DRN-4856678

The complaint

Miss R complains that Lloyds Bank PLC Ltd won't refund money she lost when she was a victim of a crypto investment scam.

Miss R is represented by a firm I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In 2023 Miss R saw an advert to invest with a firm, that I'll refer to as 'B', on social media. Interested in this opportunity, which included new customers receiving a bonus, Miss R decided to sign up. Miss R has explained that she was required to provide two forms of ID as part of B's KYC and anti-money laundering checks – which gave her the confidence B was a legitimate firm.

Under the belief it was a legitimate firm, Miss R set up a trading account with B. And she's said B guided her through the process of funding her account – which showed her *'profits'* rising, prompting her to invest further. Miss R made the following payments to a legitimate crypto exchange before forwarding the funds on to B's trading platform:

Transaction Date (Time)	Transaction type	Amount
7 October 2023 (14:40)	Debit card	£126
7 October 2023 (16:11)	Debit card	£126.79
7 October 2023 (18:19)	Debit card	£250.93
9 October 2023 (16:16)	Debit card	£1,000
9 October 2023 (18:39)	Debit card	£1,000
9 October 2023 (22:56)	Debit card	£119.87
9 October 2023 (23:35)	Debit card	£76.65
10 October 2023 (06:55)	Debit card	£100.34
10 October 2023 (12:30)	Debit card	£1,070
	Total	£3,870.58

Miss R received a £106.55 credit into her Lloyds account from the crypto exchange on 9 October 2023. This brings her total loss to £3,764.03.

Miss R realised she'd been scammed when she confided in a family member about investing with B after making these payments. C complained to Lloyds, on Miss R's behalf, on 16 November 2023 saying the payments were made as part of a scam. In short, they said:

- Lloyds has an obligation to protect customers from financial harm. But the payments debited Miss R's account without any intervention or detailed scam warnings being given. This is despite the payments being highly unusual given their value, them

being made to a new payee linked to crypto and the speed at which they were made.
- This payment activity should've flagged additional security, thereby prompting Lloyds to have questioned Miss R about the payments. Had this happened, Lloyds would've detected the scam and prevented the payments being made.
- Miss R was inexperienced with investments of this nature and found the scammers extremely professional and knowledgeable. This, alongside the trading platform that showed her 'profits', led her to think B were genuine and that her money was safe in a secure account.
- Miss R was vulnerable at the time the scam took place as she'd been the victim of domestic abuse from her ex-partner that required her to leave her family home, after recently having a new-born baby. This had a detrimental effect on Miss R's mental health and decision-making ability.
- Miss R's first language isn't English.
- Lloyds should refund Miss R whether they were aware of this vulnerability or not – as mandated under the Contingent Reimbursement Model (CRM) code.
- To settle this complaint, they said Miss R would accept a full reimbursement of her losses, 8% interest and £300 compensation.

Lloyds didn't uphold the complaint. They said Miss R hadn't verified the third party, B, nor had she checked the company's name online. And the funds were sent to an account held in Miss R's own name with the crypto exchange before sent to the scammer. Because of this, Lloyds wouldn't refund Miss R and advised that she should contact the crypto exchange for further assistance.

The complaint was referred to the Financial Ombudsman. Our Investigator didn't however think Lloyds had to do anything further. He said he didn't think the payments would've been particularly unusual or suspicious to Lloyds based on Miss R's normal account activity – noting she had made multiple payments to other merchants on the same day previously. Nor were they made in quick succession or did they drain Miss R's account. Our Investigator added that the only option of recovery was by way of chargeback, but he didn't think there was any reasonable prospect of success given Miss R received the service from the crypto exchange.

C didn't agree and, in short, they said:

- It is well known to banks that scammers groom their victims into setting up accounts with genuine crypto firms, with the crypto moved on to the scammer's wallet under the guise of a trading platform.
- They reiterated that Miss R was vulnerable at the time of the scam due to her personal circumstances and English not being her first language.
- Lloyds is responsible for ensuring unusual activity is questioned to satisfy themselves that their customer isn't falling victim to any financial harm. And they have a duty to mitigate any financial crime, fraud or scam concerns.
- This crypto exchange is well known to be used by scammers and a sudden change in spending habits should've alerted Lloyds to the potential risk posed to Miss R. And to satisfy themselves Miss R wasn't falling victim to a potential scam, Lloyds should've asked suitable open and probing questions – which they failed to do, thereby breaching BSI PAS 17271:2017.
- The payments were unusual for their vulnerable client given what they consider to be clear scam patterns here. Noting that the payments rose in value with each transaction and there being ten payments made in two days to a crypto merchant – which they consider highly suspicious.

Our Investigator's view didn't change. He acknowledged Miss R's personal circumstances and how difficult this had been for her. But he said Lloyds weren't aware of this at the time the payments were made, and it wouldn't be assessed under the CRM code as the payments weren't covered by it. And he would only expect a bank to intervene on payments that were unusual or suspicious – as it wouldn't be possible for banks to intervene on every payment. He didn't think Lloyds should've intervened just because the payments were made to a crypto exchange, as only a small number of transactions to crypto aren't legitimate. And here, he didn't think the payment activity warranted Lloyds doing anything more before processing them.

Our Investigator also clarified that the payments were made over a four-day period and that the transactions did decrease in value at times.

C still disagreed with our Investigator and so the matter has been passed to me to decide. They remained of the view that the payments were unusual for Miss R as she made three payments in less than 24 hours totalling £3,000. And that it's clear a scam was occurring given the payments rose in value with each transaction and there being ten payments to a crypto merchant in two days. C said this was highly suspicious and Lloyds failed to provide any protection to Miss R.

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 Miss R has been the victim of a scam, and I don't underestimate the impact this has had on her – particularly considering the difficult personal circumstances she has recently experienced too. I'm extremely sympathetic to Miss R's situation and I want to reassure her that I've given this matter very careful consideration. But while I accept she's lost a significant amount of money due to being deceived by the scammer, I must consider whether Lloyds is responsible for the loss she has suffered. I know this won't be the outcome Miss R is hoping for, but for similar reasons as our Investigator, I don't think they are. So, I don't think Lloyds has acted unfairly by not refunding the payments. I'll explain why.

Before I do, I'd like to say at the outset that if there is a submission I've not addressed; it isn't because I've ignored the point. It's simply because my findings focus on what I consider to be the central issue in this complaint – that being whether Lloyds was responsible for Miss R's loss.

My first consideration is in relation to the CRM code which can offer a potential means of obtaining a refund following scams like this one. But as our Investigator explained, while Lloyds has signed up to the CRM code, the payments unfortunately aren't covered under it. This is because the CRM code doesn't cover debit card payments or payments made to an account held in a person's own name – which is what happened here. And so, while I've noted C's point that Miss R should be refunded under the CRM code in light of her vulnerability, I can't fairly direct Lloyds to refund payments under the CRM code if they're not covered by it. I've therefore considered whether Lloyds should reimburse Miss R under any of their other obligations.

In broad terms, the starting position in law is that a bank is expected to process payments that their customer authorises them to make. It isn't disputed that Miss R knowingly made the payments from her Lloyds account – albeit under the direction of the scammer as she believed B to be a legitimate firm. And so, I'm satisfied she authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of her account, Lloyds are

expected to process Miss R's payments and she is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Lloyds to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

So, the starting point here is whether the instructions given by Miss R to Lloyds (either individually or collectively) were unusual enough to have expected additional checks to be carried out before the payments were processed.

When considering this, I've kept in mind that banks process high volumes of transactions each day. And that there is a balance for Lloyds to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. Here, the payments were made to a legitimate crypto exchange. And while there are known fraud risks associated with crypto, as scams like this have unfortunately become more prevalent, many individuals invest in crypto legitimately.

Having looked at Miss R's prior account usage, her account was typically used for low value day to day transactions. But while I accept the payments of £1,000 and £1,070 were higher in value than payments Miss R commonly made on her account, it isn't unusual for customers to make larger payments from time to time as part of normal account activity. Nor did these payments deplete Miss R's account balance or take her overdrawn. And so, I don't think the payments here, either individually or collectively, were of a monetary value whereby I would've expected Lloyds to have had sufficient reason to suspect Miss R was at risk of financial harm from fraud.

The nine payments made to the legitimate crypto exchange were also spread across a four-day period, varied in value, and didn't increase each time as C has suggested. And Miss R's prior account usage shows that she had sent multiple payments to other merchants on the same day previously. So, while payments made in a short period of time can be an indicator of potential fraud, this type of activity wasn't unusual for Miss R. I therefore wouldn't have expected Lloyds to have identified this frequency of payment as out of character for Miss R.

C is correct in saying that scammers do convince some victims to set up an account with legitimate crypto firms as part of a scam, as happened here. And while the crypto exchange in question here, like many others, are sometimes used for this purpose, it's also used by many individuals to invest in crypto legitimately. Because of this, I wouldn't necessarily have expected Lloyds to have carried out additional checks before processing the payments simply because they were going to a crypto merchant. But rather, I would expect them to take steps to protect customers that are proportionate to the identifiable risk.

It follows that, while there are circumstances where it might be appropriate for Lloyds to take additional steps or make additional checks before processing a payment, for the above reasons, I think it was reasonable for Lloyds to assume the payments here were being made for legitimate crypto purposes. And so, I think it was reasonable for Lloyds to process the payments upon receiving Miss R's instruction(s).

I've considered whether, on being alerted to the scam, Lloyds could reasonably have done anything to recover Miss R's losses, but I don't think they could. The only possible option for recovery here, given the payments were made by debit card, would have been for Lloyds to have attempted a chargeback against the payee – that being the crypto exchange. But given

these payments were for the purchasing of crypto with a legitimate firm, I don't think a chargeback claim would have been successful as Miss R received the service she paid for.

I have a great deal of sympathy for Miss R and the loss she's suffered. I appreciate she is the innocent victim of a scam at a time when she was highly vulnerable. But Lloyds weren't aware of Miss R's vulnerability and so, wouldn't have had reason to suspect she was at greater risk of falling victim to a scam. And it would only be fair for me to direct Lloyds to refund her loss if I thought Lloyds was responsible – and I'm not persuaded that this was the case. For the above reasons, I think Lloyds has acted fairly and so I'm not going to tell them to do anything further.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss R to accept or reject my decision before 25 October 2024.

Daniel O'Dell
Ombudsman