DRN-4752064

The complaint

Mr S complains that Lloyds Bank Plc didn't do enough to protect him from the financial harm caused by a romance 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 June 2023, Mr S received a WhatsApp message from someone I'll refer to as "the scammer" who claimed to have the wrong number. The messaging continued and over the next few weeks, they exchanged information about their jobs and families.

The scammer told Mr S that her uncle was a trader and that she invested in cryptocurrency. She showed him screenshots of her profits and told him he could make returns of 15% to 20%.

The scammer told Mr S to open an account on a trading platform I'll refer to as "L", instructing him to first purchase cryptocurrency before loading it onto an online wallet. He transferred funds to his Lloyds account and between 16 June 2023 and 13 July 2023, he made twelve faster payments and four debit card payments to seven different beneficiaries totalling £21,511.09.

Mr S believed the scammer was genuine because even though they'd never met, he'd seen what he thought was her social media page. He was also googled one of the cryptocurrency exchanges and was satisfied it was genuine and that there were no negative reviews. He was also able to view his profits on the trading platform. But he realised he'd been scammed when he tried to make a withdrawal and was told he'd have to pay an additional £8,500, which was subsequently lost to the scam.

He complained to Lloyds with the assistance of a representative, who said he didn't understand the dangers of investing in cryptocurrency, and had it intervened it would have realised there were red flags present, and the scam would have been prevented.

Lloyds said the Contingent Reimbursement Model (CRM) Code didn't apply because Mr S was sending funds to accounts in his own name. It said it intervened when he made the fourth payment, which was a faster payment for £500. Mr S said was sending money to his own cryptocurrency account using P2P trading and that he was acting alone. He was warned about the risks and told that if it was a scam, it was unlikely he'd get his money back.

In further calls on 22 June 2023 and 24 June 2023, Mr S said the payments were for home improvements and the work had been completed. And on 9 July 2023, he said he'd had to get the builders back to repair a leaking roof and to complete other jobs.

Lloyds said it stopped two further payments on 10 July 2023 when Mr S said he was making payments for cryptocurrency, and that he'd previously said he was paying for home

improvements to avoid further questioning. The call handler told him that cryptocurrency is high risk and Mr S said he understood and was acting alone.

On 11 July 2023, Mr S applied for a loan and shortly after he tried to send a faster payment for £8,981.50, which was stopped due to scam concerns. He then made two payments using his debit card before trying further payments, all of which were blocked. In a further call on 12 July 2023, Mr S said he was making the payment on his own, for his own investment and he'd completed his own research.

Lloyds argued that it intervened appropriately and that it educated Mr S about the risks of investing in cryptocurrency, but he had said he wasn't being assisted by anyone and there wasn't anything else it could have done to protect him. It said he didn't do any research into the scammer or her uncle, he didn't research L, the most recent review about O was dated in 2020, and some of the reviews were negative. Finally, it explained that it wouldn't contact the beneficiary banks for the P2P payments as the traders fulfilled their agreement to transfer the cryptocurrency, and there would be no prospect of a successful chargeback of the card payments.

Mr S wasn't satisfied and so he complained to this service with the assistance of his representative who said Mr S transferred money from his other bank accounts before sending large amounts to cryptocurrency exchanges the same day. They said this was out of character as Mr S didn't have a history of cryptocurrency payments and it's unusual to make so many high value payments to a new payee in such a short time outside of a scam. They said that Mr S told Lloyds the payments were for cryptocurrency, and had it intervened appropriately and provided scam education, it would have been obvious he was falling victim to a scam.

Responding to the complaint, Lloyds said that Mr S didn't have a contract or a portfolio, and he took the word of a stranger without checking whether L was authorised by the Financial Conduct Authority ("FCA"). It said it tried to advise Mr S, but he gave dishonest answers, stating that he'd done thorough research, he wasn't being advised by anyone, and he wasn't being coached.

Our investigator didn't think the complaint should be upheld. Analysing the calls Mr S had with Lloyds, she explained that Mr S admitted he was buying cryptocurrency and was given warnings about cryptocurrency scams in calls he had with Lloyds on 19 June 2023 and 20 June 2023. On 20 June 2023, the call handler told him that other customers had reported that the beneficiary account was fraudulent, so he decided not to make the payment and instead sent the money to different account details.

On 22 June 2023, 24 June 2023, 9 July 2023 and 9 July 2023, Mr S told Lloyds the payments related to home improvements, he hadn't been told to lie to the bank, and the payments were processed.

On 10 July 2023, Mr S accepted the payments were for cryptocurrency and explained he'd said they were for home improvements, so he didn't 'have to go through the rigmarole every time'. The call handler gave a lengthy warning about cryptocurrency scams describing how scammers get in touch with their victims, they might claim to be a trader or a broker and promise high returns and direct victims where to send the funds. Mr S confirmed he'd made the payments himself, there was no one else involved, no one had told him what to say and he hadn't been coached to lie, and the payment was processed. In a further call that day, Mr S was warned again about cryptocurrency scams, including that scammers offer unrealistic returns and ask consumers to lie to their bank.

On 11 July 2023 Mr S said he'd done some research on the company he was paying, but after a lengthy conversation, the call handler refused to process the payment. The final call occurred on 12 July 2023 when Mr S attempted to make three further debit card payments. He said the payments were for investment purposes, he was acting alone, no one had forced him to do it and he'd done research.

Our investigator commented that Mr S was asked clear, probing questions, but he gave misleading answers regarding the purpose of the payments on several occasions, which prevented Lloyds from detecting the scam. She noted that Lloyds refused to process one of the payments, but Mr S found an alternative way to pay, and he even went ahead with the payment having been told there had been reports that the beneficiary was fraudulent, so there nothing else could have done to prevent Mr S's loss.

Mr S has asked for his complaint to be reviewed by an Ombudsman arguing that Lloyds' interventions were below a reasonable standard. His representative has argued that even though Mr S was warned about cryptocurrency scams, he wasn't asked questions about what the payments were for, why he was investing in cryptocurrency, why he was sending money to so many different beneficiaries, what was happening to the cryptocurrency once it was in his wallet and why he was using his savings. Had it done so, he'd have explained that he'd been introduced to the investment by someone he met via WhatsApp and the scam would have been uncovered.

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, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr S has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

The Contingent Reimbursement Model ("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, but the code doesn't apply to payments to accounts in the consumer's own name, and the recipients of the P2P payments would be able to evidence that they'd transferred the cryptocurrency to Mr S.

I'm 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.

I haven't seen evidence of Mr S's communication with the scammer or evidence of funds leaving the cryptocurrency accounts. But there's no dispute that this was a scam and, in any event, I don't need to make a finding on whether Mr S lost money to this scam because I'm not satisfied that Lloyds missed an opportunity to prevent his loss.

Prevention

Lloyds 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.

I've thought about whether Lloyds did enough to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments

were made to genuine cryptocurrency merchants. However, Lloyds ought to fairly and reasonably be alert to fraud and scams, so I need to consider whether it ought to have intervened to warn Mr S when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Lloyds to intervene with a view to protecting Mr S from financial harm due to fraud.

Lloyds intervened several times during the scam period and so I've considered whether the interventions were proportionate and whether there was anything else it could reasonably have done to prevent Mr S's loss.

The first three payments were low value and so even though Mr S was sending funds to a cryptocurrency exchange, there would have been no reason for Lloyds to intervene. The fourth payment was £500 to a P2P seller and during a call Mr S had with Lloyds, he said he was buying cryptocurrency, and he hadn't been coached to lie. He was given a warning about cryptocurrency scams and the payment was processed. I've considered whether this was proportionate in the circumstances, and I'm satisfied that it was.

Payment 5 resulted in a call where Mr S said he was buying cryptocurrency from a P2P seller and explained they were verified by the cryptocurrency merchant. Mr S was advised that the beneficiary account might be a scam, and he said he would try to use a different seller and subsequently sent the funds to a different beneficiary. I've considered whether Lloyds did enough on this occasion and while I think it should reasonably have asked Mr S some more probing questions about the payment including why he'd been planning to pay that particular seller, because he told lies two days later and denied any third party involvement when asked on 10 July 2023 and 12 July 2023, I think it's unlikely he'd have disclosed anything concerning about the circumstances. So, I don't think more detailed questioning would have stopped the scam.

The next four interventions happened on 22 June 2023, 26 June 2023, 9 July 2023 and 9 July 2023. Each time, Mr S lied about the purpose of the payments and Lloyds failed to uncover the scam. I've considered whether there was anything else it could have done and as it wouldn't have been obvious that he was buying cryptocurrency, I don't think there was anything else it could reasonably have done.

On 10 July 2023, Mr S had two calls with Lloyds about payments he was trying to make to "U". He told the call handler he was buying cryptocurrency, and he'd lied in the earlier calls to avoid answering questions about the payments. He was given a very lengthy, clear and detailed warning about cryptocurrency investment scams and the payment was processed.

I've considered whether Lloyds did enough at this point, and I'm satisfied the call handler asked Mr S whether he'd received advice from a third party and whether he'd been coached to lie. He sounded very knowledgeable, describing how he found the seller through the app, which was regulated. He also seemed sure that he understood the risks involved. So, I don't think it was unreasonable that the payment was processed.

Mr S received loan funds into the account and tried to make a faster payment to B for £8,891.50 on 11 July 2023. That payment was blocked and in a lengthy call with Lloyds, Mr S said the payment was for cryptocurrency, it was a P2P trade with a professional seller, he'd done some research, and he had a friend who'd used them. He admitted he'd taken out a loan to fund the payment and explained that he was trying to withdraw his investment and pay back to loan. After a lengthy conversation, the call handler refused to process the payment due to concerns about the payee, the fact the payment was being funded by a loan, and the risk that the payment might be part of a scam.

Following this, Mr S made multiple attempted card payments to “B” which were declined before he managed to successfully send £1,200 to “M” via open banking on 11 July 2023. He then made two debit card payments to B for £4,035 each. Lloyds didn’t block these payments and arguably it should have done because they were high value payments to a cryptocurrency exchange. But it had already asked probing questions and providing detailed warnings in respect of the attempted payment for £8,891.50, and so it’s not unreasonable that it didn’t do so again. And even if it had done, I think he’d have continued to make payments to the scam.

The final call happened on 12 July 2023 when Mr S said the payments were for investment purposes, he was acting alone, no one had forced him to do it, and he’d done research. The payment was processed and, based on Mr S’s responses to the questions he was asked, I’m satisfied that was reasonable.

Mr S didn’t realise he’d been scammed until he was unable to access his profits, and his trading account was frozen. I note Mr S’s representative’s comment that Lloyds had gave Mr S a lot of warnings but didn’t ask probing questions and I agree with this to an extent. But even if he’d been asked more questions, I don’t think he’d have mentioned that he was investing on the advice of a third party that he’d met online, or anything else which might have indicated that he was being scammed.

Mr S was so confident that the investment was genuine that he simply sent the funds to a different seller when he learned that he was paying a fraudulent account, he misled Lloyds about the purpose of the next four payments to avoid lengthy questioning, he went ahead with investment following several detailed warnings about cryptocurrency scams which should reasonably have resonated with him, and towards the end of the scam he applied for a loan to fund the payments and became angry when the call handler refused to process the payment due to scam concerns. So, I don’t think there was anything else Lloyds could reasonably have done to prevent his loss.

Recovery

I don’t think there was a realistic prospect of a successful recovery because Mr S either paid accounts in his own name and moved the funds onwards from there, or he sent funds to cryptocurrency sellers and received the cryptocurrency he paid for.

I’ve thought about whether Lloyds could have done more to recover Mr S’s payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two ‘presentments’. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa’s arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Lloyds) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr S).

Mr S’s own testimony supports that he used cryptocurrency exchanges to facilitate the card payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It’s most likely that the cryptocurrency exchanges would have been able to evidence they’d done what was asked of them. That is, in exchange for Mr S’s payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I’m satisfied that Lloyds’ decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr S to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think he is entitled to any compensation.

I'm sorry to hear Mr S has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Lloyds is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined 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 S to accept or reject my decision before 15 July 2025.

Carolyn Bonnell
Ombudsman