

The complaint

Mr W complains that The Co-operative Bank Plc ('Co-op') hasn't refunded the money he lost to an investment scam.

What happened

The circumstances of the complaint are well-known to both parties, so I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

Around the start of June 2023, Mr W began communicating with a third party ('the scammer') he'd met on an online dating website. Mr W and the scammer would exchanged messages using an instant messaging service and spoke regularly on the phone – including via video call. This persuaded Mr W that he and the scammer were in a genuine romantic relationship.

The scammer advised Mr W to invest through an investment platform they were having success with. The scammer helped Mr W open an account with the investment platform and a digital wallet with a well-known cryptocurrency exchange – which I'll refer to as 'O'.

Between 13 June 2023 and 9 August 2023, Mr W purchased cryptocurrency from four different cryptocurrency exchanges. The cryptocurrency was deposited into his digital wallet with O and Mr W transferred it to the scammer, believing he was crediting his account with the trading platform. Unfortunately, the trading platform was fake, and Mr W lost his money.

The scam payments are as follows:

Payment	Date	Amount	Payment type	Merchant
1	13/06/2023	£100	Faster payment	1
2	03/07/2023	£1,920	Faster payment	2
3	07/07/2023	£1,500	Faster payment	3
4	11/07/2023	£3,700	Faster payment	3
5	21/07/2023	£4,300	Debit card payment	4
6	21/07/2023	£4,310	Debit card payment	4
7	25/07/2023	£1,650	Debit card payment	4
8	27/07/2023	£7,500	Debit card payment	4
9	31/07/2023	£3,270	Debit card payment	4
10	01/08/2023	£5,200	Debit card payment	4
11	03/08/2023	£4,000	Debit card payment	4
12	07/08/2023	£3,190	Debit card payment	4
13	09/08/2023	£2,415	Debit card payment	4

To fund the debit card payments, Mr W took out personal loans, with six different providers, totalling £28,000.

On 9 August 2023, Mr W reported to Co-op that the fake investment platform had scammed him, and he subsequently made a complaint regarding this. Co-op investigated Mr W's complaint but declined to reimburse the faster payments Mr W had made. However, Co-op thought it could've done more to prevent Mr W from making the debit card payments and so it reimbursed 50% of those payments (along with an additional £50 that was paid in error).

Unhappy that Co-op didn't reimburse his loss in full, Mr W referred his complaint to this service. Our Investigator didn't uphold the complaint. They didn't think Co-op could've prevented Mr W from making the scam payments or done anything differently to recover his funds. As a result, they didn't think Co-op needed to do anything more to resolve the complaint.

Mr W didn't accept our Investigator's opinion. He said Co-op hadn't given him sufficient warnings to help him identify that he was being scammed and should've reimbursed him in recognition of this failing.

As an agreement couldn't be reached, the complaint has been passed to me to decide.

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 in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account.

It's not in dispute that Mr W made the scam payments and knew funds were leaving his account. So, the payments were authorised and under the Payment Services Regulations, the starting position here is that Mr W is responsible for the payments (and the subsequent loss) despite the payments being made as the result of a scam.

However, that isn't the end of the story. Good industry practice required Co-op to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

Based on the amounts and frequency of payments 1 to 3, I wouldn't reasonably have expected Co-op to have been concerned that Mr W was at risk of financial harm from fraud when those payments were made. So, I wouldn't expect Co-op to have taken any steps to confirm the payments were being made for a genuine reason.

However, payment 4 was identifiably going to a cryptocurrency exchange and took the total sent to cryptocurrency in the space of nine days to over £7,000, which demonstrated a fraud risk. In those circumstances I'd have expected Co-op to have provided Mr W with a written warning which covered off the common features of a cryptocurrency investment scam.

I'd also expect Co-op to have provided a similar written warning when payment 5 was made. But when a second high value payment to the same cryptocurrency exchange was made later that same day, I'd have expected Co-op to have been concerned that Mr W was at increased risk of financial harm from fraud and it should've spoken to Mr W to ask him questions about what he was doing, to ensure the payment wasn't being made as part of a scam, as it should've done for several of the debit card payments.

When Mr W made payment 2, Co-op says Mr W had to verify the payment by responding to a text message it sent him, which he did. In the circumstances, I'm satisfied that was a proportionate response to the risk demonstrated to Co-op at the time.

When Mr W made payment 3, Co-op thought the payment was suspicious and it blocked it. Mr W had to call Co-op to speak to the fraud department to discuss the payment before it was released. During that call, Mr W didn't give accurate answers to Co-op. Rather than saying he was making the payment as part of an investment, Mr W told Co-op that he was sending funds to a relative in Germany, who needed financial assistance in moving house.

Mr W has confirmed that the answers he gave to Co-op had been given to him by the scammer and he was simply following their instructions, believing that the advice he was given was in his own best interests. Mr W expressed his frustration to Co-op that the payment had been blocked and that he was having to answer questions about it. He also explained that if Co-op didn't make the payment, he would find another way of sending the funds.

Given the purpose Mr W gave was plausible and he confirmed he was comfortable making the payment, despite the generic scam warnings Co-op gave him, Co-op released the payment. In the circumstances, I don't think co-op acted incorrectly and its response to the risk was proportionate.

Co-op also blocked Payment 4. Although I think a proportionate response to that payment would've been a written warning, Co-op deemed it necessary to speak to Mr W about the payment and he had to call Co-op to discuss the payment further.

This time, Mr W said he was making the payment to purchase United States Dollars ('USD'), so he could purchase building materials from abroad. Mr W has explained that when he spoke to Co-op, the scammer was listening in to the call.

Mr W was making a payment to a cryptocurrency exchange, which does allow users to exchange one fiat currency for another, for example exchanging Sterling ('GBP') for USD. However, as the payment was identifiably going to a cryptocurrency exchange, I'd have expected Co-op to have explained the common features of a cryptocurrency investment scam to Mr W, which it didn't do.

I can't say for certain what would've happened if Co-op had provided a more detailed warning about cryptocurrency investment scams – and that's because Co-op's warnings were generic and lacked detail. However, I must consider whether the available evidence shows that it was more likely than not that Mr W would've acted differently if Co-op had intervened more appropriately. Whilst I don't think Co-op did enough to warn Mr W about the common hallmarks of a cryptocurrency investment scam, I'm not as persuaded as I'd need to be that Mr W would've acted differently or could've been prevented from sending the funds to the scammer. I say this for several reasons, which I'll explain below.

When making payment 4, Mr W was following the advice of the scammer – someone he believed he was in a romantic relationship with and who was listening in to the call. The scammer had told Mr W about their own successes on the fake investment platform and Mr W believed he too had made successful returns. Mr W had been sending screenshots of what he was doing when opening accounts and making transactions and the scammer was telling him what to do at each stage. So, Mr W was being heavily coached. Not only this, but the scammer had previously told Mr W how to answer Co-op's questions and was listening in to the conversation between Mr W and Co-op.

By his own admission, Mr W thought he was in a trusting and loving relationship with the scammer and didn't know they were actually manipulating him. The messages between Mr W and the scammer which have been shared with this service suggest that Mr W truly believed he was in a serious relationship with the scammer and therefore had no reason to doubt the advice and instructions he was receiving. Mr W was frustrated that Co-op had blocked the payment (and the previous payment) and so I'm not persuaded a cryptocurrency investment scam warning from Co-op would've resonated with Mr W at the time and he would, more likely than not, have continued with the payment regardless, such was his belief that the scammer (and the fake investment platform) was genuine. This point is reinforced by the fact that Mr W was willing to borrow £28,000 from loan companies in order to fund his investment payments.

When a subsequent payment for over £8,000 was attempted by Mr W, the payment was blocked and Mr W had to speak to Co-op about it several times, including visiting his local Co-op branch on more than one occasion. Mr W did disclose that he was trying to make the payment for an investment, but other answers he gave weren't accurate – for example saying he wasn't being coached, he wasn't buying cryptocurrency, he'd heard about the investment opportunity from uncles and cousins who'd been using the same investment platform for several years and those relatives had made successful withdrawals.

During those exchanges with Co-op, Mr W again explained that he was frustrated with Co-op's attempts to protect him from fraud. He advised that he was considering ending his customer relationship with Co-op and if Co-op wouldn't let him send the funds, he would find another way to move his money. Co-op wasn't satisfied the payment was being made for a genuine reason and the payment was declined. But this didn't deter Mr W from continuing to make scam payments via a different method.

Mr W has explained that he didn't appreciate that Co-op was attempting to protect him from fraud when it blocked his payment attempts, and he believed Co-op was picking on him by not letting him do what he wanted to do with his own money. As a result, Mr W made the remaining scam payments to a different cryptocurrency exchange via debit card payments to avoid them being flagged as suspicious by Co-op.

Although he hasn't raised this with Co-op, it would appear that Mr W may have made further scam payments as the result of his relationship with the scammer. I say this because Co-op spoke to Mr W about several payments he made to a single beneficiary between October 2023 and November 2023, which Mr W said were being made for car parts. But it seems these were, in reality, payments to a new cryptocurrency exchange. So, this strongly suggests that despite reporting the investment scam to Co-op, Mr W continued making payments on the advice of the scammer and gave incorrect answers about the reason he was making those payments, having failed to identify that the scammer wasn't genuine and had been involved in him already losing a significant amount of money.

I accept that during the scam, Mr W wasn't provided with adequate cryptocurrency investment scam advice from Co-op – and the debit card payments he made weren't flagged as suspicious. I accept the possibility that Mr W would've been receptive to better scam warnings. But I'm also mindful that when Co-op questioned him, he didn't provide accurate answers, preventing the romance / investment scam from being identified. He was also very insistent that Co-op allow him to make the payments he was trying to make and if it didn't, he would find another way to send the funds.

I'd like to assure Mr W that I've thought very carefully about whether more appropriate interventions from Co-op could've prevented the scam. But based on the evidence I've seen, I don't think Co-op could've stopped him going ahead with the scam payments, such was his belief that the scammer was genuine. I've seen little evidence to suggest at the time the payments were made that Mr W had any doubts that either the scammer or the investment platform weren't legitimate and I'm not persuaded appropriate cryptocurrency investment scam warnings would've given Mr W enough doubt to stop him going ahead with the scam payments.

As a result, I'm not persuaded interventions from Co-op would've ultimately prevented his loss, as I don't think warnings would've been able to overcome the belief Mr W had that the scammer was genuine. For this reason, I don't think Co-op can be fairly held responsible for reimbursing Mr W for not preventing the scam payments being made.

Mr W's scam payments all facilitated the purchase of cryptocurrency which Mr W received and forwarded on to the scammer. So, I wouldn't have expected Co-op to have attempted to recover the faster payments from the beneficiaries. I also don't think Co-op could've reclaimed Mr W's funds from the debit card payments via a chargeback.

There is no statutory right for a chargeback to be raised and a chargeback is not an absolute right for consumers. Here, the debit card payments went to a genuine merchant – and there's been no suggestion that Mr W didn't receive the cryptocurrency he paid for. So, a chargeback against the merchant wouldn't have had any reasonable prospect of success and would've most likely been defended.

I wouldn't expect Co-op to raise a chargeback that had little prospect of success. As a result, I don't find that Co-op acted unfairly in not raising a chargeback about the debit card payments. So, I'm satisfied that Co-op couldn't have reasonably done anything further to recover Mr W's loss.

Co-op agreed it could've done more to prevent the debit card payments being made and refunded 50% of the loss from those payments. I agree Co-op reasonably ought to have done more to prevent those payments being made, but even if it had taken steps to question the debit card payments and warn Mr W about cryptocurrency investment scams, I don't think he would've been receptive to any warnings and would've likely made the payments in any event. As a result, I think Co-op's partial refund of the debit card payments is more than fair in the circumstances.

I accept that Mr W has been taken advantage of and fallen victim to a ruthless scam, orchestrated by someone he thought he was in a genuine romantic relationship with. I don't doubt that the whole ordeal has been very distressing for him. However, I'm not persuaded Co-op could've reasonably been expected to prevent the loss or done anything to recover Mr W's funds. As a result, I can't fairly hold Co-op responsible for reimbursing Mr W's loss.

In its submission to this service, Co-op offered to pay compensatory interest on Mr W's refund. If that additional payment hasn't been made already, then Co-op should do this, but I'm not directing Co-op to do anything more than it's already offered to do to resolve this complaint.

My final decision

For the reasons explained above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 3 July 2025.

Liam Davies
Ombudsman