DRN-5285053

The complaint

Mr A has complained that Lloyds Bank PLC ("Lloyds") failed to protect him from falling victim to a scam and hasn't refunded the money he 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.

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

Mr A says that he met a woman I'll refer to as "J" on a social media platform in August 2023, and they began an online relationship. They exchanged photos and messages, and over time, their conversations became increasingly romantic. J told Mr A that she ran an online store and earned a stable income by purchasing cryptocurrency through an exchange to pay suppliers. She said she made between $50,000 and $60,000 a month. They planned to meet in December 2023, as J claimed she would be travelling to Europe then. Their chats covered many aspects of their lives, and to Mr A, the relationship seemed genuine.

J encouraged Mr A to get involved in her online store business model, telling him she would help him set up his own store. She explained that opening a store was free, and there was no need to stock up on goods. J told Mr A that suppliers provided products, and when customers placed orders, he would only need to pay the cost price to the supplier. The supplier would then handle shipping and after-sales service. Mr A agreed and was told that J would share a store with him. In September 2023, the store was set up, and Mr A was sent links guiding him through the process. He's explained he believed this was a genuine store on a reputable platform and checked online to confirm that the platform hosting the store had an e-commerce function.

Mr A says he was told by J to open accounts with several cryptocurrency exchanges to make payments to the suppliers for purchasing goods in his store. From 2 October 2023, he began making payments on this basis. Mr A has explained that as time went on he struggled to make further payments, but J offered to lend him money, which further increased his trust in her.

The payments relevant to this scam were as follows:

	Date	Amount	Description
1	02/10/2023	£25	Debit card to crypto platform
2	02/10/2023	£100	Debit card to crypto platform
3	09/10/2023	£120	Debit card to crypto platform
4	09/10/2023	£15	Debit card to crypto platform
5	09/10/2023	£170	Transfer to crypto platform
6	07/11/2023	£300	Debit card to crypto platform

7	15/11/2023	£160	Debit card to crypto platform
8	15/11/2023	£200	Debit card to crypto platform
9	19/12/2023	£300	Debit card to crypto platform
10	27/12/2023	£260	Debit card to crypto platform
11	09/01/2024	£300	Debit card to crypto platform
12	15/01/2024	£550	Debit card to crypto platform
-	16/01/2024	£144.64+	Payment from crypto platform
13	29/01/2024	£2,724.24	Debit card to crypto platform
14	30/01/2024	£800	Debit card to crypto platform
15	04/03/2024	£1,300	Debit card to crypto platform
	Total loss	**£6,729.60**	

By late November 2023, J told Mr A that he had 76 unprocessed orders worth $10,078.80 and 45 processed orders worth $5,138.40. He was told that once the store was closed, he would receive a total of $15,217.20. From that point on, he followed J's instructions to close the store and access what he believed to be his earnings. However, he was told he had to make further payments to process outstanding orders and pay taxes before the profit could be released. The payments he made from December 2023 onwards were with this goal in mind. Throughout this period, J continued to guide Mr A through the process using a messaging app.

In January 2024, Mr A was able to withdraw £144.64 into his bank account, but he wasn't able to withdraw anything further after that. He says that in March 2024, he realised that the entire process, including his conversations with J, had been a scam.

Mr A made a complaint to Lloyds, but Lloyds didn't uphold the complaint. In its response it explained that it wasn't refunding the payments Mr A made under the Visa chargeback scheme, as they were made to a legitimate cryptocurrency exchange, and the cryptocurrency exchange had provided the services Mr A had paid for. So it deemed that Mr A didn't have a valid case to raise a chargeback for.

As Mr A remained unhappy he referred his complaint to this service. He added that although the payments were authorised, he was still the victim of a scam, and Lloyds should have taken steps to protect him from authorised push payment (APP) fraud. Mr A added that Lloyds should have recognised that his payments were unusual as he had held an account with the bank for some time, meaning it had a clear picture of his usual spending habits. He added that the scam payments were directed to cryptocurrency exchanges, which are commonly used in fraud schemes, and the transactions involved new payees and were the first time he'd used such exchanges. His usual account activity consisted of numerous small transactions, so he says that the large payments were highly unusual, both individually and cumulatively

Mr A believes that he acted reasonably given the circumstances. J was highly convincing and didn't appear overly pushy. She claimed to be operating through a platform Mr A was familiar with, and he even checked online to confirm the platform had an e-commerce function. J also provided detailed explanations about her earnings, which further reassured him.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that she didn't think the initial payments were sufficiently out of character for Mr A's account that Lloyds ought to have been suspicious of them. She also explained that by the time the payments increased, in late January 2024, Mr A had been making payments to the same merchant for several months. So she thought it was reasonable for Lloyds to assume that Mr A trusted it, and not intervene.

As Mr 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'm sorry to disappoint Mr A but having considered everything I'm afraid I'm not upholding his 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 Mr A authorised these payments from leaving his account. It's accepted by all parties that Mr A used his debit card and Lloyds made the payments in line with what Mr A had asked, and in line with the terms and conditions of Mr 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.

Lloyds says that it processed all of Mr A's payments in line with his instructions, without intervening or introducing any friction to the payment journey.

The payments Mr A made to the cryptocurrency platform were clearly identifiable as such. And by the time they were made, in 2023, the Financial Conduct Authority and other organisations had published several warnings about the risks associated with cryptocurrency that Lloyds would've had the opportunity to digest. But that doesn't mean Lloyds ought to have treated *all* cryptocurrency-related transactions as inherently high-risk. I recognise that many cryptocurrency transactions are made legitimately and so although I'd still expect Lloyds to have been on the lookout for potential fraud or financial harm to Mr A, I wouldn't have expected it to treat the transactions differently to others on his account solely on the basis that they were linked to cryptocurrency.

Having considered the pattern and values of the debit card payments to the cryptocurrency platform, I don't think that Lloyds ought to have identified that they carried an elevated risk of being fraudulent. I say this because although the values of the transactions increased over time, when they started they were for low values that I'd consider to be in line with Mr A's usual day-to-day spending. Although the payment values increased over time, this didn't happen until Mr A made payment 13 at the end of January 2024, by which time there was a history of what Lloyds might've regarded as the cryptocurrency exchange being a trusted merchant. I'm also mindful that whilst some of the payments were made on the same day, or within a day of another one, the overall scam took place over around five months. Fifteen transactions made in this amount of time isn't typical of a scam – where most or all of the payments are usually made in rapid succession over a much shorter time period, and often increase in size progressively.

In addition, the cryptocurrency exchange that the payments were made to is a legitimate business, and there's nothing to suggest that it was operating fraudulently, or that Lloyds ought to have been suspicious about that. The fraud didn't occur as a result of the payments made from Lloyds to the cryptocurrency exchange, but instead when Mr A transferred the cryptocurrency to the wallets the scammer had told him to, which was to some extent, outside of Lloyds' control.

Having considered everything, I've concluded that Lloyds didn't act incorrectly by allowing Mr A's debit card payments to be made without intervention, as I don't think it missed the chance to uncover the scam that it otherwise ought to have.

Whilst the transactions were identifiable as cryptocurrency-related, this alone didn't warrant Lloyds treating them as high-risk, given the prevalence of legitimate activity in this space. The payments began at low values in line with Mr A's usual spending and only increased after a period that could have established the legitimate cryptocurrency exchange as trusted. And as the payments were spread over around five months, the pattern didn't resemble a typical scam that Lloyds ought to have identified.

Recovery of the funds

Mr A made a payment (payment five) to one of the cryptocurrency exchanges by bank transfer. Whilst Lloyds could've considered attempting recovery of this payment, I don't think that would've been successful. Mr A has confirmed that he used the funds to purchase cryptocurrency, which he sent to a wallet that he'd been given details of by the scammer, so it's unlikely the funds would've been recoverable as Mr A had effectively spent them. And any unused funds that weren't used to purchase cryptocurrency would've remained in Mr A's control to return to his Lloyds account as he wished.

As the remainder of the payments were made using Mr A's debit card it's relevant for me to consider the chargeback process.

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 Mr A paid for. So although I understand Mr A used his debit card to fund his cryptocurrency account and ultimately purchase cryptocurrency, which he sent on to the "suppliers" directed by the scammer, there's no evidence the merchant didn't fulfil its obligation to provide the cryptocurrency that Mr A paid for. So the dispute doesn't lie between Mr A and the merchant, but instead Mr 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.

I've noted that Lloyds says that when Mr A initially reported the scam it mistakenly told him it would raise a chargeback, despite it not having the rights to do so. It paid Mr A £75 compensation for incorrectly raising his expectations. I agree that Lloyds wouldn't have had chargeback rights in the circumstances, and I think the compensation it paid Mr A for the misinformation is fair recognition of the disappointment this inevitably caused – but it didn't affect the outcome of the chargeback claim itself.

I'd like to reassure Mr A that I don't intend to place blame on him as its clear he's been the victim of a sophisticated scam here, and I'm very sorry that happened. But in order to uphold

his complaint Mr A has made against Lloyds I'd need to think that Lloyds was responsible for his loss, and for the reasons I've explained, I haven't concluded that it was.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 5 March 2025.

Sam Wade
Ombudsman