

The complaint

Miss B has complained Lloyds Bank PLC failed to sufficiently intervene causing her to fall victim to two authorised push payment (APP) scams or recover her funds after they occurred.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. In summary, Miss B fell victim to a fake job scam after she was contacted by a scammer and then a recovery scam after making her situation known online. She says she was told she would be paid for completing a number of tasks, but she would also have to pay in funds to the task platform periodically, using cryptocurrency via an exchange, to unlock more tasks and receive payment. After creating an account, as per the scam chat, she appears to have received two initial withdrawals of circa £10 and £60. Miss B realised she had been scammed when she did not receive her "earnings" and discovered it was impossible to complete the tasks as they always required further deposits.

Miss B's relevant transaction history is as follows:

Transaction	Date	Type of Transaction	Amount
1	15 January 2023	Card payment to B	£54
2	16 January 2023	Card payment to B	£420
3	16 January 2023	Card payment to B	£30
4	17 January 2023	Card payment to B	£500
5	17 January 2023	Card payment to B	£1000
6	17 January 2023	Card payment to B	£114
7	17 January 2023	Card payment to B	£51
8	17 January 2023	Card payment to B	£910
9	17 January 2023	Card payment to B	£910
10	17 January 2023	Card payment to B	£50
11	17 January 2023	Card payment to B	£80
12	17 January 2023	Card payment to B	£53.07
13	17 January 2023	Card payment to B	£1000
14	17 January 2023	Card payment to B	£539
15	21 January 2023	Card payment to B	£60
16	21 January 2023	Card payment to B	£100
17	22 January 2023	Card payment to B	£125
18	22 January 2023	Card payment to B	£100
19	22 January 2023	Card payment to B	£50
20	22 January 2023	Card payment to B	£40
21	22 January 2023	Card payment to B	£70
22	22 January 2023	Card payment to B	£95
23	22 January 2023	Card payment to B	£500
24	22 January 2023	Card payment to B	£500
25	22 January 2023	Card payment to B	£300
26	22 January 2023	Card payment to B	£300

27	22 January 2023	Card payment to B	£150
28	22 January 2023	Card payment to B	£600
29	22 January 2023	Card payment to B	£200
30	22 January 2023	Card payment to B	£300
31	22 January 2023	Card payment to B	£300
32	22 January 2023	Card payment to B	£350
33	22 January 2023	Card payment to B	£400
34	23 January 2023	Card payment to B	£70
35	23 January 2023	Card payment to B	£50
36	23 January 2023	Card payment to B	£30
37	23 January 2023	Card payment to B	£30
38	23 January 2023	Card payment to B	£30
39	25 January 2023 (date as per statement)	Card payment to T	£35
40	25 January 2023 (date as per statement)	Card payment to T	£120
41	26 January 2023 (date as per statement)	Card payment to T	£150
42	26 January 2023 (date as per statement)	Card payment to T	£350
43	26 January 2023 (date as per statement)	Card payment to T	£400
44	26 January 2023	Card payment to B	£356
45	30 January 2023	Card payment to B	£400
46	30 January 2023	Card payment to B	£350
47	1 February 2023	Card payment to B	£150
48	3 February 2023	Card payment to B	£300
49	6 February 2023	Card payment to B	£100
50	9 February 2023	Card payment to B	£60
51	25 February 2023	Card payment to B	£20
52	26 February 2023	Card payment to B	£32
53	27 February 2023	Card payment to B	£40
54	6 March 2023 (date as per statement)	Card payment to B	£15

Firstly, I should say that it is difficult to establish exactly which payments were part of the scams as Miss B has stated different payments at varying points. For completeness, I've included the additional payments from her statements that Miss B may well also have made to the scams. However, all parties should be aware of these payments and they ultimately do not change the outcome.

Our Investigator didn't uphold the complaint as she did not find that the payments should have been of any concern to Lloyds. She was also not convinced, considering Miss B spoke with Lloyds after her card was blocked but continued making payments, that any intervention would have prevented her losses. As our Investigator couldn't resolve the matter informally the case has been passed to me for a final 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 aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

I don't doubt Miss B has been the victim of a scam here – she has lost a large sum of money and has my sympathy for this. However, just because a scam has occurred, it does not mean she is automatically entitled to recompense by Lloyds. It would only be fair for me to tell Lloyds to reimburse Miss B for her loss (or a proportion of it) if: I thought Lloyds reasonably ought to have prevented all (or some of) the payments Miss B made, or Lloyds hindered the recovery of the payments Miss B made – whilst ultimately being satisfied that such an outcome was fair and reasonable for me to reach.

I've thought carefully about whether Lloyds treated Miss B fairly and reasonably in its dealings with her, when she made the payments and when she reported the scam, or whether it should have done more than it did. Having done so, I've decided to not uphold Miss B's complaint. I know this will come as a disappointment to her and so I will explain below why I've reached the decision I have.

I have kept in mind that Miss B made the payments herself and the starting position is that Lloyds should follow its customer's instructions. So, under the Payment Services Regulations 2017 (PSR 2017) she is presumed liable for the loss in the first instance. I appreciate that Miss B did not intend for her money to ultimately go to a scammer – but she did authorise these payments to take place. However, there are some situations when a bank should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made.

Considering the relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time - 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 payment service providers 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 decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So, I've thought about whether the transactions should have highlighted to Lloyds that Miss B might be at a heightened risk of financial harm due to fraud or a scam.

Lloyds should have identified when Miss B's payments were going to a cryptocurrency exchange as B, the merchant she sent most of her funds to, is well-known. However, that doesn't mean they *all* should automatically be treated as suspicious; particularly when there are no other concerning factors about the payments. Many banks have made the commercial decision to prevent their customers from using their service to send money to cryptocurrency exchanges. Albeit investing in cryptocurrency is a highly risky endeavour, it is ultimately a legitimate one and so certain banks and Electronic Money Institutions (EMI) do permit transfers to cryptocurrency exchanges.

I've considered Miss B's payments in the context of whether they were unusual or uncharacteristic of how she normally used her account. Having done so, the values of the payments were of fluctuating amounts that were not remarkable enough to have caused Lloyds any concern. These transactions didn't leave Miss B's account at particularly unusual balance levels and she still had funds available for her normal spending. Miss B transferring funds into her current account before sending them elsewhere is also not an uncommon way for an account holder to use their account, whether for spending or investing. I did note that on some of the days there were multiple transactions occurring, which in certain situations could be an indication that someone is being scammed. But in this instance, given the size of them, I don't think that intervention was merited. I do not consider enough of a pattern formed here to suggest Miss B might be at a heightened risk of financial harm due to fraud or a scam. So, I'm not persuaded Lloyds reasonably ought to have been concerned here.

I have noted that Lloyds did block Miss B's card when she attempted to make a £30 payment. In response she telephoned Lloyds, on 23 January 2023, to unblock the card and had a discussion with an agent. She confirmed in this call she would not be using B for further payments. She said no-one had informed her to make the current payment she was attempting and she was just sending her funds to the cryptocurrency exchange. Lloyds highlighted to Miss B the importance of reviewing their scam information on their website and to be wary of sending funds. Yet, Miss B decided to proceed to send further payments via cryptocurrency to the scammer anyway. I've not seen any evidence that Miss B's behaviour had changed, or that anything had occurred to show the influence the scammer had over her was waning, as this scam progressed. Additionally, at this stage Miss B was aware she had been involved in a scam before that involved sending funds via B. So, I would have expected her to approach requests for further funds with caution. I have noted that she was not forthcoming with Lloyds during this call and so I am not persuaded Lloyds could have prevented her losses.

For completeness, even had one of Miss B's payments triggered a scam warning, because of the frequency of payments causing concern, the most appropriate and proportionate, based on her payments being to a cryptocurrency exchange, would have been a tailored cryptocurrency investment warning. I would not have expected Lloyds to provide a specific job scam warning at the time of these payments. As she was not falling victim to an investment scam, I do not think this would have resonated with her and so I do not think it would have stopped her making further payments. This is especially so when considering Miss B's later payments; as a discussion with Lloyds via telephone did not. So, I can't fairly say Lloyds would have been able to give Miss B any information that would have led her to do anything differently. So, I think had they intervened with a tailored warning Miss B would have still proceeded with the payments.

I've noted Miss B has referenced decisions that she believes are close to her circumstances. However, we consider each case on its own individual merits and although she believes the circumstances of other decisions seem to be similar, there are key differences.

Recovery

The only method of recovery Lloyds has for payments made by card is to request a chargeback. However, Miss B didn't make the card payments to the scammer directly, she paid a cryptocurrency exchange. The service provided by the cryptocurrency exchange would have been to convert or facilitate conversion of Miss B's payments into cryptocurrency. If these funds had not already been transferred to the scammer, they would be in her control to access as and when she chose. The fact that the cryptocurrency was later transferred to the scammer doesn't give rise to a valid chargeback claim against the merchant Miss B paid. Therefore, I won't be asking Lloyds to do anything further.

The Contingent Reimbursement Model Code

Although Lloyds has signed up to the Contingent Reimbursement Model Code, the transfers Miss B made from her account aren't covered by the Code because they made the payments from her Lloyds account to her other account and not to another person. I cannot fairly and reasonably say that Lloyds should have to refund payments under the Code when it doesn't apply here.

So, in light of all of the above findings, there's no fair and reasonable basis under which I can ask Lloyds to reimburse Miss B's loss.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 20 June 2025.

Lawrence Keath
Ombudsman