

The complaint

Mrs B complains that Lloyds Bank PLC won't refund money she lost to an investment scam.

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 2022 Mrs B was the victim of an investment scam – with a firm I'll refer to as 'P'. And, as part of the scam, she sent funds by international money transfer and via legitimate crypto exchanges to P. Mrs B made, or attempted to make, the following payments:

Date (statement)	Туре	Amount	Fees
27 January 2022	Faster payment	£1	
9 February 2022	Debit card	£169.26	£5.06
3 March 2022	Debit card	£1,000	
4 March 2022	International money transfer	£3,866.64	
8 March 2022	International money transfer	£14,900	
16 March 2022	Debit card	£9,950	
16 March 2022	Debit card	£4,500	
16 March 2022	Debit card	£4,227.87	
17 March 2022	International money transfer	£8,702.46	
23 March 2022	International money transfer	£8,633.97	
28 March 2022	International money transfer	£15,158.08	
31 March 2022	International money transfer	£9,666.08	
11 April 2022	International money transfer	£25,045.34	
19 April 2022	International money transfer	£12,895.46	
21 April 2022	Debit card	£4,157.38	£124.30
21 April 2022	Debit card	£4,157.38	£124.30
22 April 2022	Debit card	£4,167.78	£124.61
28 April 2022	Debit card	£4,231.59	£126.52
28 April 2022	Debit card	£4,231.59	£126.52
28 April 2022	Debit card	£4,231.59	£126.52
28 April 2022	Debit card	£4,231.59	£126.52
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£4,252.93	£127.16
23 May 2022	Debit card	£2,551.76	
24 May 2022	International money transfer	£8,876.95	
	Total	£115,253.85	£1,774.47

^{*}The unsuccessful payments are highlighted in bold and aren't included in the total.

Mrs B also received a £1 credit on 1 February 2022. This puts her total loss, including fees, to £117,027.32.

Mrs B realised she'd been scammed when she requested a withdrawal of funds but it wasn't received. She complained to Lloyds in August 2022 asking to be reimbursed. In short, she said:

- She was contacted by P after responding to a trading advert endorsed by Martin Lewis. And before investing she checked Trustpilot and found P had positive reviews. She also spoke with her daughter and a work colleague who confirmed her initial impressions that it was all legitimate. There wasn't anything that led her to believe P wasn't a genuine firm.
- The scammer was very professional and knowledgeable. And every time he explained details of the trades, she checked what she was told was true. This wasn't because she was suspicious but rather she was trying to understand what was meant by 'share splits' and other aspects of what she was being told. As it was correct every time, it thereby added to her confidence the opportunity was genuine. The scammer also had her download an app showing the commodities they were dealing in, the amounts invested and profits.
- She received a text message from Lloyds for the first transaction asking her if she'd authorised it, to which she replied 'yes'. She then had to go into branch due to a larger payment being blocked and her online account being suspended. Lloyds took it upon themselves to call the police and told her she was being scammed but didn't provide her any evidence to that effect, as they said it was in the hands of the police. A police officer who attended the bank told her the same, but without providing evidence to show she was being scammed either. The police officer also reported the matter to Action Fraud on her behalf, even though she hadn't requested it as she was convinced it was genuine.
- The scammer took control of her phone and made transactions on her behalf doing so in lots of €5,000 at a time. She also had no idea the bank would charge for this type of transaction either.
- When she tried to withdraw funds at the end of May 2022, the scammer said he would rather send the whole amount than only a portion of it so that he would get all his commission. But he asked if she could wait until the end of June as withdrawals were dealt with quarterly. She then received a receipt form for the withdrawal request that showed the firm had change from P to another firm, to which I'll refer to as 'A'. She reviewed A online and was horrified to see it wasn't a good company and she couldn't understand how her trading with P had changed to A. She also searched P again online and found that they had since gone out of business.
- On 25 May 2022 she was visited by an individual, that I'll refer to as 'Mr Y', because
 of the report to Action Fraud. Mr Y convinced her she'd been scammed as, up to this
 point; she believed it was all genuine.
- She was told by the scammer on 7 July 2022 that the funds had been released and would be received in a few days. By the end of July, with the funds still not received, she knew she had definitely been scammed.
- Her intention wasn't to make millions but just enough to survive on alongside her state pension and possibly some home improvements. And it's not just the money that has been taken from her but it has also left her vulnerable, with her trust in people and confidence impaired. As far as she can see, she did everything correctly by checking Trustpilot and checking the information given to her by the scammer.

Lloyds didn't uphold the complaint. In short, they said:

- Although Mrs B looked P up on Trustpilot and sought the opinion of her daughter, a
 further independent search of the company name would've brought up negative
 reviews and warnings about fake celebrity endorsements. Mrs B could've also
 checked the Financial Conduct Authority (FCA) register to see if P were registered
 and licensed to trade in the UK. Most crypto isn't regulated in the UK and the FCA
 website offers warnings about the risks involved with this type of investment.
- Given the amounts and frequency, they didn't feel it necessary to intervene before
 processing the first four payments. But they thought the £14,900 payment was
 unusual activity for Mrs B and so they stopped it leaving to speak with her. After
 speaking with Mrs B, they still had concerns so referred her to branch where she
 spoke with their fraud team. Their fraud team discussed the possibility of it being a
 scam and warned Mrs B of the risks which led to Mrs B cancelling the payment.
- Despite their warning, Mrs B made four further payments over the next two weeks. But on 11 April 2022, they stopped a £25,045.34 payment and asked Mrs B to go into branch again. Mrs B did so the next day and because they had concerns she was being scammed, they asked the police to attend and speak to Mrs B about it. The police took information away about the payments Mrs B had already made and confirmed they were happy for the blocks on her account to be removed. Mrs B told them she wouldn't make the £25,045.34 payment but, as they still had concerns, they left the block in place. This meant all payments Mrs B attempted would need to be authorised by them first.
- Mrs B called them on 19 April 2022 saying the block was impacting her ability to use her account, and that she wanted to send more money. They spoke at length about scams and the risks involved with this type of investment, although removed the block as they agreed they couldn't permanently restrict access to Mrs B's account and acknowledged it was impacting her day-to-day banking. Mrs B confirmed she'd understood what they'd told her and that she'd complete further checks.
- Within two hours of that call, Mrs B tried to make another payment which was stopped again. When Mrs B called them she spoke with the same agent she'd spoken with earlier, and he reiterated the risks to Mrs B again and that, if it was a scam, they wouldn't be able to get her money back. Mrs B said she was aware of this but she was sure it was genuine and would accept responsibility if it turned out to be scam.
- Later that day, three further payments for €5,000 were made using Mrs B's debit card. The scammer logged on to Mrs B's phone using remote access software and asked her to input the card number and payment details. The payments were sent with Mrs B's consent to an account held in her own name. Mrs B then continued to make debit card payments to the same account until 20 May 2022, before making a further international bank transfer on 24 May 2022.
- Sending money by international bank transfer is like sending cash as, once it has been processed, it can't be cancelled or reversed. They'd contacted the beneficiary banks and asked them to return the funds but sadly this wasn't possible. This was because four of the banks confirmed no funds remained in the accounts, and the other two banks hadn't responded.
- This type of scam is called an authorised push payment (APP) scam. The Contingent Reimbursement Model (CRM) code was set up in 2019 with its aim to protect customers falling victim to APP scams and who are tricked into sending payments to a fraudster via Faster Payment within the UK. It doesn't however cover money sent outside of the UK or debit card payments. Therefore, they hadn't been able to assess Mrs B's claim under the CRM code.

- The debit card payments also didn't meet the requirements for a chargeback claim to be raised. This is because the payments were sent to an account held in Mrs B's own name, made with her authority and the service having been provided.
- Although they couldn't consider the payments under the CRM code, they assessed
 their duty of care for these payments. And they didn't think they could've done
 anymore to protect Mrs B or make her aware of the risks. They spoke to her on
 several occasions and even contacted the police. Despite their many interventions
 and warnings, Mrs B continued to make payments. And so, they couldn't offer a
 refund of the money she'd lost.

The complaint was referred to the Financial Ombudsman. Our Investigator didn't think Lloyds were responsible for Mrs B's losses. This was because she thought Lloyds took reasonable steps to protect Mrs B from the scam in relation to some of the payments she attempted to make before processing them. For example, Lloyds told Mrs B that she was being scammed and invoked banking protocol — which similarly led to the police warning Mrs B she was being scammed and contacting Action Fraud on her behalf. And although our Investigator thought Lloyds should've intervened before processing other payments, she didn't think this would've made a difference — as she considered Mrs B would've tried to make the payment at another time, or in a different way, due to her being convinced the investment was legitimate.

Our Investigator also thought Lloyds had taken reasonable steps to recover the funds by contacting the receiving banks but, unfortunately, this wasn't successful. And given the debit card payments were made to an account held in Mrs B's own name with legitimate crypto exchanges, there wasn't any reasonable prospect of success for chargeback claims – as Mrs B received the service from the crypto exchange, that being the conversion of the funds into crypto before it was sent to the scammer.

Mrs B disagreed and so, the matter has been passed to me to decide. In short, Mrs B added:

- She clarified her complaint is that Lloyds and the police insisted her involvement was a scam but they didn't produce any evidence to support their claim, which is what she would've expected. She hasn't said Lloyds didn't do enough to protect her or that they failed in their duty of care.
- When the policeman attended the branch, she showed him an app showing a list of
 the investments but he said this didn't mean anything although again, he gave no
 reason for this. The scammer, who she believed, gave her reasons for why they were
 investing in a particular product such as, due to the Russia-Ukraine war having
 started, why the payments were sent internationally for it to be invested in oil and
 gas.
- The scammer convinced her that if she paid her taxes in one hit, it would only be 15% rather than the 20% applicable in the UK. Although she told the scammer she would prefer to use the UK tax system, he was clever enough to convince her otherwise. And even though she explained to him the bank wouldn't allow another payment to go through, it was the scammer that found a way around this – not her.
- Mr Y wasn't from Action Fraud but rather, she believes he was from a support group for those affected by scams. Nevertheless, she accepts that at the point of this visit she was still convinced everything was genuine although he was able to convince her otherwise and provided her literature when doing so. Unfortunately, this was too late as she had already paid the taxes. If Lloyds or the policeman had looked into the wider circumstances and spoke with her as Mr Y did, explaining why it was a scam, it would've have been a completely different outcome.

- Before proceeding to invest, she reviewed Trustpilot and ran the opportunity past her daughter and a work colleague. She also checked the information the scammer provided her – such as about 'share-splits' – and it all checked out.
- She wasn't aware of the bank charges for the international transfers which has led to her losing even more.
- She found it lucky that she could speak with P, rather having to deal with matters
 online. And found it reassuring that the scammer showed her on the app what they
 were investing in and why. She was also further reassured by the scammer when he
 told her he was looking forward to sending the money back, with profits, so the bank
 would realise it wasn't a scam.
- She tried to get her money back and she can explain how, as well as asking Mr Y to confirm this, if required.
- Given she is 'old school', she believed the investment was the new way business was done these days.
- Paperwork was requested but other than a payment authorisation having been received, no other paperwork materialised.

Mrs B requested that she at least be partly reimbursed by Lloyds.

Before I go on to explain the reasons for the decision I've reached on this complaint, I want to clarify that I'm only considering the actions of Lloyds. So, while I appreciate Mrs B has made reference to the actions of the police I won't be considering or commenting on them here.

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 Mrs B has lost a significant amount of money and I don't underestimate the impact this has had on her – both financially and emotionally. But while I know this won't be the outcome she is hoping for, I don't think Lloyds has acted unfairly by not refunding her loss for similar reasons to our Investigator. I'll explain why.

At which point, I'd like to firstly acknowledge that Mrs B had put forward a number of points for my consideration in support of her complaint. I want to reassure Mrs B that I've given careful consideration to all the evidence provided. And so, I'd like to reassure Mrs B that if I don't mention a particular point, it's not because I haven't considered it, but I've focussed instead on what I believe to be important to the outcome of this complaint.

As Lloyds has pointed out, these payments aren't covered by the CRM code – which can offer a potential means of obtaining a refund following APP scams. This is because it doesn't cover debit card payments, money sent outside of the UK or payments made to an account held in a person's own name. I've therefore considered whether Lloyds should reimburse Mrs B under any of their other obligations.

In broad terms, the starting position in law is that a bank is expected to process payments their customer authorises them to make. I understand that here, Mrs B allowed the scammer to take control of her phone to make some of the transactions. While Mrs B may not have necessarily processed some of the transactions herself, it seems she knowingly consented to the scammer doing so on her behalf. I appreciate Mrs B was tricked by the scammer as she thought it was a genuine investment opportunity. Nevertheless, I'm satisfied the payments were authorised by Mrs B. So, under the Payment Services Regulations 2017 and

the terms of the account, Lloyds are expected to process the payments and Mrs B is presumed liable for the loss in the first instance.

However, taking into account 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 Mrs B to Lloyds were unusual enough - in relation to her typical account activity – to have expected Lloyds to have identified Mrs B was at risk of financial harm from fraud.

Having reviewed Mrs B's account statements, I don't think the first four payments were unusual enough for Lloyds to have been concerned she was at risk of financial harm from fraud. This is because, although Mrs B typically used her account for low value day to day transactions, it's common for customers to make occasional transactions of a higher value. Lloyds did however suspect Mrs B was at risk of financial harm at the point she attempted to make the £14,900 payment. I agree this was reasonable – as the transaction was out of character for Mrs B given both its value and as it was an international payment. And so, I've considered whether the additional checks Lloyds carried out were sufficient here.

Upon questioning about the payment, Mrs B explained to Lloyds that it was for crypto investment purposes and she was being assisted by a broker. Lloyds referred Mrs B to branch for the payment to be discussed further before it could be released. Mrs B then had a lengthy conversation with Lloyds about the payment, speaking with an agent that specialised in crypto fraud. The agent said he thought Mrs B was falling victim to fraud and asked Mrs B various questions around the investment and what checks she'd carried out to ensure the broker was genuine. Mrs B explained that she wasn't sure how to verify the person but they seemed genuine and they'd told her they were regulated. She'd also carried out an internet search on the IBAN details she'd been provided. The agent then gave advice to Mrs B that included:

- A broker can't be verified from just a phone call or message. And so, he encouraged
 Mrs B to meet the broker in person (not just a video call). She should also ensure any
 broker is credible such as an independent financial adviser who she can meet in
 person, albeit they wouldn't deal with crypto.
- She should be the only person that can access the funds in the crypto account. This is because, if the broker is a scammer, they can transfer the funds out and there wouldn't be anything to prevent them. So, she shouldn't be transferring any funds for someone else to control.
- He didn't think Mrs B would get the (circa) £4,000 she'd previously sent back. He recommended she request for it to be returned from the broker saying she's in a tricky spot. At which point, he suspects the broker would ghost her or they'd lock the account down thereby confirming it to be a scam.
- If Mrs B can't retrieve the funds, then she should let Lloyds know so they can attempt to recover them (although this would be unlikely).

The payment didn't go ahead and I'm satisfied Lloyds gave Mrs B appropriate and tailored warnings about crypto investment scams at this point – including that, to try and uncover whether it is a scam or not, Mrs B should try to request for the funds to be returned.

Just over a week later, Mrs B tried to make three debit card payments on the same day – £4,228.87, £4,500 and £9,950. These payments weren't successful and Lloyds didn't speak with Mrs B about them. Mrs B then proceeded to make four successful international

payments - £8,702.46, £8,633.97, £15,158.08, £9,666.08 - over the next two weeks. Lloyds didn't speak with Mrs B before processing any of these payments.

Lloyds did however speak with Mrs B on several occasions regarding the £25,045.34 and £12,895.46 payments she attempted on 11 and 19 April 2022 respectively. Again, I think it was reasonable for Lloyds to suspect Mrs B remained at risk of financial harm from fraud given the transactions were of significantly high values based on Mrs B's prior account usage, they posed increased risk due to being international payments and as Lloyds had reason to believe Mrs B had been previously targeted by scammers (and so was at risk of being targeted again).

Upon questioning about the payments, Mrs B reiterated that they were for investment purposes with the same broker. Mrs B explained that she spoke with the broker on a daily basis whom she'd found after answering a crypto advertisement. She also confirmed that she hadn't seen the broker in person nor did he have a website. But she'd been shown that a profit had been made on the trading account – and that she was hoping to receive the profit within the next couple of weeks. Lloyds still had concerns Mrs B was falling victim to fraud and so referred her to branch again.

While in branch, Lloyds invoked Banking Protocol – which is an initiative that allows banks to call the police in situations whereby they suspect a customer is at risk of sending funds to a scammer. A policeman attended the branch and spoke with Mrs B at length about the payment and those she had previously made. The policeman explained to Mrs B that they thought the investment was a scam and took details of what happened to refer the matter to Action Fraud. They also said a block on the account could be removed as Mrs B had confirmed she wouldn't be making any more payments. As part of the conversations with Mrs B about the attempted £25,045.34 and £12,895.46 payments, and in addition to invoking Banking Protocol, Lloyds gave advice/warnings to Mrs B that included:

- They were worried about the investment opportunity as if they can't confirm the broker is genuine, with their own website, then it does seem suspicious. And with these types of transactions, people shouldn't rely just on advertisements.
- It's highly unlikely they will be able to recover the funds if something goes wrong due to it being sent internationally.
- If there is an adviser involved with the investment then it's highly likely a scam as
 there aren't any FCA regulated advisers for crypto. And, if it's a scam, the adviser
 could take all the funds out of Mrs B's account.
- Genuine crypto websites would only allow Mrs B to have access and control of her account with no advice being provided by an adviser.
- In response to Mrs B saying she was expecting to receive profits from the investment at the end of April 2022, they recommended she not make any further payments until then as, at that point, they would know what's happened with the investment and whether it was genuine.
- They have a responsibility to try and protect customers from scams and they're worried she is making payments to a fraudster. They can't however legally stop Mrs B from using her own money.
- They 100% guarantee that any more she sends to this broker will be lost as this isn't how crypto investing works. They reiterated that Mrs B should be the only person who has control of her crypto account. And if anyone else says they can invest it on her behalf then they are 'filthy liars' and will rob her blind as they've seen this on far too many occasions.
- If the funds are sent to the broker, they 110% guarantee the money will be lost. There are plenty of genuine crypto exchanges that she can invest in crypto herself with UK account details with the funds showing in her own account. Whereas if she

sends it to someone else then they will have to show her what is happening with the money. But even if it is in her name, the broker can transfer it out to themselves. And it's not possible to track this so the money would be completely lost.

- They're not saying Mrs B shouldn't invest in crypto but she needs to be in control of the funds.
- They're worried the broker is fraudulent and lying to Mrs B.
- They recommended that's Mrs B didn't send any further funds.

These payments didn't go ahead and I'm similarly satisfied that Lloyds gave Mrs B appropriate and tailored warnings/advice about crypto investment scams at this point – including that they highly suspected it to be scam, that only Mrs B should have access and control to her funds and advising her to wait until the end of April to see if the expected profits were received before investing further.

After this, Mrs B went on to make a further 14 debit card payments – totalling about £59,000 – and a single international payment - of £8,876.95 - to the scam between 21 April and 24 May 2022. Lloyds didn't speak with Mrs B before processing any of these payments – although they did block a £2,551.76 debit card transaction on 23 May 2022. While I consider Lloyds took appropriate steps to protect Mrs B from the scam in relation to the payments she attempted between 8 March and 16 March 2022, as well as those on 11 and 19 April 2022, I've considered whether Lloyds ought to have done more before processing other payments. Specifically, those between 17 and 31 March 2022 and 21 April 2022 onwards. And, if so, whether they're responsible for Mrs B's loss as a result.

I've thought carefully about this and, although I understand the need for Lloyds to allow customers to operate their accounts and process legitimate transactions, the obligation to protect them from financial harm from fraud remains. And, in my view, I consider the aforementioned transactions should've been identified by Lloyds as likely being in relation to fraud – as they were likewise unusual and out of character based on Mrs B's typical account usage and Lloyds knew she'd been targeted by fraudsters. Therefore, in the knowledge Mrs B was being scammed – shown by the agent providing guarantees that any money sent to this broker would be lost - I think Lloyds ought to have continued to take appropriate steps to warn Mrs B about the associated risks of making these types of payments. This could've included blocking payments like these to carry out additional checks before processing them.

I must however consider whether Lloyds' actions, or inaction, relating to these payments is the cause of Mrs B's loss. Essentially, do I think Mrs B wouldn't have suffered the loss she did had it not been for this. And after careful consideration of Mrs B's specific circumstances, I don't think I can fairly conclude that here. I say this because Lloyds did take significant steps to protect Mrs B on several occasions, including invoking Banking Protocol, in relation to other payments. Yet, despite this, Mrs B remained insistent the investment opportunity was genuine and that it wasn't a scam and proceeded to make further payments. Mrs B even told Lloyds that she appreciated they were trying to protect her but that she would take full responsibility, and so it would be 'on her shoulders' if it turned out to be fraud. And so, even though she thought the bank had done everything they could to protect her, she was going with her gut instinct.

Lloyds also advised Mrs B on two occasions to not make any further payments until funds had been returned. This included the circa £4,000 that was initially invested prior to Lloyds speaking with her as well as, later, the profits Mrs B said she was expecting to receive at the end of April 2022. It seems Mrs B chose to ignore this advice and proceeded to make further payments without receiving any returns.

I'm also mindful that after Lloyds successfully stopped payments being processed, Mrs B made subsequent payments to the scam via different methods – such as the 14 debit card transactions after the international payments were blocked. I understand, from what Mrs B has said, that this change of payment method was at the direction of the scammer – likely as a way of avoiding detection. And so, given Mrs B's evident strength of belief P were genuine and the clear trust she placed in them, I think even if Lloyds had stopped further transactions then it's more likely than not she would've found alternative ways of making payments – such as sending them through another bank, electronic money institution or card provider. Particularly as I think it's probable the scammer, with whom Mrs B was clearly under their spell, would've been able to have successfully influenced her into taking such actions. I say this as it's been shown the scammer was able to persuade Mrs B to allow them to take control of her phone by using remote access software to send further payments despite powerful scam warnings and advice having been provided by Lloyds. I therefore think, even if Lloyds had taken further steps to try and protect Mrs B, I'm not convinced it would've made a difference.

I appreciate Mrs B has said that Lloyds didn't provide any evidence to show P was a scam firm. But while I'm sympathetic to Mrs B's situation, I can't fairly hold Lloyds responsible for that. This is because unless there is, for example, a regulatory warning about a firm then it is difficult for a bank to evidence – with absolute certainty – that payments are being made as part of a scam. And providing such definitive evidence would, in some circumstances, be beyond what's reasonable and proportionate to expect a bank to do. Instead, it would be reasonable for the bank to explain why they think it is scam – referring to the similarities of known scam methods and the associated risks involved with making such payments. I'm satisfied that Lloyds did this here as well as seeking the support of the police to reinforce their position. Sadly, while Mrs B seemed receptive to what she was being told at times, it appears she ultimate chose to ignore Lloyds' advice and continued to believe the investment was genuine.

I appreciate Mrs B was deceived by P and I'm not trying to place blame on her for what happened – as I understand she did what she thought were reasonable checks before proceeding to invest. But likewise, and in these specific circumstances, I can't reasonably hold Lloyds responsible for Mrs B's loss for the reasons I've explained.

Upon being informed of the scam, Lloyds contacted the beneficiary banks to try and recover the funds Mrs B lost – which is what I would expect in these circumstances. Unfortunately, this wasn't successful as some of the banks didn't respond and, those that did, confirmed the funds had been removed. In respect of the payments made by debit card, the only possible option for recovery would've been via chargeback claims. But given these payments were made to accounts held in Mrs B's own name with legitimate crypto exchanges, any chargeback claim would have likely been unsuccessful as Mrs B received the service she paid for. As such, I think it was reasonable for Lloyds not to have raised chargeback claims here. It follows that I'm satisfied Lloyds acted reasonably in this respect.

I'm sympathetic to Mrs B's situation as I realise she's suffered a significant financial loss. But it would only be fair for me to direct Lloyds to refund her loss if I thought the bank 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 Mrs B to accept or reject my decision before 24 April 2024.

Daniel O'Dell Ombudsman