000
29/07/2023	23	£4,000
29/07/2023	29	£1,900
31/07/2023	30	£835
31/07/2023	31	£200

01/08/2023	23	£3,000
01/08/2023	23	£2,000
01/08/2023	23	£3,200
01/08/2023	32	£134
01/08/2023	33	£2
02/08/2023	34	£50

Monzo considered Ms B's claim but declined to reimburse her. It said that Ms B's money wasn't lost at the point it left her Monzo account, but when it later left her cryptocurrency account to the fraudster. It therefore advised that Ms B should refer her complaint instead to the cryptocurrency wallet provider.

Ms B remained unhappy and referred her complaint to our service. Monzo failed to provide us with its file, but in spite of this, an investigator was able to consider the complaint and provide an outcome. The investigator didn't uphold the complaint. As part of the investigation, Ms B's other bank had provided information regarding its own fraud investigations that took place and calls it had with Ms B during the scam. The investigator concluded that as Ms B had repeatedly withheld the truth about the payments to her other account provider, despite them relaying serious concerns about the account activity, any action Monzo ought reasonably to have taken would also have been unlikely to stop the scam from taking place.

Ms B disagreed with the investigator's view. To summarise, Ms B considered that had Monzo blocked the scam payments she was making, her losses would have been prevented and that Monzo didn't do enough to protect her. Ms B has also said she was vulnerable to the scam as she'd recently lost her father and was trying to work remotely to return home to support her family.

As Ms B disagreed with the investigator's view, the complaint has been referred to me for a final decision. Since the complaint has been with me at decision, Monzo has now provided its business file.

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.

There's no dispute that Ms B authorised these transactions and that means that under the Payment Services Regulations 2017 and the terms of her account she is presumed liable for the loss in the first instance. The Contingent Reimbursement Model (CRM) Code does provide further protection for *some* payment transfers that were made as the result of a fraudster. However, the CRM Code does not include transfers such as this where the payments were used for the purchase of cryptocurrency, either directly or through peer-to-peer lending.

However, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Monzo ought fairly and reasonably to 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.

In addition, since 31 July 2023 when the Financial Conduct Authority's (FCA) Consumer Duty came into force, there are additional obligations on firms to avoid foreseeable harm to customers. As a result, where it would be considered appropriate based on the risk level,

we'd expect warnings provided by firms to be more 'dynamic', asking questions to better understand the scam risk and for these questions to cover potential job scams, as this was.

As Ms B had only opened her Monzo account as part of the scam, there wasn't any typical spending for Monzo to compare the scam payments to. However, on the first day Ms B used her Monzo account, she paid four new payees, with £8,000 being sent to one payee across three separate transactions. I think that Monzo ought to have done more to intervene on these payments by an agent contacting Ms B to ensure she wasn't at risk of financial harm from fraud by the time she made the third payment to payee four.

Monzo didn't intervene at this point, but I can see it did later intervene on 21 July 2023 by freezing Ms B's card and asking some questions, followed by a call to Ms B. These questions were focused on the cryptocurrency payment Ms B made that day. Ms B told Monzo she was paying back a loan, not purchasing anything and that her wallet with the cryptocurrency provider was now closed. Monzo requested evidence of the closed account which she provided.

Having considered the questions asked and the responses provided by Ms B, I don't think Monzo went far enough in getting to the bottom of the payments Ms B was making. It appears Monzo's concern at this point was that Ms B had fallen victim to an investment scam, and its warning provided was therefore focused on this. While some of the points it raised were relevant to Ms B's circumstances (for example, advising that scammers will ask you to set up multiple bank or cryptocurrency accounts), the vast majority of advice provided wasn't relevant. But having said that it's clear to see that Ms B was purposefully misleading Monzo on the purpose of the payments she was making, on the fraudsters advice and this impacted Monzo's ability to provide a more relevant warning. I've therefore had to consider whether I think further probing by Monzo would've made a difference here.

In doing so, I've considered the intervention that took place on Ms B's other bank account. Ms B's other provider questioned Ms B largely between 15 July 2023 and 19 July 2023, so at a similar point of the scam. During these calls, the advisor began by emphasising the importance of Ms B being honest, explaining that fraudsters are providing their customers with stories (as was the case here) to get payments to go through and that this is a scam.

Ms B was asked about the account she was sending funds to. Ms B confirmed it was a recently opened Monzo account and she was using it for a new business venture, buying and selling goods from her home country. The advisor questioned other payments, and Ms B advised she'd also set up another new account with a different bank. The advisor confirmed this was concerning activity, explaining fraudsters will request for people to open new bank accounts and move funds between accounts – and that this pattern appeared particularly prevalent with the two account providers Ms B had been told to use. The advisor explained there's no reason that Ms B can't send funds for payments owed directly from her account with them. The advisor also confirmed that one of the other payees Ms B had attempted to make a payment to was an account they consider highly suspicious and linked to fraud. For these reasons Ms B was asked to send evidence of her other new accounts and payments being made.

Ms B initially only sent evidence of some payments made from her Monzo account, but as the advisor refused to accept this, Ms B then sent her full statements. From these, on 19 July 2023, the advisor questioned Ms B further and was able to establish Ms B was making payments through peer to peer lending. The advisor explained the high risk involved in these types of payments and how they are more commonly linked to scams. She also questioned the link between this and Ms B's initial story that she was buying and selling items from abroad.

Ms B explained that her father passed away around a year ago and left her some inheritance, so she was looking to try new things with the funds. She explained a friend from home had been guiding her on cryptocurrency. The advisor again expressed her concerns, particularly as since blocking Ms B's card, Ms B had attended branch to bypass the blocks and made several further large payments. Ms B was questioned on other payees, which she advised she knew through friends (despite this not being true and these being more P2P lenders) and explained that the individuals who have helped her with P2P trading are long term friends.

The advisor remained concerned and advised she wanted to see Ms B's cryptocurrency wallet, evidence she can withdraw funds and photo identification from her friends before her account could be unblocked. Even when raising the scam claim with this bank, Ms B maintained a story different to the truth – that a friend from home had taken advantage of her, knowing she had inherited funds.

Based on these calls and the lengths Ms B went to conceal the truth from her bank provider and proceed with making payments, I unfortunately think that Ms B was so under the spell of the fraudster, there was little Monzo, or any bank would've been able to do to break the spell and had Monzo pushed further in its own questioning of Ms B, it also would have been unlikely to uncover the real purpose of the payments.

I think Monzo should have intervened on not just 13 July 2023, but also again by 19 July 2023 given the sheer number of high value payments to multiple payees and a further payment to a cryptocurrency platform - and again on 28 July 2023 when the value of payments increased to £10,000. However, even if Monzo had done so, I simply can't conclude this would've stopped the scam from taking place. Ms B had been warned about a number of concerning elements of her payments by another provider and had chosen to withhold the truth about the payments and provide a detailed cover story. While I think Monzo would have been highly suspicious about payments being made had it contacted Ms B on these occasions, as Ms B's other account provider was, I don't think it could have unequivocally concluded Ms B was falling victim to a scam to stop her from making further payments, and even if her account had been blocked, I think based on Ms B's insistence on making these payments, she would have simply found other ways to do so.

Similarly, as mentioned above, on 31 July 2023, the FCA's Consumer Duty came into force, which placed expectations on firms to provide better, dynamic warnings to understand the nature of payments being made. However, again, this would be reliant on Ms B providing accurate responses to questions posed. Based on the evidence available, it appears Ms B would have continued to advise Monzo that she was repaying a loan to a friend and therefore any dynamic warning would've been based on scams around these payment types. Therefore, any further warnings posed to her wouldn't have aided Monzo in uncovering the scam.

I've also thought about Ms B's comments that she was particularly vulnerable to this scam, given her personal circumstances. As Ms B's payments aren't covered by the CRM Code, there is less protection for reimbursement when considering vulnerability to a scam. I would instead need to consider what Monzo was aware of and whether it should've done more to protect her, considering any vulnerability. As Ms B had only just opened her account with Monzo, I see no reason Monzo would've been aware of Ms B's circumstances, and therefore I don't think it had reason to be more alert to payments she was making.

I've gone on to consider whether I think Monzo could have recovered any funds, once it was made aware of the scam. Unfortunately, Ms B made all her payments to cryptocurrency, either directly to a platform, or through P2P lending – meaning the movement of funds wasn't the point of loss, but the onwards movement of cryptocurrency was. Sadly, this is a

tactic commonly used by fraudsters as it makes the tracing of funds by a victim's bank far more difficult. Therefore, I don't think Monzo had any prospects of successfully recovering Ms B's funds.

Overall, while I'm sorry to disappoint Ms B – and while I don't underestimate the awful impact this scam will have had on her both financially and emotionally, I simply can't conclude, based on the available evidence, that Monzo would have been able to prevent her losses, based on any proportionate action I'd have expected it to take. As I don't find Monzo could have prevented her from making payments, it follows that I don't hold it liable to reimburse any payments she made from her account.

My final decision

My final decision is that I don't uphold Ms B's complaint against Monzo Bank Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 5 November 2024.

Kirsty Upton
Ombudsman