DRN-3448649

The complaint

Mr F is unhappy that Lloyds Bank PLC won't reimburse the money he's lost to a scam.

What's happened?

Mr F has been the victim of a scam. On 27 March 2021, he received a telephone call from someone who said they worked for Lloyds. Here's a summary of what happened during the call, and over the next few days:

- The caller told him that a fraudulent payment to a company I'll refer to as 'D' had debited his Lloyds current account, and further fraudulent payments had been attempted but blocked by the bank. Mr F checked his online banking and saw that there had been a fraudulent payment of £47.80 to D.

- Mr F was taken through security (I understand that he gave the caller his name, address and date of birth, but the caller didn't offer any personal information they knew about him) and offered an account change because of the fraud.

- Whilst on the phone, another phone call came through and the caller told him that it was the scammer trying to get into his account.

- Mr F checked the caller's telephone number against the number for Lloyds on its website and the number on the back of his Lloyds debit card. He found that the numbers matched and, when he attempted a call to the number, a Lloyds automated message played. He says this gave him confidence that he was talking to the bank.

- The caller said they'd blocked Mr F's debit card and they advised him to move his money out of the compromised account. As Mr F didn't have an alternative account that he could transfer the money in his compromised account to, they said he could send his money to a temporary 'safe' account. Mr F explained that his compromised account couldn't simply be closed after his money had been transferred because he had a cryptocurrency account with another provider that was connected to it. The caller said they would work with the cryptocurrency account provider to resolve the problem and asked him to give them his online banking login details for both his Lloyds and cryptocurrency accounts, which he did. Mr F says he was assured that he was giving this information over a secure line, and he was not suspicious of the caller because he was convinced that he was talking to Lloyds.

- Mr F transferred £5,000 and then £4,500 to two different 'safe' accounts. He says that the caller coached him through the payments – telling him to use the 'friends and family' payment option. He then transferred £2,000 to his cryptocurrency account. These payments removed most of the money from his account.

- On 28 March 2021, the caller contacted him again. They said it's possible that the scammer could take out a loan in his name via mobile banking. They asked him to do a test loan application and said he would be able to see from his credit reference file that it wasn't a real loan because it wouldn't show up (unbeknown to Mr F, new

lending would not show on a credit reference file immediately). The first loan application Mr F made for £11,000 was declined, but his second application for £10,500 was successful. The loan funds were paid into his Lloyds account on 29 March 2021. To secure the money, Mr F was asked to transfer it to his cryptocurrency account. So, he sent two payments of £5,000 and £5,200 as requested. The scammer was able to withdraw the loan funds from his cryptocurrency account, along with the £2,000 he'd transferred previously, using the login details he'd given them. Mr F says he received withdrawal notifications from his cryptocurrency account provider, but the caller told him not to worry about them as it was part of the co-operation between the two financial institutions.

- On 7 April 2021, Mr F received written confirmation from Lloyds of a new loan account. He went into a branch to query this and, at this point, it became apparent that he'd been scammed.

Mr F has said that he has been left in financial difficulties, and the situation has had a detrimental effect on his physical and mental health. The trouble and upset he's experienced has led to absence from work due to a lack of focus, which has further contributed to his financial difficulties. He feels that Lloyds should have been monitoring his account for suspicious activity and taken action to prevent the situation. So, he would like Lloyds to:

- recover his stolen money.
- unwind the loan and reimburse any contractual repayments he has made.
- cover his lost income due to absence from work.
- pay him compensation for his trouble and upset.

Lloyds declined to reimburse the two faster payments that Mr F made to third-party accounts under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code') because it said that he ignored the following effective warning, relevant to bank impersonation scams, that it gave on two occasions after he selected the 'friends and family' payment option:

"…how well do you know this person?
We'll never ask you to move your money to another account.
Fraudsters can even copy our telephone number.
Don't believe them. Hang up the phone.
Learn more about this scam (link)."

It also said that he didn't have a reasonable basis for belief when he made the payments – he was convinced by the telephone number spoofing but the warnings it gave him said that fraudsters can copy its telephone number, the scammer didn't know any personal information about him and he was asked to send the payments to temporary accounts that weren't in his name (confirmed by confirmation of payee matches).

Lloyds said that the two faster payments to third-party accounts were in line with Mr F's usual account activity and made hours apart (fraudulent payments usually follow one after the other), so they didn't seem unusual or suspicious. By the time Lloyds was notified that Mr F had been defrauded, no funds remained in the beneficiary accounts to recover. But, as the receiving bank of the beneficiary account that received the £5,000 payment, Lloyds said it hadn't followed proper account opening procedures, so it refunded 50% of that payment (£2,500).

Lloyds advised Mr F to contact his cryptocurrency account provider about the funds the fraudster had removed from that account. It declined to unwind the loan and confirmed it was holding him liable for the loan repayments.

What did our investigator say?

Our investigator thought that Lloyds should've refunded the two faster payments Mr F made to third-party accounts under the CRM Code, and taken some action to prevent the fraud altogether. But he also thought that Mr F shared some of the responsibility for his loss. He recommended that Lloyds:

- refund the fraudulent payment of £47.80 to D.
- reimburse the remaining £7,000 loss from the two faster payments Mr F made to third-party accounts.
- remove interest from the loan.
- refund 50% of the payments Mr F made to his cryptocurrency account (£6,100) and use this amount to reduce the outstanding loan balance.
- allow Mr F to repay the remaining loan balance under a reasonable repayment plan.

Lloyds accepted our investigator's recommendation, but Mr F wasn't happy with the outcome because he said it doesn't address his consequential losses. He argues that if Lloyds had have stopped the fraud as it should, then none of his losses would have occurred.

The complaint has now been passed to me to decide.

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.

Lloyds has made an offer to settle this complaint, so I've thought about whether its offer is fair and reasonable. I'm satisfied that it is, and I'll explain why.

The payment of £47.80 to D

It's unclear, from the evidence I've seen, whether the £47.80 payment to D was authorised and consented to under the Payment Services Regulations. But it does appear to have been made as part of the scam and Lloyds has offered to refund the payment, so I don't need to go on to consider this loss any further. I think Lloyds' offer is fair.

The faster payments to third-party accounts

Lloyds is a signatory of the CRM Code, which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr F fell victim to when he transferred £5,000 then £4,500 to third-party accounts, in all but a limited number of circumstances. Lloyds had argued that two of the exceptions apply in this case – it had said that Mr F ignored effective warnings it gave during the payment journeys and he made the payments without a reasonable basis for belief that the payee was the person he was expecting to pay, the payment was for genuine goods or services and/or the person or business he was transacting with was legitimate. But Lloyds has now agreed to fully reimburse the payments. I think that Lloyds' offer is reasonable in the circumstances. I don't think the warnings it gave Mr F were impactful enough to be considered effective warnings under the CRM Code, and I don't think it's unfair to say that Mr F had a reasonable basis for belief when he made the payments considering that he was in a pressured situation, Lloyds' number had been spoofed (he called the number back and heard an automated message

from Lloyds play) and the scammer had pointed out the fraudulent payment to D. I can understand why he was convinced, in the heat of the moment, that nothing was amiss.

In addition, I think that Lloyds ought reasonably to have done more to prevent Mr F from making the payments. I've looked at his account statements in the six months leading up to the scam. I can see that he had made some fairly high value payments to his cryptocurrency account and via direct debit card, ranging from £1,000 to £3,000. But the payments he made to the third-party accounts were by far the highest value transactions/faster payments he'd made, and they both went to new payees, in quick succession. I think they stand out as unusual and out of character. So, it's reasonable to expect Lloyds to have asked him some questions about the payments. Had it done so, I think the scam would've quickly unfolded and Mr F wouldn't have gone ahead with the payments.

The relevance of this finding is that Lloyds ought to have prevented the payments, rather than just reimbursed Mr F under the provisions of the CRM Code. It follows that Lloyds should pay Mr F interest from the date of loss, rather than the date it decided not to refund him under the CRM Code.

I can't know for certain what Mr F would've done with the funds he lost had he not been defrauded. But it looks like he was using his current account to save money – he kept a healthy credit balance in the account that increased over time, and he's said he lost his savings to the scam. So, it seems likely that the funds would've remained in his current account, at least for a time. So, I think it's fairest to award interest at the account rate

The loan and the payments to Mr F's cryptocurrency account

Mr F has said that Lloyds should've done more to prevent the fraud, and I agree. Taking into account what I've said about the faster payments to third-party accounts, I think the scam would most likely have unwound before Mr F started making payments to his cryptocurrency account or applied for the loan if Lloyds had intervened when I consider it should have. So, it could've prevented Mr F's loss and I think it's fair for it to bear some responsibility, as it has agreed to do. But I also think Mr F ought to have done more to protect himself from the fraud, so it's fair for him to bear some responsibility for his loss too. I say this because:

- I don't think the warning Lloyds gave Mr F when he made the two faster payments to third-party accounts was impactful enough to be considered effective under the CRM Code, but it was a pretty good warning, which was relevant to the type of scam Mr F fell victim to. It said that Lloyds wouldn't call him to ask him to move money to another account, and it pointed out that fraudsters can copy Lloyds' telephone number. I don't know how much attention Mr F paid to the warning when he made the faster payments to third-party accounts, or how much he relied on it. He says he saw it. But he was being coached through the payments by the scammer at the time, he was in a pressured situation, and the scammer knew details about his account which reassured Mr F that he was speaking to Lloyds. So, I can understand why he moved past the warning on 27 March 2021. But the scam went on for several days and I think it's reasonable to expect Mr F to have reflected on the warnings he'd been given and what he was being asked to do once the initial pressure was off. If he'd done so, I think it's likely he would've realised that all was not as it seemed, and he should take some steps to protect himself from further financial harm.

- As the scam went on, Mr F was afforded more time to think about what he was doing and the pressure to act quickly lessened. The scammer's story also got less convincing. It's difficult to understand why Mr F would need to make a test loan application for the bank or move loan funds to his cryptocurrency account to secure them if he had only made a test loan application. And then he started to receive

withdrawal notifications from his cryptocurrency account provider too, which he shouldn't have been expecting. Overall, I would've expected Mr F, or anyone else to have been put on guard and I don't think it was reasonable for him to proceed without taking steps to protect himself – such as visiting a Lloyds branch to discuss the situation, as he did after he received the letter confirming his new loan account.

- People are generally aware that it's not safe to hand over account login details and security information to anyone, even their bank. Yet Mr F gave the fraudster the login details for his Lloyds account and his cryptocurrency account.

Overall, I think both parties ought to have done more to protect Mr F from financial harm. Lloyds has agreed to refund 50% of the payments Mr F made to his cryptocurrency account (£6,100) and use this amount to reduce the outstanding loan balance. It's also agreed to remove interest from the loan and put an affordable repayment arrangement in place. I think this is a fair and reasonable offer, which is in line with my findings on shared responsibility for the loss.

Of course, Mr F can use the money Lloyds has agreed to reimburse for the faster payments he made to third-party accounts and the payment to D to reduce the loan balance to zero if he would rather not maintain contractual repayments.

Consequential loss and compensation

Mr F has said that the trouble and upset he's experienced in this matter has led to absences from work due to a lack of focus, and consequential lost income. But I don't think the lost income would've been reasonably foreseeable to Lloyds when Mr F was scammed – I'm not persuaded that it ought to have predicted Mr F would have to take time off work as a direct result of the fraud. So, I don't think it would be fair for me to ask Lloyds to compensate him for any lost income.

I'm very sorry to hear of the negative impact this matter has had on Mr F's financial, physical and mental health. I appreciate that he must have had a very distressing time. But ultimately, his loss, and the trouble and upset he's experienced, was caused by the cruel and callous acts of a fraudster. I'm satisfied that both parties could've done more to protect Mr F from financial harm. In the circumstances, I think that Lloyds has offered to do enough to address its own errors, and I won't be awarding any additional compensation.

My final decision

For the reasons I've explained, my final decision is that Lloyds Bank PLC should:

- refund the fraudulent payment of £47.80 to D.
- reimburse the remaining £7,000 loss from the faster payments Mr F made to third-party accounts, together with interest at the account rate.
- remove interest from the loan.
- refund 50% of the payments Mr F made to his cryptocurrency account (£6,100) and use this amount to reduce the outstanding loan balance.
- allow Mr F to repay the remaining loan balance under an affordable repayment plan.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 16 June 2022.

Kyley Hanson
Ombudsman