

The complaint

Ms M complains that Lloyds Bank PLC (“Lloyds”) failed to refund transactions she didn’t recognise.

What happened

Ms M noticed a number of transactions had been recorded on her account that she didn’t recognise. She reported them to Lloyds and confirmed that she hadn’t made them herself. Each of the transactions also included a “non gb fee” indicating they were made with overseas merchants. Ms M asked for a refund of these disputed transactions.

Ms M’s card was cancelled, and Lloyds looked into the payments. Lloyds identified that all the transactions had been made using Ms M’s usual device, from an IP address common to other undisputed payments and delivery details matched her home address.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

Based on this evidence, Lloyds declined to make a refund to Ms M who was left unhappy with their handling of her situation. She made a complaint to Lloyds about their decision and the way her request for a refund had been dealt with.

Lloyds again examined the payments but didn’t change their position regarding a refund. They did accept that Ms M had been on the phone for an overly long time and made a £15.00 payment towards her phone costs.

Ms M continued to disagree with Lloyds and brought her complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to Ms M’s complaint and both parties were asked for information about the situation.

Ms M was able to say that:

- She was unaware of the disputed transactions prior to checking her account.
- She hadn’t dealt with the merchants listed on her account.
- IP addresses and personal data can be accessed by fraudsters.

Lloyds provided details of their records concerned with Ms M’s claim, which in summary said:

- Ms M reported purchasing an item from abroad prior to these disputed transactions which may be linked to them.
- Ms M told Lloyds that no one else had access to her card and she hadn’t clicked on any suspicious links.

- Genuine transactions were compared to the disputed transactions and IP address data matched.
- Some of the disputed transactions were verified through an additional security step involving Ms M's registered device.
- There was no evidence of a compromise of Ms M's account.
- £15 was paid to recognise the length of time Ms M was on the phone.

The investigator prepared a report based on an assessment of the available evidence and didn't recommend that Lloyds make a refund. They commented that:

- The disputed transactions were made using Ms M's card details including the security code.
- Further security was required for some of the transactions requiring a response from Ms M's device using a One Time Passcode (OTP).
- The payments used Ms M's usual device (phone).
- It wasn't plausible that an unknown fraudster would have access to Ms M's device or acquire the OTP.
- The IP address matched to normal use of the account.

Ms M strongly disagreed with the outcome of the investigator's investigation and commented that:

- The transactions were fraudulent.
- Ms M didn't subscribe to anything.
- Ms M believed that audio recordings had been listened to and wanted copies of them.
- Ms M didn't believe her complaint had been dealt with objectively.
- The situation was impacting her mental health.
- Ms M was honest and didn't like the implication that she was responsible.
- Ms M didn't believe her side of the story had been considered.
- Ms M wanted a further review of her complaint.

As no agreement could be reached, the complaint has now been passed to me for 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'd like to clarify a few matters before going on to look at the evidence submitted by both

parties. Ms M believed that audio evidence (conversations) had been considered and not sent to her. Having examined all the evidence in this complaint – there are no audio recordings from the bank that were sent to our service. I think there's been a misunderstanding with the use of the word "audit". I hope Ms M understands that she's been provided the evidence relied on in the investigator's review.

Secondly – Ms M has raised issues that somehow her integrity has been questioned. That's not the case at all with her complaint. There's no suggestion here that Ms M has been anything other than genuine when she raised these payments that she didn't recognise.

I have to base my decision on the available evidence and if that indicates it was likely Ms M who was responsible, then that is the extent of the decision. I have no doubt that Ms M strongly asserts that she wasn't responsible, and I've taken that into account. But, the evidence from Lloyds indicates a number of connections between Ms M, including her device, the IP address and her card details. Based on this, I won't be recommending Lloyds make a refund and I'll explain why.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Lloyds can hold Ms M liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them. Lloyds can only refuse to refund unauthorised payments if it can prove Ms M authorised the transactions, but Lloyds cannot say that the use of the card details for online payments conclusively proves that the payments were authorised.

Unless Lloyds can show that consent has been given, it has no authority to make the payment or to debit Ms M's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Ms M. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Ms M responsible for the disputed transactions or not.

It's the case here that Lloyds can show:

- A matching IP address used by Ms M for both undisputed and disputed transactions.
- Her card details were used to make the payments, including the three-digit security number.
- OTPs were sent to Ms M's device and were responded to.
- Ms M's home address was used in the payment process.

During the investigation, Lloyds recorded that Ms M hadn't provided her card details to anyone else or clicked on suspicious links.

In order to carry out these transactions, access to Ms M's card details, home address information and her device would be required. Whilst I accept it's possible to obtain some of these details, for example her home address information and some of her card details from use on other websites, I don't think it's likely that all the elements were obtained by an unknown third party. Lloyds data showed a consistent IP address was used as part of the payment process. What that means is that the device was registering the IP data when used. I don't doubt that this IP information could be obtained by fraudsters, but I'd question why someone would go to the trouble of purposely implicating Ms M when all they had to do was to use her details to make purchases?

The OTP's were also recorded as being received and responded to. There's no evidence to show a different device was used to receive them or had been used in the transaction process. So, what that means here is that Lloyds evidence points to Ms M's actual device (her regular phone) being used as part of the payment process.

The overall evidence shows that it's unlikely anyone else was involved and there was no compromise of Ms M's account. Her card details were used (including the three-digit security code), her own phone was used from a regular IP address and her home address was entered into the payment systems.

Whilst I understand Ms M's strength of feeling here that she wasn't responsible, and I'm sure she'll disagree with me, the evidence that I've considered leads me to the conclusion that, on the balance of probabilities, it was more likely than not that Ms M authorised or allowed her card details to be used to make the payments. So, taking everything into account, I think it is fair and reasonable for Lloyds to hold Ms M responsible for these transactions.

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 Ms M to accept or reject my decision before 18 March 2024.

David Perry
Ombudsman