DRN-4785731

The complaint

Mrs A has complained that Lloyds Bank PLC ("Lloyds") failed to protect her from falling victim to an employment scam, and hasn't refunded the money she lost.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mrs A has used a professional representative to refer her complaint to this service. For the purposes of my decision, I'll refer directly to Mrs A, but I'd like to reassure Mrs A and her representative that I've considered everything both parties have said.

At the end of July 2023 Mrs A says she received a message on a popular messaging app from an individual ("the scammer") claiming to represent a recruitment company. , working on behalf of a digital marketing agency. The representative claimed to have found Mrs A's contact details on a recruitment website where she'd posted her profile. As Mrs A had in fact added her details to a recruitment site she says she didn't doubt their legitimacy, especially as online reviews about the company appeared positive.

The job offer was for a data generator role, which involved completing daily tasks to generate website traffic. The tasks required purchasing and reselling discounted products, and Mrs A was promised 0.5% commission in return. Mrs A created an account on the company's professional-looking website, submitted her ID, and followed the scammer's instructions to link her account to a cryptocurrency account as she says she was told she'd need to maintain a balance in her work account to fund the tasks. She made an initial payment of £1.00 on 31 July 2023, which was followed by her being able to make a withdrawal of £83.00, which understandably, she says added to her confidence in the company's legitimacy.

On 2 August 2023 Mrs A encountered an issue funding a task. She referred this to the scammer and they explained that occasional deposits were necessary to unlock tasks, but these led to higher commission and larger profits. Two days later, on 4 August 2023, a similar issue arose, leading Mrs A to make a payment of £8,062.00. Although Lloyds raised concerns and placed a hold on the transaction, it allowed the payment to proceed after it had spoken to Mrs A about it by phone. But she's explained that there were problems with her cryptocurrency account and a payment of £7,170.62 was returned to her Lloyds account.

Over the next few days, Mrs A made additional payments totalling £6,788.79 to clear what the scammer described as a negative account balance. She says that Lloyds didn't intervene, and the supposed success stories shared in a group chat she'd been added to further convinced her to continue. She later made payments from a different account until the scammer demanded tax payments to enable withdrawals. At this point, Mrs A realised she'd been scammed.

The payments Mrs A made and received related to this scam were as follows:

Date	Amount	Description
31/07/2023	£1.00	Transfer to crypto platform F
31/07/2023	+£83.00	Credit from crypto platform F
02/08/2023	£32.54	Debit card payment to crypto platform C
04/08/2023	£8,062	Transfer to crypto platform F
04/08/2023	+£7,170.62	Credit from crypto platform F
04/08/2023	£82.00	Debit card payment to crypto platform C
07/08/2023	£42.39	Debit card payment to crypto platform C
07/08/2023	£220.16	Debit card payment to crypto platform C
07/08/2023	£410.86	Debit card payment to crypto platform C
07/08/2023	£588.21	Debit card payment to crypto platform C
07/08/2023	£1,381.81	Debit card payment to crypto platform C
07/08/2023	£1.65	Debit card payment to crypto platform C
07/08/2023	£10.68	Debit card payment to crypto platform C
07/08/2023	£4,143.71	Debit card payment to crypto platform C
Outstanding loss	**£7,723.39**	

Mrs A made a complaint to Lloyds on the basis that she made ten payments totalling £14,884.83 within seven days to a new payee linked to cryptocurrency. She believes Lloyds failed in its duty to intervene as it should've identified red flags, such as the high-value transactions, the speed at which funds were being depleted, and the fact the payee had never appeared on her account before. Mrs A said that Lloyds should've flagged this unusual activity as suspicious and contacted her to question the payments or provide fraud warnings. She believes that if Lloyds had taken these steps, she wouldn't have proceeded and could've avoided the financial harm she's now suffered.

Lloyds didn't uphold Mrs A's complaint. In its response it noted that some of the payments were made as transfers to cryptocurrency accounts in Mrs A's own name, and the others were made as debit card payments. It also said that neither of the payment types seen in this scam fall under the Contingent Reimbursement Model ("CRM") Code and it therefore declined to reimburse Mrs A for her losses. It also highlighted that it had spoken to Mrs A before she made the payment for £8,062 and given her multiple warnings related to cryptocurrency, but she chose to proceed with the payment regardless.

Mrs A remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that although Lloyds had intervened at the point she thought it ought to have, which was when Mrs A attempted to make the payment for £8,062, Mrs A didn't reveal the full circumstances behind the payment so she didn't give Lloyds the opportunity to prevent the scam.

As Mrs A didn't accept the investigator's opinion, the case has been passed to me to make a 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.

I've considered all available evidence and arguments to decide what's fair and reasonable in the circumstances of the complaint.

I'm sorry to disappoint Mrs A but having considered everything I'm afraid I'm not upholding her complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mrs A authorised these payments from leaving her account. It's accepted by all parties that Mrs A gave the instructions to Lloyds and Lloyds made the payments in line with those instructions, and in line with the terms and conditions of Mrs A's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I've firstly considered whether the payments are covered by the CRM Code. And I'm satisfied that Lloyds is correct that they are not – on the basis that the transfers were made to an account in Mrs A's own name, under her control, and the others were made by debit card. Neither of these payment types benefit from the protections of the CRM Code, but Lloyds still has a responsibility to protect Mrs A from financial harm, which I've gone on to consider next.

I've carefully reviewed the payments that Mrs A made as a result of this scam and having done so, I agree that Lloyds ought to have intervened before Mrs A made the payment on 4 August 2023 for £8,062. This payment was significantly out of character when considered alongside Mrs A's usual spending pattern, and the fact it was identifiably being sent to a cryptocurrency platform means Lloyds ought to have known it carried a higher risk of being fraudulent.

Lloyds blocked this payment and spoke to Mrs A by phone before it was released. I've listened to that call and although I won't transcribe it word-for-word, I've included a summary below.

At the start of the call Lloyds checks the payment is being made to a cryptocurrency exchange and confirms with Mrs A that the funds would be used to fund her cryptocurrency wallet, which Mrs A confirms to be correct. Lloyds then asks whether she has other cryptocurrency accounts, and Mrs A mentions she'd previously used an account with another cryptocurrency platform but had stopped using it around a year earlier. Lloyds also enquires whether Mrs A had made previous payments to cryptocurrency accounts, which she says she has.

Mrs A then assures Lloyds that she had opened her cryptocurrency accounts after conducting her own independent research into cryptocurrency, and confirms she has sole control of the accounts, with no one else having access. Lloyds asks whether any traders, brokers, account managers, or financial advisers have been involved in explaining cryptocurrency, opening accounts, or promising returns on investments, and Mrs A is clear that this isn't the case. She also denies being approached or influenced by anyone offering assistance or claiming she could recover money from past investments.

Lloyds then goes on to give Mrs A a detailed scam warning, outlining common tactics used by fraudsters, such as approaching customers via social media or cold calls, making unrealistic promises of returns, and encouraging them to download remote access software. Lloyds explains how scammers can gain control of accounts and leave victims without any funds, and Mrs A confirms she understands the warning and reiterates that the decision to make the payment is entirely her own.

Finally, Lloyds confirms the source of the funds for the payment, which Mrs A says is from her account overseas. Having completed these checks and reconfirming that Mrs A was acting independently and that she understood the risks, Lloyds releases the payment.

Given the information provided by Mrs A, it's clear that her responses aligned with Lloyds' due diligence process and didn't raise any concerns that she was under undue influence or being coerced. She demonstrated a clear understanding of the risks involved and assured Lloyds that the payment was her decision.

All things considered, I'm satisfied that it was reasonable for Lloyds to process the payment of £8,062 following its intervention, as Mrs A was given ample opportunity to provide further information on the payment and the true reasons behind it. That would've allowed Lloyds to more accurately assess the risks involved and to further intervene in an attempt to protect Mrs A from financial harm, but Mrs A chose not to divulge that information.

It's also important to note that in reviewing this complaint I've reviewed Mrs A's complaint about another bank connected to the same scam. That bank intervened several times and at no point did Mrs A reveal the true reason she was making the payments, again despite being given ample opportunity to do so. She told that bank she was purchasing goods (which she later explained to be facial products) and making a loan repayment.

With all of this in mind, I don't hold Lloyds responsible for Mrs A's losses, as although its intervention wasn't successful, I don't believe that was because of a failure on Lloyds' part. I'm also not persuaded that interventions at any other points during the scam would've uncovered or prevented it, as I've seen nothing to suggest that Mrs A would've given more accurate information or elaborated on the reasons she was making the payments at any point.

Recovery of the funds

I haven't been provided with information on whether Lloyds attempted to recover the funds made by bank transfer to cryptocurrency platform F, but I'm not persuaded that makes a difference in this case. As Mrs A has explained she used the funds to buy cryptocurrency, she'd effectively spent the funds as soon as they arrived in her account at the cryptocurrency exchange. Any funds she didn't use to purchase cryptocurrency would've remained in her account under her control and wouldn't be considered a loss.

As the payments to cryptocurrency platform C were made using Mrs A's debit card, the chargeback process is relevant here. In simple terms a chargeback is a mechanism for a consumer, via their card provider, to reclaim money from a retailer's bank when something has gone wrong, provided the transaction meets the eligibility criteria. It's for the card provider to decide whether to raise a chargeback, and it only needs to do so if it has a reasonable prospect of success.

It's also relevant to note that raising a chargeback isn't a legal right, and it's for the debit or credit card provider to decide whether to make a chargeback request to the retailer's bank. The process for managing these claims is determined by a set of rules by the card payment

networks and there are no guarantees the card provider will be able to recover the money through the chargeback process.

In order for Lloyds to raise a successful chargeback it'd need to provide evidence that the merchant didn't provide the goods or services that Mrs A paid for. So although I understand Mrs A used her debit card to fund her cryptocurrency account and ultimately purchase cryptocurrency, which she sent on to the scammer, there's no evidence the merchant didn't fulfil its obligation to provide the cryptocurrency that Mrs A paid for. So the dispute doesn't lie between Mrs A and the merchant, but instead Mrs A and the scammer. As there wasn't a reasonable prospect of a chargeback claim being successful, I don't think that was a route that Lloyds ought to have pursued.

Finally, I note that Mrs A's representative has referred to Lloyds' failure to invoke the Banking Protocol in this case. But the Banking Protocol is an initiative between banks and the police to identify consumers who are in the process of sending funds to a scammer, specifically in person in one of the bank's branches. As that's not how Mrs A made these payments, the Banking Protocol isn't relevant here.

I'm very sorry that Mrs A has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Lloyds responsible for that.

My final decision

I don't uphold Mrs A's complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 12 February 2025.

Sam Wade
Ombudsman