DRN-5244997

The complaint

Mr N complains that Lloyds Bank PLC (Lloyds) won't refund money he lost in a job scam.

What happened

What Mr N says:

Mr N was self-employed and short of work and money. He was looking for other work and had signed up to some recruitment agencies. He got a call from someone claiming to be from a well known agency who introduced him to a job opportunity with a firm which claimed to be dealing with 'app manufacturing'. His role was to boost the appeal of apps in order to make them look appealing and reach a wider audience. He was asked to simulate purchases and then provide five-star reviews to help marketing and boost sales. To do that he had to pay in his own money to simulate sales. He was told he could earn £7,000 per month if he completed three sets of 35 tasks each day.

He was told he needed to send the money to a crypto currency exchange and from there to a wallet address. He was told he would get payments of his commission together with a refund of the money he'd paid. He borrowed £19,000 on a loan from Lloyds to fund the payments. The payments were made both direct to crypto exchanges and to his account at bank X – from where some payments were made to the crypto exchange (to the value of £13,540).

The payments were:

No.	Date/Time of transaction	Payment	Amount
1	2 August 2023 – 1128	Faster payment – crypto exchange A	£30
2	3 August 2023	Debit card – crypto exchange B	£100
	6 August 2023	*Loan credited*	*(£19,000)*
3	6 August 2023	Debit card – crypto exchange B	£570
4	6 August 2023	Debit card – crypto exchange B	£50
5	6 August 2023	Debit card – crypto exchange B	£3,000
6	6 August 2023	Debit card – crypto exchange B	£3,000
7	6 August 2023	Debit card – crypto exchange B	£3,000
8	6 August 2023	Debit card – crypto exchange D	£3,000
9	6 August 2023 -1639	Faster payment – crypto exchange C	£1,000 *(intervention and cancelled)*
10	6 August 2023 - 1729	Debit card – crypto exchange B	£100

11	6 August 2023 - 1731	Faster payment – Mr N's account bank X	£500
12	6 August 2023 - 1755	Faster payment – Mr N's account bank X	£500
13	6 August 2023 - 1812	Faster payment – Mr N's account bank X	£500
14	6 August 2023 - 1818	Faster payment – Mr N's account bank X	£500 *(intervention)*
15	6 August 2023 - 1852	Faster payment – Mr N's account bank X	£4,000
16	7 August 2023 - 2150	Faster payment – Mr N's account bank X	£3,000
	Total payments		**£21,850**

As things progressed, he was told he needed to pay in more money to compete further tasks. And when he wanted to withdraw money, he was told he needed to upgrade to higher value tasks with more demanding targets. Then he realised he'd been scammed.

Mr N brought a complaint to Lloyds on 31 August 2023. He says Lloyds should've done more to protect him. The payments were unusual for him to make and Lloyds didn't intervene effectively or warn him. He says Lloyds should refund the money he's lost plus interest at 8% per annum.

What Lloyds said:

Lloyds didn't refund any money and said:

- Mr N didn't act responsibly. Genuine companies don't offer job opportunities in this way or employ someone without an interview or an employment contract.
- It was also unusual to expect an employee to pay money to the employer, and especially in bitcoin.
- Mr N should have therefore researched the company more thoroughly – but he acted on a link provided by the third party 'recruitment agency'.
- The first four payments (sic) were in line with Mr N's normal account activity so they had no reason to intervene. He took out a personal loan; after which he made a series of debit card payments – which the bank would normally see as a loan was used up.
- Mr N tried to make a payment of £1,000 on 6 August 2023 – Lloyds intervened and Mr N then cancelled it. He said he hadn't been asked to make the transfer by anyone or been asked to move money.
- When Lloyds stopped the payment to bank X on 6 August 2023, Mr N told the bank it was easier to move it into other currencies and to use to buy things abroad. He said no one was trying to scam him.
- None of the payments were covered by the Contingent Reimbursement Model (CRM) code.

Our investigation so far:

Mr N didn't agree and brought his complaint to us, through his advisors. Our investigator didn't uphold it either. He said:

- On Lloyds' first intervention call, it was evident the call handler noticed there were a lot of payments going out. He asked Mr N what the loan was for – he said it was for a number of things. The call handler was concerned – as Mr N also said he was transferring it into ‘US dollars’. The call was transferred to the complex fraud team, but Mr N then cancelled the payment and no more discussions took place.

- On the second intervention later that day – regarding a payment to Mr N’s account at bank X. Lloyds’ call handler asked where the payments were going to from bank X and Mr N said they were to various people in various currencies. He also said he was transferring money to family abroad and to buy things abroad. He said no one had contacted him about the payments, nor asked him to make them. He said *“…nobody try to scam me”*

- Our investigator said Lloyds’ questioning should have gone further, but even if it had, it wouldn’t have made any difference – as Mr N wasn’t truthful in his responses and would likely have not revealed the true purpose of the payments. So, the payments would likely have gone ahead anyway.

- On recovery of funds - the money had been to pay for crypto currency and in those circumstances, there wasn’t anything to be recovered.

Mr N didn’t agree. Through his advisers (who listened to the calls), he said:

- Lloyds didn’t intervene effectively. The bank should’ve asked open and probing questions and hold answers to a reasonable level of scrutiny. Lloyds failed to do this.
- Lloyds are well aware of job/task-based scams involving crypto currency payments, and should’ve asked questions with this in mind.
- It is clear that Lloyds had some concerns. For example, they highlighted the loan funds received and were concerned it was being used to fund the payments.
- Given this, they failed to act on this and ask Mr N more questions.
- Mr N did reply to the questions honestly- as he said he wanted to transfer the money into USDT. He told Lloyds he was using the money to ‘buy goods’ – which was the case given the type of the job scam. But ‘buying goods’ in crypto currency didn’t make sense.
- Lloyds should’ve dug more deeply by asking open ended and probing questions and properly scrutinising Mr N’s answers.
- Had Lloyds asked such open-ended questions, the firm would have seen the red flags and the scam would’ve been uncovered.
- Given this, Lloyds should’ve invoked the banking protocol, stopped the payments and asked Mr N to go to a branch.

Our investigator didn’t agree. He said Mr N had the chance to tell Lloyds what was happening but didn’t.

As no agreement could be reached, Mr N asked that an ombudsman look at his complaint, and so it has come to me.

<u>I reached a provisional decision which upheld Mr N’s complaint:</u>

I’m sorry to hear that Mr N has lost money in a cruel scam. It’s not in question that he authorised and consented to the payments in this case. So although Mr N didn’t intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. 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 make 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 need to decide whether Lloyds acted fairly and reasonably in its dealings with Mr N when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary– and in this case, the payments were made to Mr N's own accounts with either bank X or the crypto wallets in his name.

The first consideration here is: if the payments were of a sufficient size and were out of character with how Mr N normally used his account – then we would expect Lloyds to have intervened and spoken to him about them.

I looked at Mr N's account. He made some payments on a regular basis, but always for less than £500. So, it's fair to say the larger payments of say £1,000 (which was then cancelled) and £3,000 were unusual for him to make. And also – I have to take into account the velocity of the payments being made. The table of payments shows the date and time the payments were actioned and authorised by Mr N – not when his account was debited. And it shows he made 13 payments for £21,720 in two days (of which 12 were on one day – 6 August 2023) And another for £1,000 was cancelled by Mr N.

And – the loan was credited to his account at the same time, so it was clearly related to the payments being made.

So, given all of this, Lloyds had some concerns and spoke to Mr N twice. The calls are important and I listened to them. I show some of the important points here:

Call – 6 August 2023- payment for £1,000 (16.43):

Mr N tried to make a payment to a crypto exchange. He said it 'was to buy USDT' i.e. crypto. But – Lloyds' call handler misheard this as 'USD' and questioned why he was ending money to a crypto exchange which wasn't involved in purchases of (regular) currencies. He therefore referred it to Lloyds' complex fraud team but then Mr N cancelled the payment before that second conversation could take place. But the important parts of the call were:

Lloyds' call handler: what was the loan for? Mr N: for multiple purposes, I need am self-employed and I need to, kind of….

Lloyds call handler: firm C don't offer any type of currency exchange service? Mr N: it is peer to peer transaction.

Lloyds' call handler: Right, OK.

Lloyds call handler referred the matter internally. He says to a colleague it looks like an investment and there is a loan credit just in.

(After taking advice about firm C) *Lloyds' call handler*: asked Mr N if it was to buy crypto currency – Mr N: yes, it is, £1,000. He then cancelled the payment.

Call – 6 August 2023 – payment £500 (18.33):

Lloyds call handler could see there were a lot of payments going out and there had been a large credit paid in (the loan).

Lloyds' call handler: There is a large payment into your account, a lot of payments going out, so the bank wanted to make sure that it is actually something that you are doing and nobody contacted you or asked you to make the payments. Mr N: yes they are all my payments.

Lloyds' call handler: Are they going to the same place or to different places? Mr C: I am sending to (bank X) as it's easier to transfer to other currencies and I am buying things abroad.

Lloyds' call handler: So they are not going to the same beneficiaries? Mr N: no.

Lloyds' call handler: what is the reason you are transferring the money, to be able to get money to your family abroad? Mr N: yes and buying things abroad.

Lloyds' call handler: just checking you've not had any phone calls from anyone? Mr N: no, all by myself. Nobody trying to scam me.

Lloyds' call handler: And to confirm you are making the transfer of your own accord and no one has asked you to move money? Your own choice? Mr N: yes

I must review these calls in the context of what Lloyds could see – by the time of the second call, Mr N had made (or attempted) six faster payments in less than two hours. And on tin addition on the same day, he had made six other payments for crypto related purposes. And while they were debit card payments, Lloyds' evidence shows that were made before the faster payments later that day. I therefore assume Lloyds could see these in their system also – as they'd been authorised by the bank.

And there had been a large payment into the account – from the loan Mr N took out. And Mr N's account was completely drained of funds – he went into an overdraft of about £1,800 debit. Before the scam, he had a consistent credit balance of about £1,000.

So there was clearly something suspicious going on. And given that, I think the interventions from Lloyds should've been proportionate to the evident risks that a scam was taking place. And that means that Lloyds should reasonably have asked a series of more demanding questions and asked more probing, follow on questions of Mr N, but I'm not persuaded they did enough given what was happening.

I think Lloyds accepted too readily the limited answers they were given, and actually asked some closed questions at some points.

Such job task scams were (and are) common - Lloyds was the expert in such matters and in the interventions, we would expect a number of open and probing questions such as:

- Why are you making the payment?
- And where are you transferring the money to from bank X?
- Who to?
- For what purpose?
- How did you hear about the scheme?
- How were you contacted about it?
- Where did the money come from that you're sending?
- Where is the money going to from your crypto wallet? Why?
- What do you know about bitcoin investing?
- Have you made bitcoin investments before?

I would've expected Lloyds to ask several follow on and more challenging questions such as:

- Why are you making payments of £500 and not one payment?
- Tell me which relatives you are paying and where?
  What are you buying for them?
- Tell me how you are spending the £19,000 – that seems a lot to send to buy things for relatives.
- Why not send the money from your Lloyds account, why use bank X?
- Why are you buying crypto currency to buy things for relatives – that doesn't add up.

I think this would've revealed more about what was going on – or if Mr C declined to give the answers, or if they didn't add up, Lloyds could've refused to make the payments. The bank also could have asked Mr N to go to a branch to validate what was happening.

I'm also mindful that these were crypto related payments. And we expect that from January 2023, firms ought to recognise that cryptocurrency related transactions carry an elevated risk of the likelihood of the transaction being related to a fraud or scam. This is because, by this time many leading firms had appreciated this risk and placed blocks or restrictions on cryptocurrency related transactions, and there had been widespread coverage in the media about the increase in losses to cryptocurrency scams.

So, I'm persuaded that Lloyds should refund the payments Mr N made. In deciding from which point I assume the debit card payments of £3,000 could be seen by Lloyds from early on 6 August 2023. And so, it's reasonable to say the bank should have intervened and been able to stop the scam with effect from the third debit card payment of £3,000 – I accept that the first two were made before a pattern could be established.

So, Lloyds should be liable for payments made from then on the first instance - £15,100.

Contributory Negligence:

But that's not the end of the story here. I also considered whether Mr N could've done more to protect himself and whether he should therefore reasonably share some of his losses. And I think he should. In thinking about this - we apply a test of what we would expect a reasonable person to do in the circumstances. We don't (for example) apply a test of what we would expect a finance professional to do:

- He took a call from someone out of the blue posing as a recruitment company – this was understandable as he had signed up to various recruiting fit rms looking for work.
- But he accepted the 'job' without any interview, or contract.
- He made payment to an employer for who he was working – this was a strange thing

to do.

- And the payments were in crypto currency – which was odd.
- He didn't carry out sufficient research but relied on a link provided by the 'recruitment firm'.

So, I think it's reasonable that Mr N is responsible for some of his losses. Two respondent banks were involved and in cases such as that, our service applies a deduction of 33% for contributory negligence (as compared to 50% on most other cases).

Mr N has brought a complaint against bank X – from which bank he made payments of £13,540 to his crypto wallet. So, Mr N's losses as paid to the crypto wallet (from either Lloyds or bank X) are:

Lloyds	Payments direct to crypto exchange	£12,750
Bank X	Payments direct to crypto exchange	£13,540
Mr N's payments to crypto exchange		**£26,290**

The payments out of bank X were funded by transfers from Lloyds to bank X of £9,100, all of which should reasonably have been prevented by Lloyds. But as I've said, if I was making a decision on Lloyds' liability alone, it would likely be higher - £15,100.

In my provisional decision regarding bank X, I determined it should be responsible for payments totalling £12,540 (payments of £13,540 less £1,000 requiring no intervention).

Payments that couldn't have been reasonably stopped – where either Lloyds or bank X couldn't have been expected to intervene. I worked these out to be:

Lloyds	Payments 1-6	£6,750
Bank X	First payment	£1,000
Payments not refundable		**£7,750**

So, in total, Mr N should receive a refund of £18,540 (£26,290 less £7,750), less a deduction for contributory negligence of 33% - so a refund of £12,236. In all the circumstances here, I think it is reasonable that Lloyds and bank X share this equally - £6,118.20 each.

Recovery:

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Lloyds took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

And here, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover.

Responses to the provisional decision:

Mr N accepted my findings. Lloyds didn't comment.

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.

As Mr N accepted my findings and Lloyds didn't comment, my final decision is unchanged from the provisional decision.

My final decision

I uphold this complaint. And Lloyds Bank PLC must:

- Refund £6,118.20 plus interest at 8% per annum simple from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 4 February 2025.

Martin Lord
Ombudsman