DRN-3407575

The complaint

Mr H complains that Lloyds Bank PLC won't refund money he was tricked into transferring to a fraudster.

What happened

Mr H became involved with what he believed to be a genuine investment opportunity. He was shown a trading platform that he says used algorithms to place trades on his behalf. After a small initial deposit of £300 in early 2020, Mr H was encouraged to deposit increasing sums with the fraudsters.

Mr H's investments seemed to be doing well until March 2021, when his balance suddenly dropped and he started having difficulty contacting the investment company. Mr H asked to withdraw his money but was told it was unsafe to do so. Within a couple of weeks his investment had been reduced to nothing.

Unfortunately for Mr H, he hadn't been dealing with a genuine investment company, but fraudsters.

From his account at Lloyds he made five payments totalling £14,693.70 to the fraudsters – a mixture of international payments and those made through 'Open Banking'.

Mr H reported the matter to Lloyds, but it said that it couldn't refund the payments he made as, though it is a signatory of the Lending Standards Board Contingent Reimbursement Model "CRM Code", which requires firms to refund victims of APP scams in all but a limited number of circumstances, the payments Mr H made weren't covered as they were either international payments or made through Open Banking and to a cryptocurrency wallet held in Mr H's name.

It also didn't think that the activity which took place on Mr H's account was particularly out of the ordinary, so it had no reason to intervene before allowing the payments to take place.

The matter was referred to our service and one of our investigators didn't uphold it. They agreed that the payments weren't covered by the CRM Code and there was no reason for Lloyds to find them suspicious as Mr H had made payments of similar amounts to the disputed payments.

Mr H's representatives disagreed. In summary, they said:

- Banks ought to have been aware of the risk of cryptocurrency trading since at least the middle of 2018 and ought to have found new payments made to cryptocurrency providers suspicious.
- Though Mr H had made payments of similar amounts to the ones in dispute, all those payments were to accounts in his own name and wouldn't carry the same risk as a payment to a new international payee or cryptocurrency website.
- By January 2021, Mr H had made a series of high value payments to international

payees and a cryptocurrency website. This ought to have caused the bank concern.

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.

There's no dispute that Mr H authorised the payments in dispute. So, under the Payment Services Regulations 2017, he is presumed liable for the loss in the first instance.

But that's not the end of the story. I've first considered whether the payments should be considered under the CRM Code.

There's little dispute that international payments are excluded from the Code. Open Banking was used to make the other payments. In practical terms this meant the faster payment from Mr H's Lloyds account was initiated by him from the cryptocurrency provider's own platform.

I've reviewed the cryptocurrency provider's platform and it appears to be a cryptocurrency exchange. It does not appear to hold customer funds or cryptocurrency. Therefore it's likely that rather than Mr H's using the payment as a way of funding an account in his own name, he instructed the cryptocurrency provider to transfer cryptocurrency to an external wallet held by either himself or the fraudster.

To be covered by the CRM a payment must be a faster payment, CHAPS or internal book transfer between UK-domiciled, GBP accounts. In this case, though the first step (from Mr H's bank account to the cryptocurrency provider) does meet this criteria, the second step (from the cryptocurrency provider to him or the fraudster) does not. As such, the payments are not covered by the CRM Code.

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 Lloyds 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 made 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.

I've considered the circumstances of this case carefully and I'm sympathetic towards Mr H's circumstances.

I accept that firms like Santander have been aware of the risk of cryptocurrency trading for some time and that it should be alive to the risk of scams associated with cryptocurrency. But that doesn't mean that it should question its customer about every transaction to a cryptocurrency provider. Instead, it should do so where it identifies a transaction that is otherwise out of character and unusual for that particular customer.

I've looked at Mr H's statements over the period of the scam, and six months before the first payment. Mr H's spending is generally quite modest and the balance of his account rarely exceeds £1,000, but Mr H very frequently, often more than once a day, moves money between his accounts. His statements show that this account was often funded by another of his accounts. One of those accounts – his 'Online Saver' was used to fund the disputed payments. On each occasion credits were received from the Online Saver and sent on as part of the fraud. So, while the amounts of the disputed transactions might have been greater than other, legitimate, transactions – the activity was consistent with the established pattern of funding this account from a savings account and sending that money on.

I also note that there were two payments in the six months before February 2020 that exceeded the size of the first disputed payment (though these appear to be domestic, rather than international payments).

Even so, considering those transactions and the size of the first payment, I don't think the fact it was to a new international beneficiary made it remarkable enough for the bank to have reasonably believed that Mr H was at risk of financial harm from fraud. Neither was it followed by additional payments of a similar type and nature for almost a year.

By the time the second payment took place almost a year later, Mr H had made a similar payment the year before for a similar amount. Although the third payment was for a larger amount, it went to an existing payee – the same payee that had been paid about a week before. While a series of payments to a new payee might be indicative of a scam, there was a reasonably significant gap between these two payments.

Turning to the payments made via Open Banking to a cryptocurrency provider. These payments were of similar amounts to payments by Mr H in the past and were not obviously connected to the earlier international payments. So, I don't think these payments, nor the pattern of activity overall was sufficiently concerning that Lloyds ought to have intervened before allowing the payments to proceed.

In relation to recovery, I understand the payments made through Open Banking were converted into cryptocurrency and paid to a fraudster. Therefore, I don't think there was any realistic possibility of recovery.

Lloyds did attempt to recover the three international payments, but the responses from the banks involved either said that the money had already been removed or that they would seek the permission of their account holder in order to recover it. So, I don't think Lloyds could have done any more in this regard.

I know this will be very disappointing for Mr H, but I don't think Lloyds have made a mistake by declining to refund these transactions.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 14 October 2022.

Rich Drury
Ombudsman