DRN-4475518

The complaint

Miss K complains that Capital One (Europe) plc ("Capital One") failed to refund transactions she didn't recognise.

What happened

Miss K experienced difficulties with various other financial accounts, believing that she was the victim of a "hack". As a precaution, she contacted Capital One and told them she'd had problems with these accounts and wanted a new card. She said this was to enable her to access the account, pay off the outstanding balance with a view to closing it. Capital One sent Miss K a replacement card.

Miss K paid off the outstanding balance on her account and shortly after, numerous transactions were carried out using her new card details. Capital One sent a message to Miss K's phone to check the authenticity of these payments and received a confirmation that they were legitimately made by her. Other payments also required additional security steps to confirm the transactions.

Capital One called Miss K to ask about these transactions and Miss K told them she wasn't aware of them. She confirmed she hadn't seen or responded to the confirmation message sent by Capital One or carried out any of the additional security steps to authenticate the various transactions made from her account. Miss K asked for a refund of these payments.

Capital One looked into what had happened and declined to refund Miss K, believing she was responsible for them. Miss K complained to Capital One about the situation and after investigating her complaint, they again declined to refund Miss K.

Miss K was left unhappy with her complaint and brought it to the Financial Ombudsman Service for an independent review where it was looked into by one of our investigators. Both parties were asked for information about the situation and Miss K was able to say that:

- She called Capital One to replace her card because her bank account's security had been breached. She argued that Capital One should have known these transactions were fraudulent because she asked them to block such payments.

- Her accounts and phone had been "hacked", but evidence of this was difficult to obtain.

- She hadn't received any messages from Capital One or checked her online account.

Capital One provided details of their investigation and information concerning the operation of the account, including:

- A message was sent to Miss K's phone to check the transactions and a reply was received.

- Additional security was confirmed for the disputed transactions requiring Miss K to

respond to each message with a One Time Passcode (OTP).

- IP addresses matched for both disputed/undisputed transactions and use of the mobile banking app.

  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.

- Use of the mobile app was recorded during the period the disputed transactions were carried out, but no action was taken to notify Capital One or block the card.

- It was a new card that hadn't yet been used for spending, so it was difficult to ascertain how the details would have been known to anyone else but Miss K.

- There were no further attempts to use the card after it was reported to Capital One.

After reviewing the evidence, the investigator didn't think that Capital One should have to do anything and Miss K's complaint wasn't upheld. The investigator commented that:

- Whilst Miss K advised Capital One that she was updating her card due to a breach of her bank account, she didn't ask them to block any transactions.

- Capital One data shows Miss K's usual device (mobile phone) logging into the account consistently from the same IP address used to make the disputed transactions.

- Multiple OTPs were sent to Miss K which were used to confirm the individual transactions.

- These payments were made from a new card that no one else knew about.

- Miss K likely authorised the transactions herself.

Miss K strongly disagreed with the investigator's outcome and asked for a further review of her complaint, which has now been passed to me for a decision.

Miss K stressed that Capital One shouldn't have let these transactions leave her account because they'd been informed that fraud had already taken place on her other account.

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 was sorry to hear that Miss K has been going through a difficult time recently. My role here is to make a decision on the outcome of her complaint. I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. Where the information I've got is incomplete, unclear or contradictory, as some of it is here I have to base my decision on the balance of probabilities.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that Capital One can hold Miss K liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them.

Capital One can only refuse to refund unauthorised payments if it can prove Miss K authorised the transactions, but Capital One cannot say that the use of the card details for online payment details conclusively proves that the payments were authorised.

Unless Capital One can show that consent has been given, it has no authority to make the payment or to debit Miss K'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 K. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Miss K responsible for the disputed transactions or not.

When Miss K called Capital One, she told them about the breach of her bank account and asked for a new card. During the conversation she told Capital One that she wanted a new card to access her account and then she was going to pay it off and close it. Having listened to the call, there's no request to block transactions made by Miss K.

When Capital One replaced Miss K's card, I don't think they had any other information about the potential risk to Miss K's account. I think the cancellation of the current card was a reasonable step for them to take based on what they'd been told. They weren't asked by Miss K to block her new card, and it raises a question why Miss K would need such a card if she was intent on closing her account as she told them in the call.

Based on the data provided by Capital One, it's hard to see how anyone other than Miss K was responsible due to the recording of her device being used to answer various messages and OTP's. In order to do this, it would normally require access to Miss K's device, which was protected by a security code and enter a different set of security information to open the Capital One app. It's my understanding that Miss K was the only person who had these details and she hadn't given them to anyone else or been asked for them (in an attempt to scam her out of the information).

Additionally, there's IP address data that shows Miss K's device was used in the same locations both before the disputed transactions were carried out and during the time they were made. Also, Miss K's mobile app was opened, providing an opportunity for Miss K to see what was happening with her account.

It's Miss K's case that she believes her account was compromised somehow and her phone hacked, enabling an unauthorised third party to use her account to make the disputed transactions. This included answering the various messages and codes sent by Capital One and the merchant who the payments were made to. Unfortunately, there's no evidence that her device/account was compromised. Whilst it's possible that some form of technical attack was mounted against Miss K, I don't think that's the answer here.

I understand Miss K believes that the IP address was spoofed, to make it appear the phone was being used from her usual location. I'm sure this is technically possible, but I'd question why a thief (the hacker) would go to those lengths to implicate Miss K, rather than just take those funds without going to the additional trouble of spoofing the IP address.

When I take the other factors into account, particularly the use of the new card details, which weren't wholly available to anyone else apart from Miss K or had been used to make any new purchases, it seems unlikely that a hacker could readily find out this information.

Additionally, the pattern of spending stopped once it had been reported, indicating that whoever made those transactions knew the card was no longer working (because it had been reported). It's often the case that stolen cards continue to be used because the thief

isn’t aware of the problem – but here the last transaction was authorised, meaning that the thief hadn’t any reason to stop trying to use the card. If for example it had been blocked for some time and repeated attempts against were records, this could have indicated someone was unaware it had been blocked.

If a hacker had access to the Capital One account, I would have expected to see other attempts to manipulate the available spending such as trying to raise the credit limit, but that didn’t happen here.

I understand Miss K feels strongly that she’s the victim of an account take over and will no doubt disagree with me, but overall, and based on the available evidence, I think it’s more likely than not that Miss K was responsible for these transactions. I think it was both fair and reasonable for Capital One to hold her liable for the disputed 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 K to accept or reject my decision before 30 January 2024.

David Perry
Ombudsman