DRN-5683554

The complaint

Ms W complains that Monzo Bank Ltd won't refund the money she lost when she fell victim to an investment scam. Ms W is represented in this complaint, but I'll refer to her as it's her complaint.

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 W explains that, prior to the scam, she'd experienced sad family bereavements which she found difficult to come to terms with. She feels this impacted her emotionally and she wasn't in a clear head space, making her more susceptible to the scam.

Ms W was attracted by a cryptocurrency investment advert after using an internet search engine. Ms W says she did some research on the company (Company A) and, after being impressed with the professionalism of their website and directors she made enquiries with them.

Ms W was contacted by X (a scammer) who said they were an account manager. Ms W was impressed with X and was informed she would have an online trading account, assigned traders and an investment broker who would instruct her on how and what to invest in.

As Ms W was led to believe she could make a lot of money through Company A she decided to invest with them. To pay Company A she was given details of a crypto wallet.

Ms W made payments from a crypto account she already had with crypto exchange Company C. She later paid through another crypto exchange company (Company U).

As she could see increasing investment profits on Company C's trading platform, Ms W paid more and more money. Ms W made the following 47 payments to the scammers Company A crypto wallet, totalling £46,309.

Number	Date	Payment Type	Payee	Amount
1	29 March 2023	Card	Company C	£1,000
2	2 May 2023	Card	Company C	£1,100
3	30 May 2023	Card	Company C	£1,000
4	13 June 2023	Card	Company C	£10
5	14 June 2023	Card	Company C	£10
6	16 June 2023	Card	Company C	£1,480
7	16 June 2023	Card	Company U	£500
8	17 June 2023	Card	Company U	£500
9	18 June 2023	Card	Company U	£500

10	19 June 2023	Card	Company U	£500
11	20 June 2023	Card	Company U	£125
12	20 June 2023	Card	Company U	£375
13	21 June 2023	Card	Company U	£500
14	22 June 2023	Card	Company U	£500
15	23 June 2023	Card	Company U	£500
16	23 June 2023	Card	Company C	£1,500
17	24 June 2023	Card	Company U	£500
18	25 June 2023	Card	Company U	£500
19	26 June 2023	Card	Company U	£500
20	27 June 2023	Card	Company U	£500
21	28 June 2023	Card	Company U	£500
22	29 June 2023	Card	Company U	£500
23	30 June 2023	Card	Company U	£500
24	1 July 2023	Card	Company U	£500
Sub-total A				£14,100
25	1 July 2023	Card	Company C	£7,500
26	7 July 2023	Card	Company U	£500
27	8 July 2023	Card	Company U	£500
28	9 July 2023	Card	Company U	£110
29	11 July 2023	Card	Company U	£500
30	12 July 2023	Card	Company U	£500
31	13 July 2023	Card	Company U	£500
32	13 July 2023	Card	Company C	£2,600
33	16 July 2023	Card	Company U	£500
34	17 July 2023	Card	Company U	£500
35	18 July 2023	Card	Company U	£500
36	19 July 2023	Card	Company C	£4,900
37	20 July 2023	Faster Payment	Company U	£99
38	20 July 2023	Faster Payment	Company U	£600
39	20 July 2023	Faster Payment	Company U	£500
40	26 July 2023	Faster Payment	Company U	£100
41	26 July 2023	Faster Payment	Company U	£1,000
42	26 July 2023	Faster Payment	Company U	£2,000
43	26 July 2023	Faster Payment	Company U	£900
44	27 July 2023	Faster Payment	Company U	£100

45	27 July 2023	Faster Payment	Company U	£3,900
46	28 July 2023	Faster Payment	Company U	£100
47	28 July 2023	Faster Payment	Company U	£3,800
Sub-total B				£32,209
Total				**£46,309**

In mid-July, Ms W told X that she wanted to withdraw some of her funds. However, she was told there was a requirement to pay release fees.

Following this, Ms W received an email which had supposedly come from HMRC. This email explained that her funds were being held by HMRC and to release her funds she was required to pay tax. Ms W was concerned and contacted a legitimate HMRC number to discuss this. HMRC informed her it was a scam email. It was at this point that Ms W started to feel wary of the scammer and ultimately realised that she had been scammed.

Ms W complained to Monzo seeking a reimbursement of the monies lost, 8% interest and £300 compensation. She considers that they '*failed to detect the known hallmarks of this scam as it unfolded'* and feels that if they had intervened on transaction number 1 all of her loss could've been prevented.

Monzo didn't uphold Ms W's complaint. They said:

- They acted in accordance with her instructions.
- Ms W *'made the payments despite having been provided with and having access to education on scams similar to the Scam'.*
- The Contingent Reimbursement Model Code (the Code) doesn't apply.
- They're unable to refund the payments made via card as there are restrictions in place on the type of chargebacks that can be raised for investment purposes. Also, the card payments were authorised by 3DS (3D Secure),

Ms W escalated her complaint to our service and our investigator considered that Monzo should've intervened at payment number 25 and, if they had, her loss from this point could've been prevented. She also considered that because of contributory negligence from Ms W liability should be shared equally between both parties from payment 25.

Ms W accepted her view but Monzo disagreed. So, this case has been referred to me to look at.

Monzo's reasons for disagreeing included the following:

- There is conflicting information about Ms W's experience in crypto investments.
- Ms W had used Firm C and Firm U before and made payments for similar amounts.
- Our service hasn't considered a transaction for the same amount as payment 25, that was made more than six months previously.

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, my decision is to partially uphold this complaint. And I'll explain why.

I should first say that:

- I'm persuaded by Ms W's submissions that a scam has occurred here.
- I'm very sorry to hear that Ms W has been the victim of this cruel investment scam and lost a significant amount of money.
- Although a voluntary code was in place in 2023 (the Contingent Reimbursement Model Code – CRM Code) to provide additional protection against some scams and Monzo adhered to the principles of this code, as the payments were made to an account in Ms W's own name (before they were sent to the scammer) and also by card, they're not covered under the CRM Code.
- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on the balance of probabilities.
- Although I've read and considered everything Ms W and Monzo have said, I won't be responding to every point individually. If I don't comment on any specific point, it's not because I've not considered it, but because I don't think I need to comment on it in order to reach the right outcome.
- I did consider Ms W's vulnerability points even though the FCA's Consumer Duty came out at the end of July 2023.
- The Payment Services Regulations 2017 (PSR) apply here.

  Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Ms W made the payments here, so they are considered authorised.

  However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

  So, I consider Monzo should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
  - Have systems in place to look 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, r made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

With all the above in mind, I considered whether:

<u>Monzo should've recognised that Ms W was at risk of financial harm from fraud and intervened?</u>

Having viewed Ms W's Monzo statements and information on transactions over six months (dating back to November 2022, which our service can consider), together with Company U statements (which I requested), I found that Ms W did:

- Have experience of investing in crypto.
- Use her Monzo account fairly regularly to pay her crypto exchange account and this included a payment for the same amount as payment number 25 (£7,500).

Although Monzo rightly point out that Ms W's crypto transactions weren't out of character, my analysis showed that Ms W's crypto transactions in the months of June and July 2023 were unusual because of both the scale and frequency.

My analysis is as follows:

<u>Crypto transactions in the 12 months prior to June 2023</u>

- In the previous 12 months (June 2022 to May 2023) Ms W made 12 payments:
  - Including £7,500 in November 2022.
  - Excluding 3 payments to the scammers in March and May 2022.
- Payments were only made in 6 of the 12 months. There were:
  - 2 months with more than one payment:
    - 2 in January 2023 and 5 in May 2023
  - 4 months where just one payment was made.
  - 6 months where no payments were made.
- The total spend in the 12 months was £11,390, so the monthly average was less than £1,000.

<u>Crypto transactions to the scammers in June and July 2023</u>

- In June 2023, there were 20 payments.
- In July 2023, there were 24 payments.
- The 44 payments in these two months totalled £44,209.
- The average over 2 months was £22,104.50.
- Prior to payment number 25 on 1 July 2023, there were daily payments for two consecutive weeks.
- At the point at which payment 25 was made, the rolling weekly average payment was £11,000, which was almost the total in the 12 months prior to June 2023.

I can't see that Monzo did this or any other analysis, noticed this significant contrast and increase in velocity or have provided sufficient evidence to persuade me they intervened or that the payments weren't unusual, and it wasn't proportionate for them to intervene.

If a bank doesn't question payments that might be at risk, then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, I believe it ought to have contacted Ms W, regardless of her previous crypto activity, to check she wasn't at risk of falling victim to fraud.

Monzo are fully aware of the types of scams, what they look like and what they involve such as the payment journeys that they can take. Also, crypto investment scams were well known to banks in 2023. So, even though Ms W was transferring funds to a crypto account in her name, Monzo ought to have been on the lookout for unusual transactions and patterns.

In this case I also consider payment 25, which made it £11,000 Ms W was paying in seven days, which was higher than any previous week (and transaction), to be the point they should've stepped in to probe what was happening.

I think it more likely than not that Monzo would've given automated warnings to Ms W (and signposted her to their scam warnings) when the crypto exchange companies first became payees, and these would've included information on common investment scams together with the importance of due diligence checks especially where the contact is through social media.

Despite this, I think Monzo should've given Ms W further automated warnings prior to a human intervention where the velocity started to noticeably increase, after one week of daily payments. However, considering Ms W's experience in crypto and the likelihood that similar automated warnings would've been given by Company U and Company C, I'm not persuaded these would've resonated with her.

As I think Monzo should've put in place a human intervention, I then considered, on balance of probabilities:

If a Monzo agent experienced in fraud and scam would've prevented her loss from payment 25 (the intervention trigger point)

From reviewing Ms W's dialogue with the scammers, I can't see that Ms W was influenced or coached to mislead Monzo about how she was approached and what she was investing in. So, I think Ms W would've answered probing open questions honestly. Also, I noted how she had by this point become dissatisfied with Company A having written a critical review about them.

When considering what would've likely occurred on the call, I think that before asking questions an agent would've initially said the following:

- Crypto investments were very high risk and they were seeing a lot of fraud heading to crypto platforms.
- There was an FCA warning about these very high-risk crypto investments and that Ms W should be prepared to lose all of her money.
- That scammers are very convincing encouraging customers to invest and pay release fees. And their stories are very believable, and the scam can take a long time to materialise.

They then would've likely asked fact finding questions about the company, the research Ms W had done and whether this included an important FCA check. Also, the likely returns and her ability to withdraw.

I think, more likely than not, that:

- A fraud and scam agent would've:
  - Very quickly picked up on scam risk indicators such as payments going to a wallet Ms W didn't control, returns sounding too good to be true, lack of company internet presence and basic Companies House and FCA checks.
  - Become highly suspicious that a scam was occurring.
  - Completed a quick FCA and Companies House check (or blocked the payment whilst Ms W did) and these would've immediately shown Company A wasn't authorised / registered and Ms W was likely being scammed.

    - Blocked any further payments.

- Ms W would've listened and cancelled any further payments.

So, having considered the above, I think it's reasonable to assume that, had a human intervention taken place at payment 25 asking probing questions and giving a clear warning that it was likely she was being scammed, the scam would've been unravelled.

I've also thought about whether Ms W did enough to protect herself from the scam, and I don't think she did.

Although I appreciate Ms W found the scammer very convincing, I think she ought reasonably to have completed the due diligence described above and not relied upon a search engine. Also, as she had concerns about the investment and Company B's withdrawal processes, messaging and location, I think she should've sought independent financial advice from a qualified and approved financial advisor. In addition, Ms W had crypto experience and I think she should've been concerned that a third-party wallet address would be going to another individual rather than her own trading account.

Considering all the above, my findings are that Monzo should've intervened, this would've more likely than not unravelled the scam and prevented further loss and that there was contributory negligence from Ms W.

In a situation where both the customer and the business are equally at fault, I think it is only fair and reasonable for liability to be shared from the point – which I consider to be payment number 25 – the payments to the scammer would've likely been stopped.

Finally, regarding Ms W's claim for compensation, although I think Monzo should've done more here, as it is the scammers that caused her distress and inconvenience, I don't think it would be fair and reasonable to require them to make such a payment.

Putting things right

So, having considered the above and all the information on file, I'm partially upholding this complaint, and to put things right I think a fair and reasonable refund amount should be 50% of £32,209 (see sub-total 2 in above table) – so Ms W should receive £16,104.50, plus interest at 8% per annum.

My final decision

My final decision is that I partially uphold this complaint against Monzo Bank Ltd, and I require them to provide Ms W with:

- A refund of £16,104.50.
- Plus, simple interest at 8% per annum from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms W to accept or reject my decision before 1 November 2025.

Paul Douglas
Ombudsman