DRN-5732466

## The complaint

Mrs F complains that Lloyds Bank PLC won't reimburse her after she fell victim to a job scam.

## What happened

The circumstances of this complaint, as well as a list of payments complained about, have been set out in detail by our investigator so I don't intend to repeat them here. But briefly, both parties accept that in around January 2024, Mrs F was approached by instant messaging by an individual purporting to offer a job opportunity. Unknown to Mrs F at the time, this individual was in fact a fraudster.

Mrs F was led to believe that the job available was related to app optimisation, and Mrs F's understanding was she would receive commission for increasing the 'rank' of sites. Mrs F was told that occasionally, through completing her work, she will receive a 'combo' task, which will increase her commission but require her to add funds first to the account via cryptocurrency, which Mrs F did. However, when she tried to withdraw funds, she was told she needed to pay tax bills. She was then told her cryptocurrency had been sent to the wrong wallet and that Mrs F would need to pay security deposits and bounty guarantees to retrieve the lost funds.

After paying a number of fees and being asked for further funds, Mrs F realised she'd fallen victim to a scam and raised a claim with Lloyds. During the scam, Mrs F made payments via peer to peer lending, direct card payments to cryptocurrency platforms and payments to an e-money account in her name (which were then transferred onwards to cryptocurrency).

Lloyds considered Mrs F's claim but didn't reimburse her. It considered it had intervened appropriately during the scam and provided warnings, but that Mrs F had continued in spite of this. Lloyds also said that its records confirmed Mrs F was required to attend branch following suspicious payments made, which she did.

Mrs F remained unhappy and referred her complaint to our service. An investigator considered the complaint and upheld it in part. She reviewed calls made to Mrs F on two dates – the first in January 2024 where Mrs F had made payments to an individual's account (via peer to peer lending). During the intervention call, Lloyds explained it had concerns the recipient account was being used for fraud. Mrs F incorrectly told Lloyds that the payment was to purchase goods, but that she would cancel it if Lloyds had concerns. This payment was therefore stopped.

Lloyds then called Mrs F again during payments made to her own e-money account in February 2024. The investigator didn't think this call did go far enough in questioning Mrs F. She noted that Mrs F was asked about cryptocurrency payments recently made and why she was moving funds to an e-money account, but was given no scam warnings and there was no further probing. The investigator therefore considered Lloyds should be held liable from this payment onwards for Mrs F's losses. However the investigator also thought there were warning signs that Mrs F should also have identified in the scam. She therefore thought a fair outcome was for Mrs F to also share 50% liability for her losses.

The investigator also noted that it appears Mrs F never attended branch as Lloyds' records suggest, as it appears she wasn't in the country at the time Lloyds state the branch attendance occurred. This was supported by Mrs F providing evidence of her flight tickets. Lloyds maintained that it appeared Mrs F had attended the branch and requested further evidence to support this wasn't the case, which has been provided. However, Lloyds hasn't provided further comments on this evidence.

As Lloyds didn't agree with the investigator's view, the complaint has been referred to me for a final decision.

**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 Mrs F authorised these transactions and that means that under the Payment Services Regulations 2017 and the terms of her account she is presumed liable for the loss in the first instance. The Contingent Reimbursement Model (CRM) Code does provide further protection for *some* payment transfers that were made as the result of a fraudster. However, the CRM Code does not cover payments made to another account held and controlled by the customer, card payments or payments to cryptocurrency as was the case for these payments.

However, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Lloyds ought fairly and reasonably to have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

Lloyds *did* intervene in January 2024, based on Mrs F making payments to an individual where there were already fraud concerns. Having listened to the call between Lloyds and Mrs F it's clear Lloyds had concerns that Mrs F was falling victim to a scam and may not be providing the correct reason for her payments. However, as Mrs F maintained that she was making payments to someone she knew for goods, and agreed to cancel the payment based on Lloyds' suspicions, no further action was taken after the payment was cancelled. I think that based on what Mrs F told Lloyds, and her decision to cancel the payment, the action taken by Lloyds was proportionate to the scam risk identified at that point.

Lloyds' records state that Mrs F's card was later blocked and that Mrs F visited branch to have blocks removed. Lloyds has provided notes that support this, although it's not clear what system these notes were obtained from. In any event, Mrs F has explained that she never attended branch and was abroad at the time payments were made. Mrs F has provided evidence of her flight to prove this. Having reviewed payments made that Mrs F is now claiming for, I can see that they were made from an IP address in the country she claims to have been in. Having listened to a call between Mrs F and Lloyds two days after the alleged branch visit, I can also see that she was asked if she was abroad, which she confirmed she was. During this call, there is also an interaction between two Lloyds staff members where one confirms to the other that Mrs F was supposed to visit branch, but as her payment has been refused, the branch visit has been resolved'. I therefore don't think the overall evidence supports that Mrs F did attend branch, or that any scam education was provided at this point.

I've therefore thought about the second call intervention that Lloyds had with Mrs F. In this call, there was a discussion between staff prior to speaking to Mrs F, where concerns about Mrs F's account were flagged – namely that Mrs F had made a number of payments already

to cryptocurrency platforms and concerns that these account transfers may also be being made to cryptocurrency.

When the advisor spoke to Mrs F, he did ask why Mrs F was making transfers to her own account. Mrs F explained she was building up funds in this other account. Mrs F was also asked about cryptocurrency payments she'd made and she said that the cryptocurrency platform was restrictive, so she was moving away from it. The advisor then removed blocks on Mrs F's account.

Having considered the scam indicators here, I don't think Lloyds went far enough in this intervention. By this point Lloyds were aware of the following:

- Concerns had already been raised less than two weeks previously regarding large funds being transferred to an account associated with fraud, one of which had a cryptocurrency platform name as its payment reference.

- Mrs F had since attempted a number of payments to a cryptocurrency platform, which was a new type of account activity for her.

- Mrs F had set up payments to a new payee account in her name with an e-money provider and was attempting the third payment of the day to that account. By this point in time, Lloyds would have been aware of the prevalence of multi-stage scams and fraudsters directing consumers to transfer money, often to e-money account providers to facilitate the withdrawal of funds, often to cryptocurrency.

Based on these factors, I think Lloyds ought to have been on alert that Mrs F was at risk of financial harm from fraud and questioned her in more detail about the payments she was making.

I'm aware Lloyds had intervened with Mrs F during an earlier payment and Mrs F hadn't been honest about what she was doing, so I think it's possible the same could have happened this time. However, at the time this second call took place, Lloyds had a lot more information available to it – it now knew Mrs F was making payments towards cryptocurrency, which could have helped narrow down the potential scam risks to cover with Mrs F, particularly as the subsequent payments since the last call increased that risk.

I therefore think Lloyds should have asked open questions relating to some of the most common scams at that time, to better understand what Mrs F was doing. These payments also occurred after the inception of the Financial Conduct Authority's Consumer Duty, which places additional obligations on firms to avoid foreseeable harm to customers. As a result, where it would be considered appropriate based on the risk level, we'd expect warnings provided by firms to be more 'dynamic', asking questions to better understand the scam risk and for these questions to cover potential job scams, as this was.

Had Mrs F been provided with questions and general warnings about job scams, I think these would have resonated with Mrs F – I say this because the scam Mrs F fell victim to bore all the typical hallmarks of such a scam – contact by message offering a job opportunity, completing tasks to unlock commission and payments made by cryptocurrency to 'unlock' wages. I therefore think a warning covering off some of these hallmarks would've made Mrs F pause and take heed of any warning provided by Lloyds, ultimately stopping the scam. I therefore think it's fair that Lloyds should be held liable for Mrs F's losses from the point it made this second intervention call that failed to go far enough.

*Should Mrs F bear any responsibility for her losses?*

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that there were aspects to this scam that would have appeared convincing. Mrs F has provided evidence that the fraudster provided her with an employment platform, which no doubt added a level of legitimacy to the opportunity. She's also explained that she wasn't asked from the outset for payments towards the role, which I think would've built some trust before payments were then requested. I can understand why Mrs F would be reassured by these factors that this was a legitimate role.

I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mrs F to be reduced, but I think it should.

While I accept the above would have gone some way to reassure Mrs F, I still think there were elements of this scam that ought reasonably to not have been overlooked by her, prior to proceeding. For example, Mrs F was told that the fraudster had received her information by a named individual, the name of which Mrs F didn't recognise. Mrs F has accepted this ought to have been a red flag, but unfortunately assumed this was someone who was part of a larger community she was part of. In addition, the entire premise of making payments to an employer is a complete inversion of the typical employee/employer relationship that I think would strike most as unusual. Mrs F was also told by the fraudster what to payment purposes to provide to her bank, which strikes me as something underhand for an employer to do.

Mrs F also appears to have begun working without any form of interview process or contract, which I think ought to have struck her as unusual, particularly given the large figures she appeared to have been able to earn.

I've therefore concluded, on balance, that Lloyds can fairly reduce the amount it pays to Mrs F because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

*Could Lloyds have done anything else to recover Mrs F's money?*

I've also thought about whether Lloyds could have done more to recover the funds after Mrs F reported the fraud.

The majority of payments were made by card to a cryptocurrency provider and that cryptocurrency was sent on to the fraudsters. So, Lloyds would not have been able to recover the funds.

In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency platform performed its given role in providing cryptocurrency in return for payment in sterling.

For the payment transfers Mrs F made, some were made for peer to peer lending – so Mrs F received cryptocurrency in return for the payments and the recipients of her funds weren't necessarily involved in the scam in question. I therefore don't think Lloyds had any prospects of recovering these funds either. Other payments were made to Mrs F's own external account (then onto the fraudster) so recovery attempts by Lloyds would be against Mrs F's own account.

Overall I think a fair outcome in this complaint is for Mrs F and Lloyds to be equally liable for all losses Mrs F incurred from her Lloyds account from the payment on 7 February 2024

where Lloyds intervened onwards in the scam and for Lloyds to reimburse her 50% of these losses.

## My final decision

My final decision is that I direct  Lloyds Bank PLC to reimburse Mrs F:

- 50% of Mrs F's losses to the scam from the payment intervened in on 7 Febriary 2024 onwards.

- 8% simple interest from the date each payment was made, until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 24 November 2025.

Kirsty Upton
**Ombudsman**