

The complaint

Mr W complains that Lloyds 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.

Mr W was the victim of an investment scam. In August 2023, he met someone on a dating site, who I'll refer to as "the scammer". The scammer told Mr W she invested in cryptocurrency and that she'd spent many years doing it, having learned about it from her father. She showed him screenshots of her successful investments and explained she'd used a trading platform I'll refer to as "M".

The scammer told Mr W she'd show him how to invest and encouraged him to open accounts with M, and a trading wallet I'll refer to as "L". She told him to first purchase cryptocurrency through M, and then load the cryptocurrency onto L. Between 29 August 2023 and 15 September 2023, he made seven payments to M totalling £27,650 using a debit card connected to his Lloyds account.

On 30 August 2023, Mr W successfully withdrew £74 from the platform, but when he later tried to make a larger withdrawal, the scammer said he'd have to pay 10% of his profit, which he paid on 1 September 2023. He realised he'd been scammed when the scammer told him he'd have to pay tax on his profits, and he didn't receive any funds.

Mr W contacted Lloyds, but it refused to refund any of the money he'd lost. It said Mr W had authorised the payments and the Contingent Reimbursement Model (CRM) Code didn't apply to debit card payments or payments into accounts in the customer's own name. It also said it couldn't raise a chargeback request because the service that was offered was provided. And the payments weren't suspicious or unusual because he'd made large payments previously and there were enough funds in the account to cover each payment. It also said Mr W should have done more checks before investing his money.

Mr W wasn't satisfied and so he complained to this service. He said Lloyds failed to protect him when he made the payments, and it should have intervened as he made large payments to new payees in a short space of time.

Lloyds maintained the payments were in line with the usual activity on the account and Mr W didn't do sufficient due diligence. It said he accepted what he was told by the scammer at face value, he was swayed by improbable returns (when he tried to withdraw his profits, he believed the balance on the account was \$46,000) and didn't try to verify who he was speaking to before he made the payments. It also said he should have questioned why he needed to make further payments to make a withdrawal.

Our investigator thought the complaint should be upheld. He thought payment three on 31 August 2023 was unusual because Mr W hadn't previously paid cryptocurrency merchants, and £10,000 was unusual for the account. He said Lloyds should have called Mr W to ask tailored questions about the payment and had it done so, he'd have mentioned the scammer and Lloyds would have provided a meaningful scam warning.

He thought Lloyds should refund the money Mr W had lost from that payment onwards, but that the settlement should be reduced for contributory negligence because he didn't think he performed enough due diligence. He commented that Mr W had placed his trust in someone he'd met online and there were multiple warnings and negative reviews online about M.

Mr W asked for his complaint to be reviewed by an Ombudsman. He said he thought the investment was genuine, and he did do some due diligence before he made the payments. He said it wasn't fair to ask him to share liability because Lloyds failed to safeguard his account.

My provisional findings

I explained 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 W says he's fallen victim to, in all but a limited number of circumstances. Lloyds has said the CRM code doesn't apply to debit card payments or payments to accounts in consumer's own name, and I was satisfied that's fair.

I was satisfied Mr W '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 W is presumed liable for the loss in the first instance.

There's no dispute that this was a scam but although Mr W didn't intend his money to go to scammers, he did authorise the disputed payments. 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.

Prevention

I thought about whether Lloyds 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 a genuine cryptocurrency exchange company. However, Lloyds 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 ought to have intervened to warn Mr W 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 W from financial harm due to fraud.

The payments didn't flag as suspicious on Lloyds' systems. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr W normally ran his account and I thought they were. All the payments were to a legitimate cryptocurrency merchant, and the first two payments were relatively low value, so I didn't think Lloyds needed to intervene. However, I thought Lloyds ought to have intervened when Mr W paid £10,000 to M on 31 August 2023 because the amount was unusual for the account and he was paying funds to a high risk cryptocurrency merchant, which he hadn't paid before.

I thought a proportionate response would have been to provide a tailored written warning which was relevant to cryptocurrency investment scams. However, I thought carefully about whether this would have likely prevented any further loss in this case, and, on the balance of probabilities, I didn't think it would.

I would expect a written warning to have covered off some of the key features of cryptocurrency-related investment scams, including the fact victims are usually targeted via social media or email, there will often be a third-party posing as a broker or account manager, victims are often asked to download remote access software, and fake online trading platforms can appear professional and legitimate. But as the scammer was guiding Mr W from the perspective of having met her on a dating site, there was no broker or account manager involved. Further, Mr W has explained that hadn't realised that L was separate to M (hence only checking that M was legitimate) and so he wouldn't have realised he was making an onwards payment from the cryptocurrency exchange. Similarly, he hadn't been told to download remote access software, he hadn't yet encountered any difficulty withdrawing his profits, and he hadn't yet been led to believe he'd made unrealistic returns.

So, I didn't think there were enough red flags present for a warning to have resonated with Mr W. And as M was a legitimate cryptocurrency merchant, there wouldn't have been any other reason for him to suspect he was being scammed.

I also thought about whether there Lloyds should have intervened before any of the later payments, and I didn't think it should.

Recovery

Mr W has described that he paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I was satisfied there was no prospect of a successful recovery.

Mr W's own testimony supports that he used a cryptocurrency exchange to facilitate the transfers. 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 W's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that Lloyds' decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Customer service

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

Developments

Mr W has indicated that he doesn't agree with my provisional findings, specifically that a tailored written warning from Lloyds wouldn't have prevented him from making the payments. He's argued that there was no reason for him to disregard Lloyds' advice as he wasn't an experienced investor and would have followed any guidance, and that it's unfair to base my decision on an assumption of how I think he might have acted.

Mr W has questioned the comment in my provisional decision that "he hadn't yet encountered any difficulty withdrawing his profits", commenting that he tried to make a larger withdrawal on 1 September and was told he'd have to pay 10% of his profit. He's argued

that if he'd received a warning from Lloyds on 31 August 2024 (as I concluded he should have done), he wouldn't have gone ahead with the payments the following day.

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.

Mr W disputes that it's fair to reach a conclusion based on how he might have reacted to a written warning, but I've carefully considered all the evidence and reached a conclusion on what I think is likely to have happened if Lloyds had done what we'd expect it to have done, and I'm satisfied that's fair.

I've considered Mr W's additional comments, but I'm afraid the findings in my final decision will remain the same as the findings in my provisional decision. While I accept he was told he'd have to pay 10% to make a withdrawal on 1 September 2023, he hadn't encountered any difficulty withdrawing his profits before 31 August 2023, and fact remains there weren't many significant red flags present, so I don't think a warning on 31 August 2023 would have resonated with him.

I've gone on to consider whether, having had a tailored written warning on 31 August 2023, Mr W would have paused to consider what he was doing the following day when he was told he'd have to pay 10% to make a withdrawal, but I don't think he would have. As I've already explained, I don't think the written warning would have resonated with him on 31 August 2023, and so it wouldn't have been at the forefront of his mind the next day. And, while I accept the requirement to pay 10% was unexpected, the fact he paid it suggests to me he still thought the investment was genuine and I don't think a written warning the day before would have changed his mind about that.

Therefore, I remain satisfied that while Lloyds should have intervened when Mr W made the third payment, I can't fairly ask it to do anything to resolve this complaint because I don't think this represented a missed opportunity to prevent the scam.

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 W to accept or reject my decision before 20 January 2025.

Carolyn Bonnell
Ombudsman