DRN-5319032

The complaint

Miss T complains that Lloyds Bank PLC ('Lloyds') won't reimburse the money she lost when she fell victim to a scam.

What happened

Miss T says that she was contacted by someone on a messaging app who claimed to be from a recruitment company. Miss T's details were passed on to a representative of a company I'll call M in this decision, who explained that M was an affiliate marketer for a large company and was offering a remote role. The role involved completing sets of tasks to review hotels to improve their reputation and increase bookings. Miss T didn't know at the time, but the representatives of M were scammers and M was a fake company.

Miss T was provided with a link to M's website and was asked to create her own account. She was then supported to complete tasks and advised to open an account with an electronic money institution ('EMI').

After completing some sets of tasks Miss T was advised that she needed to make payments to a cryptocurrency exchange from her EMI account to be able to withdraw funds. Miss T transferred funds from her Lloyds account to her EMI account as follows:

Payment	Date	Amount
1	04/10/23	£9,238
2	04/10/23	£8,000
Total		**£17,238**

When Miss T was asked to make further payments, she realised she was the victim of a scam and raised a claim with Lloyds.

Lloyds didn't agree to reimburse Miss T's loss. It said there was no bank error when Miss T made the transfers to her EMI account.

Miss T was unhappy with Lloyds' response and brought a complaint to this service. In summary, Miss T said Lloyds didn't do enough to protect her when the transfers were made and that she should have been asked to go into branch. Miss T also explained that the scammers gave her the cover story she gave to Lloyds and that because she wanted to get her money back, she didn't question it.

When providing this service with its file, Lloyds said that when Miss T made payment one, she chose the move my money payment reason and was provided with an onscreen warning based on this payment reason. Lloyds also spoke to Miss T about the transfer. During the call Miss T said she was transferring funds to her own account with an EMI to send to a friend abroad. Lloyds also spoke to Miss T when she made the second payment and provided scam advice.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. She said that Lloyds acted reasonably in recognising that both transfers to a new account carried a heightened risk of harm. But, when Lloyds intervened, Miss T provided misleading responses to its questions which meant Lloyds was prevented from uncovering the scam. And there was nothing Lloyds could have done to recover Miss T's funds, as they were sent to an account in her own name.

Miss T didn't agree with the investigator's findings and asked for a final decision, so her complaint has been passed to me.

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 deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

The Lending Standards Board's Contingent Reimbursement Model Code ('CRM Code') doesn't apply in this case. This is because it only applies to payments to another person, and in this case Miss T transferred funds to her own EMI account. In the circumstances, I can't apply the provisions of the CRM Code.

In broad terms, the starting position at law is that a bank like 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.

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 October 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.

Given what Lloyds knew about the payments, I've thought about at what point, if any, it ought to have identified that Miss T might be at a heightened risk of fraud.

Payment one was to a new payee and followed a transfer of funds from Miss T's savings account to her current account. It was also of higher value than previous transactions on Miss T's account. So, I consider that Lloyds acted reasonably in blocking the payment and speaking to Miss T about it.

I've listened to the call Miss T had with Lloyds at the time she made the payment. When asked the reason for the payment Miss T said it was a payment to a friend and she was sending it to the EMI (which specialises in international money transfers) because she was sending it abroad. Miss T was asked if she'd previously sent funds to the friend and advised that she had, but from an account with another bank. The Lloyds adviser checked that Miss T would get the funds back and went on to provide scam advice.
The Lloyds adviser explained that Lloyds were seeing a lot of situations where customers are called by fraudsters who persuade them that they are the bank, police or a company, and provided safe account scam education. He then discussed the fact that if Miss T had been contacted and told to move the funds or lie to Lloyds, it was very unlikely she would get them back.

Given that Miss T was transferring funds to an account in her own name that specialises in international transfers, I consider Lloyds' intervention was proportionate. In any event, given what I say about the call in respect of payment two below, I'm not persuaded further intervention would have uncovered the scam or prevented Miss T's loss.

The second transaction in the table above was highly unusual. It was the second high value transfer to Miss T's EMI account that day. So I consider Lloyds was right to block the payment and ask Miss T questions about it.

During this call the agent noted that Miss T had made the earlier transfer and asked the reason for the payment. Miss T said it was to send funds abroad without being charged and that some of the money would go to a friend (and she would get it back). When pressed for further details Miss T explained that funds were going to her business partner of five years who she trusted with her life and who was abroad sourcing a manufacturer. She provided detail about the nature of the company and what would be sold and confirmed that she and her business partner were in regular contact.

The Lloyds adviser provided scam advice and referred to high risk investment scams involving cryptocurrency where victims are advised to open another account. Miss T was asked whether anyone had prepared her for the conversation or told her what to say to make the payment go through. She confirmed that they hadn't. The adviser went on to say he asked the question (and others) because the payment method didn't offer any extra protection.

Having carefully considered the content of the second call I'm not persuaded Lloyds needed to do anything more. It asked Miss T questions to establish the reason for the payment and gave relevant scam advice. But Miss T's responses prevented Lloyds from uncovering what was actually happening, and from uncovering the scam. Whilst I wouldn't expect Lloyds to take everything a customer says at face value, I'm satisfied Miss T provided persuasive and plausible answers and that Lloyds went far enough.

I appreciate that Miss T was told to mislead her bank. Scammers often coach victims in this manner to ensure that scam payments are processed. It was for this reason that the Lloyds adviser enquired whether anyone had prepared Miss T for the conversation with him or told her what to say to make the payment go through. Whilst it would have been helpful if the Lloyds adviser explained that if Miss T had been advised what to say it was a scam, given what I say below about what Miss T was told the previous day, I'm not persuaded it would have made a difference in the particular circumstances of this case.

I'm also mindful of the fact that Miss T used her Lloyds account to transfer funds to her EMI account after another bank intervened and asked her questions about transactions she was making as part of the same scam the day before. Miss T's other bank wouldn't allow her to make further payments. During the calls Miss T had with her other bank she was clearly advised that if anyone told her to lie to or misled her bank, including giving an incorrect payment reason, it was a scam. Her bank gave her other relevant advice about cryptocurrency scams, including someone helping and that she would not be able to get her money back.

Miss T has said that Lloyds should have asked her to go into branch before processing the transactions to her EMI account. But I consider Lloyds could take comfort from the fact it was clear the funds were going to an account in Miss T's own name. And Miss T provided plausible reasons for transferring funds to her EMI account and was convincing in the calls. So I don't consider Lloyds ought reasonably to have had sufficient concerns to require Miss T to attend a branch.

Overall, whilst I'm very sorry to hear about this cruel scam and the impact of the loss, I can't fairly ask Lloyds to reimburse Miss T.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 25 March 2025.

Jay Hadfield
Ombudsman