DRN-4727837

The complaint

Mr H complains that The Co-operative Bank Plc (Co-op) won't refund money he lost in an investment scam.

What happened

What Mr H says:

Mr H says his wife saw an advert for bitcoin investments on Facebook. It was apparently endorsed by a TV finance personality. Mr H clicked on a link and was put in touch with an 'investment firm' (which I will call 'A'). The firm gave him an account manager who said he would teach Mr H how to trade. Mr H told us he had no investment experience. Nor did he do any research into the firm A. He considered the website and trading platform to look legitimate.

Mr H had to open an account with an online bank (which I will call 'B'). He gave access to his devices by agreeing to download screen sharing software. He put a small amount of money in to start with; followed by larger sums. He received a withdrawal of euro1,000 (£860) – which gave him confidence the scheme was genuine.

He was persuaded that he was making large profits and made more payments. Firm A told him he could make profits of £200,000 on an investment of £10,000. The money was sent to his account at the online bank, and from there to the crypto exchange to apparently buy crypto currency.

Mr H told us he gave control over his account at B to the scammers. He made total payments of £25,218 from his Co-op account to his account at B. He paid a management fee of £219 to firm A. He also borrowed £10,000 to put into the scheme (**continued):**

	Date	Payment	Amount
1	5 June 2023	Debit card – firm A's fee	£219
2	6 June 2023	Faster payment to Mr H's account at B	£1,600

3	13 June 2023	Faster payment to Mr H's account at B	£3,450
Credit	22 June 2023	Credit – loan drawn	(£10,000)
4	27 June 2023	Faster payment to Mr H's account at B	£9,900
5	28 June 2023	Faster payment to Mr H's account at B	£100
6	17 July 2023	Faster payment to Mr H's account at B	£9,949
	Total payments		**£25,218**

Mr H realised he had been scammed when A contacted him to say the value of his investment was euro91,000. When he wanted to withdraw the money, he was told he had to pay a fee of euro18,000. This was said to be the firm's commission. The website, and his 'investment account' was fake.

Mr H made payments from his account with firm B totalling £25,099.

Mr H contacted Co-op on 1 September 2023 to report the scam. He also contacted firm B, which rejected his claim – and that complaint was also referred to this service.

Mr H complains – he says Co-op should have done more to protect him. He says he didn't get any warnings about the payments from his Co-op account. The payments were unusual for him to make. Co-op had a responsibility to protect him and failed to do so.

Mr H says Co-op should refund the money he's lost.

What Co-op said:

Co-op rejected Mr H's claim for a refund. The bank said:

- The payments made weren't flagged by their fraud detection systems as being suspicious.

- But he was sent a warning when he set up the transfers. However Co-op couldn't provide evidence of the warnings.

- The funds were sent to an account at firm B in Mr H's name and from there to the scammers. So, it was from firm B where Mr H's losses occurred.

- The chargeback for the fee of £219 was unsuccessful.

Our investigation so far:

Mr H brought his complaint to us. Our investigator initially upheld it. She said Co-op should've intervened in the payment of £9,900 on 27 June 2023. She said Co-op should refund 50% of the payments from that time – so should refund £10,019.

But, after further reviewing the complaint concerning firm B, she concluded that as Mr H

ignored the warnings given by that bank, if Co-op had intervened – he would likely have also rejected any warnings from Co-op. So, she didn't uphold Mr H's complaint or recommend any refund.

Mr H disagreed. He said:

- Co-op should've flagged the transactions as unusual or suspicious.

- As his main bank, Co-op had a deeper understanding of his account usage and banking relationship.

- Because of this, he said any warnings from Co-op would've been taken more seriously by him.

- Therefore, if Co-op had intervened, the payments wouldn't have been made and his losses prevented.

Mr H asked that an ombudsman look at his complaint. And so it has come to me to make a final decision.

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.

I'm sorry to hear that Mr H has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr H didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. 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 Co-op 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 make 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.

I need to decide whether Co-op acted fairly and reasonably in its dealings with Mr H when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary– and in this case, the payments were made from the Co-op account to Mr H's own account with online firm B.

The first consideration here is: if the payments were of a sufficient size and was out of character with how Mr H normally used his account – then we would expect Co-op to have intervened and spoken to him about some or all of them. I looked at Mr H's account from January 2023. And it's fair to say that some of the larger payments were unusual compared to the way in which he used his account – which was to make day to day expenditures of low value. Mr H did make some payments, but these were generally below £1,000, and normally in the region of £500 to £600 or less.

But - there's a balance to be made: Co-op has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think Co-op acted reasonably in processing the lower value payments up to and including the third payment (£3,450).

But after that – it's reasonable to say that the larger payments (starting with the fourth payment for £9,900) were unusual for him and therefore Co-op should've intervened in that one and thereafter. Co-op say they provided some online warnings – but can't provide the evidence for that. So, I must consider that they didn't provide any warnings.

Co-op was the expert in such matters and if they'd intervened, held the payments and contacted Mr H we would have expected them to ask open questions such as:

- Why are you making the payment?
- Who to?
- For what purpose?
- How did you hear about the investment?
- How were you contacted about it?
- Where did the money come from that you're investing?
- Where is the money going to from your account with firm B – to 'bitcoin'?
- What do you know about bitcoin investing?
- Have you made bitcoin investments before?
- How were you given the bank account details where the money was to be paid to?
- Have you given control on your devices to anyone else?

Co-op would've found out that Mr H had found the advert on Facebook and the contact had originated from the internet. The bank would've found out he was using an investment firm A, and he had been promised very large returns - which were too good to be true. And – he had given control of his devices to the scammers.

Mr H said Co-op should've known firm A was fraudulent – but I don't agree with that. I couldn't find any warnings on the internet for that period about firm A. The Financial Conduct Authority published a warning about A in November 2023 – after the scam took place. So - I don't think Co-op could've had any knowledge or said anything specific about firm A.

But – it is reasonable to say that Co-op should've given warnings to Mr H about the risks he was taking; even though the further payments were then being made from his account with B.

What would Mr H's reaction have been to any warnings from Co-op?

This brings me to the crux of this decision – whether (if Co-op had provided warnings) he would've taken notice of those warnings and stopped the payments. I must form a view about this.

And here (as our investigator did), I looked at the evidence from firm B in connection with the complaint that we reviewed. I found the evidence compelling – that Mr H would've gone ahead despite any warnings that Co-op may have given.

I can see that on 13 June 2023, firm B declined two payments for crypto purchase – each for £3,450. But, after those declines, 50 minutes later - Mr H made the same payment again using firm B's 'push to card' process. So – he found another way to make the payment.

On 28 June 2023, firm B again declined two payments for £5,000 and £4,980. A few minutes after that, Mr H made two payments for £5,050 and £3,737 using the 'push to card' method again. So – he found another way to make the payment.

At the same time, firm B told Mr H "*I am afraid this payment was declined due to its possible high risk nature. In this case, sadly, similar payments directed to this merchant might not get completed for the same reason".*

Then, when Mr H set up a new transfer, he was warned "*If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."*

Mr H was given messages asking him to stop and reflect. Firm B asked him what the purpose of the transfers were for – he said they were for 'goods and services' – and not investments. This was not the real reason of course. But - Mr H went ahead with the payments.

On 28 June 2023 – when Mr H's payments were blocked, on live chat he was warned *"I believe it is highly likely that the transactions you are attempting to make are part of a SCAM. We've recently spoken with another customer who attempted very similar transactions to yours - they confirmed it was a scam. Please assist me with this review, we want to keep your funds safe and secure."*

Firm B then asked he validate the transfer with a selfie. But Mr H didn't respond with that until 4 July 2023, when he was asked questions:

"Have you recently downloaded any screen sharing application….?

Were you advised to create an account (with firm B) after learning about an Investment opportunity advertised on social media?

Have you received any unsolicited calls or messages recently telling you need to move your money to a safe account or to create an account (with firm B) for investment purposes?

Are you buying cryptocurrencies"

Mr H answered 'no' to all questions - which of course, wasn't truthful.

Mr H was asked to "*confirm that you understand the risks associated by sending a selfie holding a piece of paper with the following sentence handwritten: (firm B) has warned me about the scam risks, and in the event that such utilisation leads to a scam, recovering my funds may be unlikely."* This Mr H did.

Mr H then contacted firm B and asked about the credibility of investment firm A.

Firm B said (on 17 July 2023): *"I'm sorry to inform you that our experts have told me that this website was reported as a scam. I suggest you stop using them for trading and do not use their services anymore. If you have any more concerns please do not be afraid to contact us about them."*

Despite this warning, Mr H then made two further payments from his firm B account for a total of £10,000 later that day – 45 minutes later.

So here - it seems to me that Mr H was very determined to make the payments from his firm B account - as he went ahead, despite several very significant warnings. I found this to be compelling evidence: that even if Co-op had intervened and warned Mr H, he would not have been stopped from making the payments.

I've considered what he's said about the possible impact of a warning from Co-op. But given the weight of evidence about the warnings from firm B, I'm not persuaded that Co-op could've prevented Mr H from making the payments.

Therefore, I don't hold Co-op as liable to refund any of the money to Mr H.

Recovery:
We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Co-op took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. I couldn't see that they'd contacted firm B – but I'm persuaded that had they done so, no funds would've remained – as he'd moved them onto the trading platform. Also – he didn't report the scam until 1 September 2023 – almost three months after the first payment had been made. I don't consider it was likely any funds would've remained by that time.

Chargeback:
The chargeback process is a voluntary one – customers are not guaranteed to get money refunded, and there are strict scheme rules in place by the card schemes (e.g. Visa and Mastercard) which govern chargebacks. In general terms, the chargeback can provide a refund where a customer has bought goods or a service which isn't provided or is not what was advertised. So – that isn't the case here. This was an authorised payment and a chargeback had no reasonable prospects of success.

I'm sorry Mr H has had to contact us in these circumstances. I accept he's been the victim of a cruel scam, but I can't reasonably hold Co-op responsible for his loss.
(**continued)**

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 14 May 2024.

Martin Lord

Ombudsman