DRN-3171803

The complaint

Mr W is seeking to recover around £14,800 from The Co-operative Bank Plc (Co-op); a payment he made as a result of a third-party scam.

What happened

Mr W received a message on social media from someone claiming to be a well-known presenter of a series exploring investments including bitcoin and cryptocurrency. The 'presenter' messaged Mr W and encouraged him to invest in bitcoin and offered to mine it on his behalf to increase its value.

As Mr W had seen an investment series presented by this individual recently, he was convinced it was the well- known presenter. Mr W used a forum to find a bitcoin seller and under the fraudster's instruction opened a wallet with a third-party cryptocurrency exchange to place the purchased bitcoin. Mr W shared his cryptocurrency exchange log in details and password with the fraudster on the understanding that the fraudster would mine the bitcoin on his behalf.

Mr W made the following transactions:

Transaction Value	Date
£3,000	24 June 2020
£1,500	25 June 2020
£2,900	29 June 2020
£7,418.26	3 July 2020

Initially, the investigator did not uphold the complaint. She said the complaint wasn't covered by the Contingent Reimbursement Model Code (CRM code) because it concerned a legitimate purchase and there was no loss caused in the transactions between Mr W's Co-op account and the bitcoin seller. However, she reconsidered the position and felt that the final payment Mr W made, ought to have caused Co-op concern Mr W was at risk of financial harm. She felt that if Co-op had intervened by the fourth transaction, it ought to have realised that Mr W was falling victim to a cryptocurrency scam.

Mr W still felt all four transactions should have triggered but accepted the offer to refund the final payment as outlined in the investigator's letter.

Co-op didn't agree. It said the transfers processed by the bank reached the intended destination and it cannot be held responsible for the actions of a customer thereafter. It feels Mr W's actions with regards to his bitcoin account were irresponsible and he recklessly divulged his log in details to a fraudster.

It considers that a sending firm's liability concludes when the payment instruction is executed in accordance with the customer's instruction, where that payment successfully reaches its intended destination and the amount transmitted complies with the customer's instruction.

As the case could not be resolved informally, it was been passed to me for a 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.

When considering what is fair and reasonable, I'm also 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 relevant time.

It is not in dispute that Mr W authorised the payments. Mr W was duped into sending funds from his bank account to a cryptocurrency exchange where he purchased cryptocurrency from genuine sellers. The scammers deceived him over social media into thinking he was making a legitimate cryptocurrency investment for further trading. So, although Mr W did not intend the money to go to the scammers, under the Payment Services Regulations 2017, and the terms and conditions of his account, Mr W is presumed liable for the loss in the first instance.

As the investigator explained, Mr W's complaint is not covered by the Contingent Reimbursement Model (the CRM Code). This is because the payments were made to a legitimate cryptocurrency exchange from where Mr W transferred the purchased cryptocurrency into an account in his own name with second exchange company. So, because the payment didn't go directly to the scammer from Mr W's Co-op account, it's not covered by the CRM Code.

And it doesn't automatically follow that Co-op is liable for a loss, just because a customer is a victim of fraud.

However, 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 Barclays 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.

What can be considered unusual or uncharacteristic activity clearly requires reference to common activity on the account. So, I've looked back at the account statements as far as December 2019.

The first payment did in fact flag on Co-op's systems. As a result, it sent Mr W a text message asking him to confirm the transaction as genuine. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption

to legitimate payments and it would be impossible to prevent all fraud without a significant number of genuine payments being delayed considerably and inconveniently. It remains that the payment wasn't fraud on the account itself. To the bank, it was a genuinely authorised payment. And Mr W was confirming this was the case. On the face of it, it seems to me that that there was no reason why the payment wouldn't have seemed genuine, after the check Co-op made had been carried out. I don't think there was enough suspicion about the size of the payment, that Co-op needed to do more. I think the text message it sent was proportionate in the circumstances. The two payments that followed were similar and Co-op no longer holds any records of whether these payments triggered on its systems – but by now they were to the same known payee and the amounts were relatively small – so I don't think Co-op needed to intervene at this point.

But I think the payment on 3 July 2020 was unusual and uncharacteristic for Mr W and the account. There had been no comparable legitimate payments in recent times – with the largest amount being the £3,000 on the 24 June 2020. In my opinion, the payment for £7,418 was a payment instruction that Co-op ought to have realised warranted additional checks before it simply processed it without question. I think in a situation like this Co-op should have spoken with Mr W to check everything was in order, to protect him from the risk of financial harm. I have therefore thought about what most likely would have happened if Co-op had spoken appropriately to Mr W about his instruction for the £7,418 payment on 3 July 2020, before it executed it.

As a financial services professional, I think Co-op would have been aware at the time that fraudsters use genuine firms offering cryptocurrency as a way of defrauding customers. Cryptocurrency scams had been increasing in frequency and both the FCA and Action Fraud had published specific warnings about these scams in 2018. In my view, by 2019, Co-op had had time to understand these warnings and put mechanisms in place to detect and prevent this particular type of fraud.

Whilst it may have appeared on face value to have been a legitimate payment to a legitimate organisation, and even though the money appeared to be going somewhere safe or on (as it did) from here to the consumer's own wallet, I don't think the conversation should have stopped there.

Based on the industry warnings at the time, I think Co-op ought to have had a good enough understanding of how these scams work – including that consumers often move money to a wallet in their own name before moving it on again to the fraudster or (as I understand was the case here) the fraudster having control or access to the wallet.

Co-op could have asked how the customer had been contacted, whether he'd parted with personal details in order to open a trading account, whether the investment opportunity was linked to a prominent individual, advertised on social media.

If Co-op had asked who Mr W was paying his cryptocurrency to when he was making the £7,418.26 payment, I think Mr W would have told them about the social media contact from a well-known presenter and that he had shared personal details with them including his password and Co-op would have been concerned about this. With further questioning, I think Co-op would have been on notice that Mr W was falling victim to a scam. And if Co-op had given Mr W some warnings about cryptocurrency scams; including pointing out that scam firms can manipulate software to distort prices and returns and scam people into buying non-existent currency – I think this would have caused sufficient doubt in Mr W's mind not to proceed with the payment. In other words, if the Co-op had carried out further or better questioning in line with the bank's duty of care, it seems probable that Mr W would have become credulous about the scam in time and stopped the payment in its tracks. The fraud would have been uncovered and Mr W would not have lost £7,418.26.

I've thought carefully about what Co-op's obligations were, as set out above. But another key issue is whether Mr W acted reasonably taking into account all the circumstances of the scam. So, I have also considered whether Mr W should bear some responsibility by way of contributory negligence.

However, it is clear that up to and including the time of authorising the payments, he was still totally in the dark and simply did not appreciate what he was doing or the consequences of his actions. I realise Co-op thinks Mr W's actions were irresponsible and it feels he recklessly divulged his log in details to a fraudster, but Mr W thought he was dealing with a genuine expert in cryptocurrency at this point. Mr W told us he searched the company online and found nothing of concern. As I understand it, he was also provided with a trading platform or portal in which he could view the investments increasing in value. Overall, I think this was a very sophisticated and believable scam, and I am satisfied there was no contributory negligence on this occasion, Mr W was simply the unwitting victim of a clever fraudster. The bank was the professional in financial matters; Mr W was a layperson.

In the circumstances I am satisfied Co-op should fairly and reasonably reimburse Mr W for the loss he suffered without any reduction together with interest. Mr W says he's not sure what he would have done with the money but may have bought household equipment or paid off bills. I think it's likely that he would have used his money if he had not been defrauded or spent it on other things. So, I consider it fairest to award 8% simple interest.

Putting things right

In order to put things right for Mr W, Co-op should:

- Refund the payment of £7,418.26
- Add simple interest at the rate of 8% per annum from the date the transaction was made to the date of settlement

If Co-op deducts tax from this interest, it should provide Mr W with the appropriate tax deduction certificate.

My final decision

My final decision is I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 27 May 2022.

Kathryn Milne
Ombudsman