

The complaint

Ms K complains that Lloyds Bank PLC trading as Lloyds Bank won't reimburse her with the money she lost to a scam.

Ms K initially brought her complaint to us with the assistance of a professional representative and she is now representing herself. For ease I'll refer to the professional representative's submissions as being from Ms K.

What happened

In mid-2025 Ms K was looking for work online when she was contacted on a popular instant messaging platform about a job opportunity. She understood she'd need to complete a set number of tasks each day to earn commission related to raising the profile of social media 'influencers', with extra commission for special premium tasks or challenges. Ms K was told to open a cryptocurrency wallet and to make payments to unlock the premium tasks. She received an initial payment but was later asked to pay withdrawal fees to recover her money and receive her commission earnings. When she was unable to withdraw any money, she realised she'd been the victim of a cruel scam.

Ms K had made the payments to the scammers from her account with Lloyds, both by Faster Payment transfers and by using her Lloyds debit card. She reported the scam to Lloyds, saying it hadn't done enough to protect her from the scam.

Lloyds refunded Ms K with £929 being the full amount she'd lost to the scammers by making Faster Payments between 10 and 12 June 2025. Lloyds said these payments were refunded under the Payment Systems Regulator Authorised Push Payment mandatory reimbursement rules (that I'll refer to as ASR) designed to protect customers who've lost money in a scam.

But Lloyds said the ASR didn't cover the debit card payments that Ms K had made to two cryptocurrency exchanges that I'll refer to as B and B2 as follows:

Payment Number	Date	Time	Payee	Amount
1	12.06.25	16:10	B	£850
2	12.06.25	17:05	B2	£750
3	12.06.25	20:01	B2	£4,000
4	13.06.25	11:29	B2	£3,800
5	13.06.25	11:31	B2	£5,000
6	14.06.25	12:58	B	£4,800

7	14.06.25	13:01	B	£4,320
			Total	£23,520

Lloyds said it had intervened by blocking payments, questioning Ms K several times on the telephone and giving her information around job scams and investment scams. It also asked her to attend her local Lloyds branch where it gave her further information about scams including by way of a cryptocurrency social engineering video and fraud and scam leaflets. But Ms K had wanted to proceed with the payments. Lloyds added it couldn't recover the money from the cryptocurrency exchanges which had provided the service of transferring money to cryptocurrency in a named wallet.

Unhappy with the outcome, Ms K asked this Service to look into her complaint. Our Investigator didn't uphold it. In summary, he thought Lloyds had made proportionate interventions but ultimately Ms K hadn't been entirely honest and open about her reasons for making the disputed payments. As such he didn't think Lloyds could reasonably have uncovered the scam.

Ms K didn't agree and asked for an Ombudsman's review. In summary, she said Lloyds should have done more to protect her from the scam. I'll refer more specifically to her comments in my findings below.

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.

I am sorry that Ms K has been the victim of a cruel scam and I don't underestimate the impact on her. But I don't uphold her complaint. I will explain why focusing on the main reasons for my decision.

Ms K has referred both to the Contingent Reimbursement Model (CRM) and the more recent ASR in support of her argument that Lloyds should reimburse her for the money she lost to the scam.

As our Investigator explained the CRM doesn't apply to Ms K's disputed transactions, because they were made after the ASR came into effect for payments made on or after 7 October 2024.

Under the ASR Lloyds correctly reimbursed Ms K for the Faster Payment transfers she made, totalling £929. But the ASR applies only to Faster Payments and CHAPs transfers between banks. Ms K's card payments do not fall under the scope of the ASR (and would not have been under the scope of the CRM either). But this is not the end of the story as I will consider whether Lloyds fairly and reasonably could have uncovered the scam.

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 (2017) and the terms and conditions of the customer's account.

It isn't in dispute that Ms K authorised the card transactions in question. She is therefore presumed liable for the loss in the first instance. However, Lloyds is aware, taking longstanding regulatory expectations and requirements into account, and what I consider to be good industry practice at the time, that it should have been on the look-out for the possibility of fraud and made additional checks before processing payments in some

circumstances.

Did Lloyds recognise that Ms K was at a heightened risk of financial harm from fraud?

I think Lloyds correctly assessed that Ms K was at a heightened risk of financial harm from fraud when she made the disputed card payments to cryptocurrency exchanges B and B2. The amounts and pattern of her payments to cryptocurrency exchanges were out of character and unusual for her account.

What did Lloyds do to warn Ms K?

I will describe when the interventions took place and then go on to explain whether I think the interventions were proportionate to the risk the payments presented.

- I see that on 12 June 2025 - between payments 1 (£850) and 2 (£750) - Ms K's attempted 5 payments of £350 (3 attempts) and £750 (two attempts) respectively 'bounced back' and so weren't successful. Ms K attempted to make a payment of £4,000 to B2 but Lloyds stopped the payment and she telephoned the bank ('Intervention 1'). She was then able to make card payment 3 (£4,000) to B2.
- Ms K then attempted to make 5 payments to B2 on 12 and 13 June 2025 for amounts of £4,800 (3 attempts), £3,800 and £100 respectively but again the payments bounced back and were not successful. On 13 June 2025 Lloyds then stopped Ms K's attempted payment of £100 to an Electronic Money Institution (EMI) that I'll refer to as R. Ms K spoke to Lloyds ('Intervention 2') and she was then able to make further payments.
- On 13 June 2025 Ms K made card payments 4 (£3,800) and 5 (5,000). But on 14 June 2025 Lloyds then stopped the attempted card payment of £4,200 to B. After Ms K called Lloyds and then went into her local Lloyds branch (Intervention 3) she was able to make payments 6 (£4,800) and 7 (£4,320) to B.

I've listened to Ms K's calls with Lloyds and I'll set out what I consider to be the key points below, referring where relevant to Ms K's responses.

Intervention 1

During its first conversation with Ms K, Lloyds explained the massive increase in cryptocurrency scams that were coming through. I consider this gave some context to the warnings it went on to give Ms K about the two scam types it was seeing:

- *Cryptocurrency investment scams.* Lloyds explained the key features were that: the customer was contacted by social media by someone they believe to be an adviser or who was recommended by family or friends; the broker would explain how to open a crypto portfolio to fund the account; after making what seemed to be a quick profit the customer would have to pay fees and taxes to withdraw the money to a third party crypto wallet.
- *Job and task scams* (and Lloyds' call handler added that the previous caller had experienced a job scam). Lloyds explained the key features are: the customer being put in touch with someone who says they can get the customer commission for tasks they complete; this can include leaving reviews for products, liking or commenting on videos and earning commission for every task the customer completes; after earning commission, the customer is told they'll have to pay fees or taxes to withdraw their funds.

Lloyds then asked Ms K several questions about cryptocurrency including: how long she'd been dealing with B; what swayed her into getting into crypto; whether she was in contact with anyone about the investments or was receiving financial advice; that in line with Financial Conduct Authority (FCA) guidance, she should be prepared to lose any money she invested in crypto and whether she was happy with that; whether anyone had access to her crypto accounts and whether she'd been told to move this money by anyone else; and finally whether she was sure the attempted payment was genuine and made at her own request.

I don't consider all Ms K's answers to Lloyds' questions were entirely open or honest. By her own evidence, she'd opened the crypto exchange accounts in order to pay money to the people she now knows were scammers. But she said she'd always been interested in crypto and thought she'd 'get into it'. She said she wasn't in contact with anyone regarding her 'investments' but that wasn't the case – she wasn't paying money to the crypto account for an investment but as part of a job opportunity. She had been offered money for certain tasks as part of a job opportunity.

Intervention 2

Ms K called Lloyds a second time because her debit card had been blocked when trying to transfer money to R and B. Lloyds asked Ms K whether she was transferring money to her own account. Ms K said she was and Lloyds asked a few questions: whether anyone had asked Ms K to transfer the money or lie to the bank about the transfer; why she was transferring the money (Ms K said she was 'into cryptocurrency'); whether Ms K was aware of the risks of cryptocurrency and that the bank wouldn't be liable for any losses; how long she'd been investing; and whether anyone had told her to move the money or said they were calling from the bank. Lloyds said it was asking these questions because customers do get coerced into making these types of payments by fraudsters impersonating the bank.

Again Ms K said that she had been investing for a while which was not correct and was not the reason she was making payments to cryptocurrency exchanges.

Lloyds went on to explain some key risks of cryptocurrency investments: which the FCA said were not regulated in the UK and so very little could be done if the investment went wrong; that she would be unable to raise a dispute with the bank as there's no guarantee of a gain; and if someone had told her to move the money they're likely to be a fraudster or were trying to get money from her.

Intervention 3

During the third call, Lloyds asked Ms K: how she'd got to know B, whether someone advised her or through her own research. Ms K said she was doing it (cryptocurrency investment) from her own research and with a friend. Lloyds asked her more about the friend and Ms K said it was someone she'd grown up with – the friend wasn't advising Ms K but they were doing it from their own separate accounts and discussing it.

Lloyds went on to ask if it was Ms K's first investment into something like this and what her plan was (short or long term) and whether she was aware of the risks. Ms K said it was her first time and she was investing in the short term.

Lloyds then expressed concern about the amount of money she was investing in her account with B and checked whether Ms K had been forced into it. Ms K said not. Lloyds said that the amounts Ms K was investing over a short term was a concern and Lloyds' job was to protect her and her money in case she was being scammed.

Ms K became impatient at this point, because she said from her point of view it was her

money and she was doing it (cryptocurrency investment) for herself. She said she was into cryptocurrency and asked what the problem was.

Lloyds explained that it had already blocked payments, because its systems flagged when something was out of character or was a concern to it. Lloyds noted it was the third time it had blocked payments and the situation was high risk so it was going to have to ask her to go into her local branch with some identification before it would remove the blocks on the account.

Ms K expressed frustration at this, saying it was her money and she was going to close her account when the payment had been authorised. She explained it was difficult to park at the bank and she'd need to do this today. Lloyds expressed concern about why she needed to do it that day and Ms K said she was going abroad the following week and had to sort it out before she went. Ms K criticised the Lloyds' staff member and asked again for the transaction to be authorised on the phone. After a further discussion about this and Ms K expressing her annoyance she was told to take photographic identification to the branch.

Ms K then went to the branch and I've listened to the call between Ms K, the branch staff member and Lloyds' fraud team. The branch staff member said 'we've watched the video and she'd [Ms K] still like to go ahead'. The fraud team member checked whether Ms K had understood the social engineering video and the branch staff member said yes she'd shown Ms K the crypto one.

I've seen a transcript of the video which described some of the key features of cryptocurrency scams, including the ones Lloyds had already set out to Ms K.

The fraud team member then asked Ms K whether she'd watched the video and Ms K said 'yes'. Lloyds went on to ask whether she was making an investment and Ms K said she was 'into cryptocurrency'. Lloyds asked whether she'd checked the company (B) and Ms K said she had. Lloyds warned her again that if she lost money on the investment, the bank wouldn't refund the money if it turned out to be a scam, and Ms K acknowledged that.

The fraud team member said she was looking through the transactions and asked about how Ms K knew about B. Ms K said she saw it on 'social' and went on to it. Lloyds again asked how she knew about B and Ms K said it was on the internet, and she'd then registered with B online. Lloyds asked if she'd checked it was genuine and whether anyone recommended B to her. Ms K said she'd read reviews and no-one had recommended B to her. Lloyds again checked no-one had forced her to make the payments and that she'd read B's terms and conditions.

Ms K asked whether the fraud team member would stay on the line while she made the transfers, and the team member said she wouldn't. After some further checks the fraud team member then told Ms K her card had been unblocked.

As above, I don't consider Ms K was entirely open and honest with Lloyds. By her own account she wasn't making cryptocurrency investments with a friend, but rather she was sending money to a company she was working for to release her commission.

Were the warnings Lloyds gave Ms K proportionate to the risk presented by the payments?

I consider Lloyds' interventions were proportionate to the risk presented by Ms K's payments. I consider Lloyds asked open and probing questions of Ms K and challenged her answers. Lloyds blocked payments until it had spoken with Ms K and also required her to come into a branch to view an educational video about cryptocurrency investment scams.

During the interventions, Lloyds gave Ms K warnings which I think covered the key features of both cryptocurrency investment scams and (during Intervention 1) job scams. It gave her some context for its questions being concerns around cryptocurrency scams, job or task scams and safe account/impersonation scams.

Could Lloyds reasonably have uncovered the scam and prevented Ms K's loss?

I don't consider Lloyds could reasonably have uncovered the job or task scam to which Ms K had fallen victim.

I say this because, as set out above, I don't consider Ms K gave entirely open or honest answers in response to Lloyds' open and probing questions. Lloyds had given Ms K a clear warning about the risks and key features of job or task scams. Unfortunately this warning didn't resonate with Ms K despite the warning covering features of the scam to which she'd fallen victim.

I find that Ms K's answers to Lloyds' questions weren't entirely open or honest, despite it explaining why it was concerned about the risk she could be falling victim to a cryptocurrency or job scam. Ms K's explanation that she was investing in cryptocurrency based on her own research and that she was doing it alongside a childhood friend wasn't correct.

Ms K says that Lloyds spoke to her in branch and she was shown the fraud video, but Lloyds should have done more. She earlier said that she'd been left on her own to watch the video. She says the staff and fraud agent were aware she was under pressure to make the payment and the conversations show clear signs of social engineering that should have prompted stronger intervention (such as delaying or blocking the transaction).

Having listened to the final call, it's not clear to me that Ms K was left on her own to watch the video. And Ms K did confirm she'd watched the video. She says she was vulnerable in the branch but I've not seen or heard any evidence to show that Lloyds overlooked any vulnerability when speaking with Ms K and unblocking the payments.

I don't agree with Ms K that Lloyds' staff members were aware, or should have been aware she was being put under pressure to make the payment by any third party. Lloyds asked her why she'd wanted to make the payment that day and she told them that it was because she was going abroad the following week. She maintained that she was investing in cryptocurrency based on her own research. Lloyds asked her repeatedly whether she was being told to make the payments or was under pressure to make the payments and she said she was not. I don't agree that given Ms K's answers to its questions that Lloyds should have recognised 'clear signs of social engineering' as she suggests.

Lloyds had blocked three payments, and didn't unblock them before speaking to Ms K at length each time. So I don't consider a proportionate response to the risk the payments presented was to delay or block the transactions further. Given Ms K's repeated explanations that she was investing in cryptocurrency I don't consider Lloyds should reasonably have refused to unblock her account.

Ms K says the scammers' control was psychological and situational. But given Ms K's answers to all the interventions Lloyds made, I don't consider it's likely, on the balance of probabilities, that Lloyds could reasonably have uncovered the scam or broken the spell of the scammers.

I do appreciate being the victim of a cruel scam has had both a financial and emotional impact on Ms K. Despite my natural sympathy for her, I don't consider I can fairly or

reasonably require Lloyds to reimburse her – either in full or in part - for the money she lost to the scammers.

Recovery

I don't consider Lloyds could reasonably have recovered any of the money Ms K lost to the scam. She'd paid the money to cryptocurrency accounts in her own name before converting it to cryptocurrency to send to the scammers. Any chargeback procedure would not have succeeded because the money had been used to buy cryptocurrency.

My final decision

For the reasons I've explained, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms K to accept or reject my decision before 27 February 2026.

Amanda Maycock
Ombudsman