DRN-5295233

The complaint

Miss D complains that Lloyds Bank PLC won't refund the money she lost as the result of an authorised push payment (APP) scam.

Miss D brought her complaint to this service through a professional representative and they made submissions on her behalf. For ease of reading, I'll refer solely to Miss D in this decision.

What happened

The details of the scam are well known to both parties, so I won't repeat them in full here. In summary, Miss D was contacted via WhatsApp about an investment opportunity with company C. On 27 September 2023 she made two faster payments totalling £450 to a cryptocurrency exchange account she had opened in her own name. The following day she sent a further £200. From there, she converted her funds to cryptocurrency and sent them on to the scammer.

She realised she'd been scammed when she didn't receive the promised returns, and the contact with the scammer stopped. She contacted Lloyds on 27 March 2024 but it rejected her refund claim.

It said the payments were not unusual for her account so it had no reason to intervene. And as the payments went to an account in Miss D's own name they were not covered by the provisions of the Contingent Reimbursement Model (CRM) code.

Our investigator did not uphold Miss D's complaint. He agreed Lloyds had no reason to stop Miss D from making the payments, and there was no reasonable prospect of it recovering Miss D's funds as she had already moved them from the recipient account to the scammer. He also said based on the documentation submitted to date there was no evidence of Miss D's loss and this was needed.

Miss D disagreed and asked for an ombudsman's review. She said this loss had caused her significant stress and impacted her health, plus her savings have been significantly depleted. She said the investigator is wrong not to have assessed this complaint under the provisions of the CRM code as these payments showed a higher risk of being associated with an APP scam.

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.

In broad terms, the starting position at law is that a bank such as Lloyds is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account. And in this case it is not in dispute that Miss D authorised these three payments.

But taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in September 2023 that Lloyds should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

It is in this context I do not find Lloyds can fairly be held liable for Miss D's loss. In deciding this, it's important to remember that firms like Lloyds process hundreds of thousands of payments each day. It wouldn't be fair or reasonable, nor would it be practical, for it to intervene on every single payment it processes. Firms need to strike a balance between protecting customers from financial harm and avoiding unnecessary disruption to legitimate payments.

And in this case I am satisfied that that neither the value nor the pattern of the payments ought to have caused Lloyds concern. Miss D's statements show she'd made payments of a similar or larger value. The payments did not have characteristics that indicated possible financial harm – they not drain her account, they were not made in rapid succession and they did not increase in value.

I accept they were to an identifiable cryptocurrency platform and that cryptocurrency scams have increased in prevalence, such that by the time Miss D made the payments, I'd expect Lloyds to have been aware of this elevated risk for such payments. However, that doesn't mean it ought to intervene on every and any payment that appears to be associated with cryptocurrency – as many of these payments will be legitimate. Instead, I'd expect it to take into account all the information known about the payments at the time. And as I've explained here, there wasn't enough going on for Lloyds to have reasonably been concerned.

I am aware there was an FCA warning about company C, but that was published after these payments on 12 December 2023. And more crucially, even if the warning had been live at the time, Lloyds had no knowledge that company C was the end destination for Miss D's money.

Overall, I do not find Lloyds acted unreasonably by following Miss D's payment instructions without making further checks. So I cannot find it acted unfairly towards Miss D.

To note, this service did not receive evidence to substantiate Miss D's loss but I don't need to consider that point further as I have not found Lloyds needed to take additional steps before processing the payments.

Did Lloyds do what we would expect to recover Miss D's funds?

I'm not persuaded there was any reasonable prospect of Lloyds being able to recover Miss D's funds. The payments were made to an account in Miss D's own name, and from there, she forwarded cryptocurrency to the scammer. So, there's nothing more Lloyds could have reasonably done to recover her funds.

The CRM Code

Miss D says Lloyds ought to refund her under the CRM code as there was an identifiable APP scam risk at the time of the payment journey. I'm sorry to disappoint Miss D, but I agree with Lloyds and our investigator that Miss D's claim can't be considered under the CRM code.

Whilst Lloyds is a signatory of the code, specific conditions must be met for a claim to be covered. One of those conditions is that funds go to another person. But in this case, the payments were made by Miss D to another account in her name. So, the CRM code doesn't apply, and I can't fairly or reasonably ask Lloyds to refund Miss D's loss under its provisions.

This means I am not instructing Lloyds to refund any money to Miss D. This is a difficult decision to make, I'm sorry Miss D lost a considerable amount of money which was very distressing for her. I can understand why she would like to be compensated for her losses. But I can only consider whether the bank, which had no involvement in the scam itself, should be held responsible for what happened. For the reasons set out above I do not find Lloyds can fairly be held liable in the circumstances of this case. Similarly, I have also found no grounds to award the £1,000 compensation she requested.

My final decision

I am not upholding Miss D's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 1 May 2025.

Rebecca Connelley
Ombudsman