DRN-4586567

The complaint

Miss G complains that Lloyds Bank PLC ("Lloyds") failed to refund transactions she didn't recognise.

What happened

What Miss G says

Miss G explained that she was preparing to pay her outstanding balance on her Lloyds credit card and expected the balance to be in the region of £1,000. When Miss G opened her Lloyds banking app, she saw that about £4,000 of additional transactions were recorded which she didn't recognise.

Miss G examined these transactions and noted they were to money remittance providers. The following day, Miss G contacted Lloyds about them and explained she wasn't responsible.

Lloyds looked at the payments and told Miss G they were unable to refund them due to payment information linking her to the disputed transactions. Miss G was told that an "IP address" match showed normal banking activity had taken place from the same place as one of the disputed transactions.

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.

Miss G said that she contacted one of the remittance providers who told her the funds were sent as cash and collected in an overseas location. Miss G hadn't arranged for this herself or held an account with them. Miss G also reported the loss of her funds to Action Fraud.

Miss G complained to Lloyds about their refusal to refund her. Lloyds again looked into the situation and told Miss G that they weren't going to refund her and noted that biometric data had been used to authorise the payments. Miss G said she hadn't got this facility enabled on her phone.

Miss G remained unhappy with Lloyds handling of her complaint and brought it to the Financial Ombudsman Service for an independent review.

What Lloyds said

Lloyds told Miss G they weren't prepared to refund her as the IP address data matched her use of her online app and the payment information using biometric data. They concluded there wasn't enough evidence to show that fraud had taken place. Lloyds agreed to freeze the interest on her credit card balance for three months while Miss G took further advice.

The investigation so far

Miss G's complaint was assigned to an investigator who asked both parties for information about the situation. Miss G was able to confirm her version of events as described above. Miss G also confirmed that no one else had access to her phone or online banking details. She went on to explain that she'd experienced considerable stress as a result of the situation.

Lloyds provided details of the account held by Miss G and the disputed transactions, including data about the use of her account and IP address data for the payments.

In summary this said:

- Miss G had opened the account only recently.
- About two weeks after opening Miss G reported fraudulent use of her account.
- Lloyds took on some of the payments (and made a refund) but declined others due to a matching IP address linked to other activity (on the banking app) and data from an undisputed transaction.
- Miss G's card was replaced.
- Within a few days, further disputed transactions were made.
- Lloyds determined that matching IP address data linked Miss G's device(s) to the disputed transactions and use of her banking app.
- Audit data showed that biometrics had been used to access the banking app.
- Lloyds had one phone recorded for Miss G.
- Miss G told Lloyds she'd changed her phone and telephone number after the original fraud claim, but records show the same device (and phone number) were used by Miss G to cancel her card some weeks later.

After reviewing the evidence provided by the parties, the investigator didn't uphold Miss G's complaint, commenting that:

- Lloyds data showed biometrics were used to log onto Miss G's app around the time of each transaction being made.
- The ID device is consistent throughout the complaint, including the one used to cancel the card.
- IP address information identified that the transactions were matched to recognised (undisputed) activity on Miss G's account.
- Miss G logged on to her device almost every day and likely would have noticed the disputed transactions sooner.
- The disputed transactions stopped two days before they were reported which isn't how fraudulent accounts are usually operated.
- There are unusual gaps in the disputed transactions which isn't indicative of fraudulent behavior.

Miss G disagreed with the investigators outcome and asked for the evidence that had been relied on. IP address data was sent to Miss G and she continued to strongly disagree.

Miss G said:

- There are multiple IP addresses contained within the information she was sent that don't show which ones are linked to Miss G.
- Miss G argued that she wasn't the one logging into her account based on the number of times this happened.
- The payments don't fit her spending patterns.
- Miss G maintains she was a victim of fraud.
- IP addresses can be manipulated via VPN (Virtual Private Networks).
- Lloyds bank allowed Miss G's identity to be stolen.

- Miss G was concerned that interest may be added to her account.

The investigator informed Miss G that as no agreement could be reached, an Ombudsman would review her complaint. Lloyds agreed to further freeze the interest payments for a further period of time.

The complaint has now been passed to me for a decision. As part of my investigation, I asked Lloyds to provide the list of IP addresses linked to the disputed transactions.

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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that Lloyds can hold Miss G 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 Miss G 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 Miss G'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 Miss G. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Miss G responsible for the disputed transactions or not.

It's Miss G's case that these transactions were carried out by persons unknown without her knowledge or permission, whilst Lloyds believe she was responsible. Where there's a dispute about what happened, as there is here, I must reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence.

Lloyds records show that Miss G had registered one phone number with her account (and it's the same one she's used with our service). Further data shows that a consistent "device" was used to access her online banking app bearing this number. From this, I think it's reasonable to conclude that Miss G was using her phone to access the banking app.

There are a number of different IP addresses associated with the banking app and this isn't particularly unusual. Having examined the evidence, it's apparent there's a wide variance in the recorded location of those addresses which seem unlikely to consistently relate to the devices location at the time. As explained above, the physical location identified by the IP address can sometimes be linked to other factors related to the provider of those internet services.

What is apparent though is that those IP addresses linked to the disputed payments are the same addresses recorded when opening the banking app. This would indicate that the same device was used to both access the banking app and be recorded against the payment details when the disputed transactions were made.

Miss G has said that no one else had access to her phone or knew her banking details, so it

seems unlikely that an unknown third party could be responsible for using that phone without her knowledge or be able to log into her banking app (because they wouldn't have her online security details). There are no records showing any other device was used to access the banking app, although Lloyds data shows an "iPad other" is related to the payments themselves, but with the same IP addresses as those used by her phone.

Miss G said that "*On the 11th of September, I went to make a payment to clear my credit card, which I believed the debt to be £1033, however when I accessed my banking app, there was circa £4118.46 of transactions recorded that I haven't made."*

From this information, it can be seen that Lloyds recorded IP address data (on 11 September) which matched some of the disputed transactions. That data also matches the device registered by Miss G when she originally set up her banking access, despite saying she'd changed it and her phone number (I've not seen any record of that change).

There's also matching IP address data related to earlier undisputed transactions which shows that both disputed and undisputed transactions took place with the same device from the same location.

I understand Miss G said she hadn't set up "fingerprint" access on her phone, but Lloyds information confirmed that "biometrics" were used on numerous occasions to validate processes when using the banking app. This can be different types of biometrics, generally dependent on the phones technical capabilities - not solely "fingerprints".

I've also thought about the way those payments were made. There are some gaps in the use of Miss G's account, one for about a week. This is an untypical use of a stolen card because any thief who'd gained access to the account would generally use the card as fast as they could because they wouldn't know when it would be reported as stolen. They'd also be unlikely to stop using it until it was blocked, but that didn't happen here. It appears that whoever was using stopped short of the available credit, so likely knew the limit. Not something I'd expect a thief to do.

Taking everything into account, it seems unlikely that anyone else could have carried out these transactions without Miss G's knowledge or permission. While I'm sure Miss G will 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 Miss G authorised or allowed her banking details to be used to make the payments. So, taking everything into account, I think it is both fair and reasonable for Lloyds to hold Miss G 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 Miss G to accept or reject my decision before 1 April 2024.

David Perry
Ombudsman