

The complaint

Mr S complains that The Co-operative Bank Plc didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

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.

In November 2020 Mr S met someone on a dating app, who I'll refer to as "the scammer". They began to communicate regularly, building what he believed was a relationship. After several weeks, the scammer encouraged Mr S to invest in cryptocurrency and recommended an investment company I'll refer to as "T". She guided him through opening an account on Meta Trader 5 and told him to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet.

Between 17 December 2020 and 24 January 2022, Mr S made 135 transfers from his Co-operative account to two cryptocurrency exchange companies I'll refer to as "B" and "C". The payments totalled £449,461.60, and during the scam period he received 11 credits totalling £78,744.46.

In October 2021 the scammer advised Mr S to make a withdrawal as he had maximised his profits. But when he tried to withdraw his funds he was told he needed to pay taxes. The scammer tried to convince him to take out loans and borrow money to pay the tax, but he was alerted to the fact he'd been scammed by a family member and so he contacted Co-operative.

His representative said it hadn't intervened regarding any of the payments and that Mr S didn't authorise the payments as he was being deceived. But Co-operative refused to refund any of the money he'd lost. It said it had contacted the receiving banks, who had confirmed that no funds remained. It also said it had assessed the case in line with the requirements of the Contingent Reimbursement Model ("CRM") code and other industry standards, but the payments went to an account in Mr S's own name which he had access to and he was able to withdraw funds back into his Co-operative account. It said the fraud occurred from the beneficiary accounts, and as he had access to the accounts and they were in his name, it wouldn't be looking into it as fraudulent activity on his Co-operative account.

Co-operative said the payments were flagged by its fraud detection system and it told him it was concerned he could be a victim of a scam, describing the particular scam it was concerned about and how it worked. It also told him what he would need to do to be certain that he was paying a genuine person and that it thought the payment could be fraudulent.

It said conversations happened on more than one occasion and Mr S asked it not to block any future payments stating he was fully aware of the risks and had completed his own checks. It also said he had continued to use cryptocurrency platforms despite initiating a scam claim, and he didn't check the Financial Conduct Authority ("FCA") register to establish

if T was properly authorised. Had he done so he would have realised it wasn't authorised and that there was a warning it was engaged in illegal activity. It also said Mr S didn't seek any independent advice and that he acted on the instructions of the fraudster without considering the implications of what he was being asked to do.

Finally, it accepted the overall service Mr S received in respect of the complaint should have been better and it apologised for any delays, distress and or inconvenience caused.

Mr S wasn't satisfied and so he complained to this service. He accepted Co-operative had contacted him, but he was only given generic scam advice and he made many more high-value payments to B which it should have challenged. And it didn't challenge any of the payments he made to C. He said the scam payments were unusual because the account was previously used for direct debits and he thinks Co-operative was responsible for his losses from 14 April 2021 onwards.

Mr S accepted he was still in contact with the scammer when he contacted his representative in November 2021 and that she managed to persuade him to send more money to C, but he didn't forward it on to the scammer's wallet. He argued that Co-operative failed to flag these payments despite a fraud case having been raised.

He said he didn't recall checking the FCA register, but he did check the FCA warning list and he doesn't accept there was a warning when the scam started. He also checked Companies House, he didn't see any negative reviews and he was allowed to make significant withdrawals into his cryptocurrency account.

Mr S also complained that Co-operative failed to update him about his claim and his right to refer his complaint to this service was unclear. And he described the impact of the scam on his finances and personal life and the effect it has had on his mental health.

Mr S's representative argued that it's unfair that complaints are not upheld in cases where victims have misled their bank because scammers often manipulate their victims to control their actions, leading them to provide false information, as they are under the false illusion that the investment is legitimate. They said Mr S transferred £150,000 within three days through multiple transactions and Co-operative failed to take preventive measures.

My provisional findings

I explained that CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. Co-operative has said the CRM code didn't apply in this case because Mr S paid accounts in his own name and I was satisfied that's fair.

I was also satisfied Mr S 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr S didn't intend his money to go to scammers, he did authorise the disputed payments. Co-operative is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I thought about whether Co-operative could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I'd seen, the payments were made to genuine cryptocurrency exchange companies. However, Co-operative ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it did enough to warn Mr S when he tried to make the payments.

Between 17 December 2020 and 10 February 2021, Mr S made multiple payments to B, none of which were flagged for checks. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr S normally ran his account, and I didn't think they were. All the payments were to a legitimate cryptocurrency exchange, none of them were for particularly large amounts, and they weren't out of character for the usual spending on the account. So, I didn't think Co-operative missed an opportunity to intervene.

Between 13 February 2021 and 24 February 2021, Co-operative intervened in three payments for £500 and one for £2,000. During the five calls that took place, Mr S was asked probing questions about the payments including whether he'd researched the investment himself, whether he'd been contacted out of the blue, whether he'd checked he wasn't dealing with a cloned company and whether he'd responded to any adverts on social media. He was warned there was little Co-operative could do to recover the money if it turned out to be a scam.

During each of the calls, Mr S was open about the fact he was buying cryptocurrency, but he didn't mention T or disclose that he was being advised by a third-party who he'd met on a dating site. And he repeatedly asked Co-operative to treat B as a known payee in an effort to avoid calls each time he tried to make a payment. He denied having been told to lie to Co-operative, he said he was happy he wasn't dealing with a scam website, and he maintained he hadn't been approached to make the payments and it was a personal investment.

Mr S was told that binary options aren't regulated by the FCA, that genuine brokers wouldn't approach people on social media, and that if an investment sounds too good to be true, it often is. He was also given a tailored warning about investment companies and told to seek independent financial advice, and to verify the investment company. He said he hadn't checked the FCA warning list but he knew B was the world's largest cryptocurrency exchange.

I considered the interventions that took place across the five calls and I was satisfied Mr S was asked probing questions and that he was provided with warnings that were relevant to the circumstances. Unfortunately, because he wasn't open about the fact he was being advised by someone he'd met on a dating site, Co-operative was unable to identify that he was being scammed. And, unfortunately, because Mr S was so convinced that the investment was genuine, he failed to follow the advice he was given concerning additional due diligence which might have led to him discovering sooner that he was being scammed.

Since complaining to this service, Mr S had said that he was contacted by the scammer after the interventions took place, but he hadn't produced any evidence to support this claim and the information he gave to Co-operative confirmed the scam transactions happened between 17 December 2020 and 20 October 2021. Because of this, I was satisfied, on balance, that he was in touch with the scammer prior to the interventions that took place in February 2021.

Mr S had complained that after 24 February 2021, he went on to make further payments to the scam without any intervention from Co-operative and that it failed to intervene in any of the payments he made to C. I accepted he repeatedly asked Co-operative not to flag the

payments to B, but soon after the final intervention the payments increased significantly in value, with transfers of £10,000 and £19,999 on 13 April 2021. And the following day he made a payment of £10,001 followed by four consecutive payments of £15,000. This represented a significant increase in value to the payments Mr S had previously made to the scam and even though B had become an established payee and Mr S had asked Co-operative not to flag the payments, the amounts had escalated to such an extent that it ought to have contacted him to ask him some more questions.

I said that Co-operative ought to have contacted Mr S again to ask him whether there was a third party involved and if so how he met them, whether he'd been promised unrealistic returns, whether he'd been told to download remote access software to his device and whether he'd made any withdrawals. He should also have been asked about the nature of the due diligence he'd undertaken and given advice on additional checks he could make to check the investment wasn't a scam.

However, there was no reason to think Mr S would have responded any differently if Co-operative had intervened again meaning it wouldn't have enough information to identify that the payments were being made to a scam. This would mean it wouldn't be able to provide a more tailored warning or any advice which would make Mr S do more research or think twice about making the payments.

Mr S didn't accept there were any warnings about T on the FCA website when the scam started. He also checked on Companies House, he didn't see any negative reviews and he had made significant withdrawals into his cryptocurrency account. All of this supported the conclusion that he believed the investment was genuine and that with limited information about the circumstances of the investment, there was very little Co-operative could have done to change the outcome if it had intervened again.

Mr S went ahead with the payments in February 2021 despite probing questions and repeated warnings from Co-operative about cryptocurrency investments. Significantly, he continued to make payments to the scam after he'd instructed a representative to look into whether he'd been scammed and while I noted his explanation that the scammer had managed to persuade him to make further payments, I was satisfied this showed he trusted the scammer and was convinced the investment was genuine.

Because of that, while I accepted that Co-operative should have intervened again during the scam period, I didn't think it would have made any difference to the outcome and so I didn't think its failure to intervene again represented a missed opportunity to have prevented Mr S's loss.

Recovery

I didn't think there was a realistic prospect of a successful recovery because Mr S paid an account in his own name and moved the funds onwards from there.

Compensation

Co-operative accepted the overall service Mr S received in respect of the complaint should have been better and it apologised for any delays, distress and or inconvenience caused. I thought this was fair and I didn't think it needed to pay any compensation.

Mr S had described the impact of the scam on his finances and personal life and the effect it had on his mental health but as this is due to the scam and not because of any failings on Co-operative's part, I said I couldn't fairly ask it to do anything further to resolve this complaint.

Developments

Mr S's representative has responded to my provisional decision, querying the statement 'if the bank intervened' and stating that it's essential to clarify that Co-operative didn't intervene.

They have argued that transfers exceeding £50,000 per day wasn't normal for the account and that standard banking protocol wasn't exercised. They've questioned whether Co-operative used all available measures and followed necessary procedures to establish if Mr S was being scammed.

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've reviewed the additional comments that have been made on Mr S's behalf and I'm afraid the findings in my final decision are the same as my provisional findings.

I accept Co-operative missed opportunities to intervene after 24 February 2021, in particular on 14 April 2021 when Mr S made a payment of £10,001 followed by four consecutive payments of £15,000. I think those payments were unusual for the account and represented a significant increase in the value of the payments Mr S had previously made to the scam.

Because I accept Co-operative missed an opportunity to intervene, I have considered what would have happened if it had intervened in order to decide whether this was a missed opportunity to prevent the scam.

As I've explained in my provisional decision, I don't think a further intervention would have made any difference to Mr S's decision to go ahead with the payments because there was no reason to think he would have responded any differently if Co-operative had contacted him again to question him about the payments. This means that if it had intervened again, it wouldn't have been able to provide a more tailored warning or give any advice which would have made Mr S do more research or think twice about making the payments.

Significantly, Mr S didn't accept there were any warnings about T on the FCA website when the scam started, he'd checked on Companies House, he didn't see any negative reviews, he'd made significant withdrawals into his cryptocurrency account and he believed the investment was genuine. Further, I remain satisfied that he went ahead with the payments in February 2021 despite probing questions and repeated warnings from Co-operative about cryptocurrency investments and that he continued to make payments to the scam after he'd instructed a representative to look into whether he'd been scammed. So, I don't think a further intervention after 24 February 2021 would have made a difference to the outcome.

Mr S's representative has questioned whether Co-operative used all available tools and measures and followed necessary procedures to establish if Mr S was being scammed and as I've explained above, while I accept it could have intervened again, I don't think this amounted to a missed opportunity to have prevented his loss so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

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 S to accept or reject my decision before 19 March 2024.

Carolyn Bonnell
Ombudsman