DRN-3184839

The complaint

Mr M complains that Barclays Bank UK PLC failed to refund transactions he didn't recognise.

What happened

Mr M explained that he received two calls that appeared to be from Barclays and was suspicious because they asked for his three-digit security number from the back of his debit card. Mr M says he never gave this to them and ended the call. The day after the last text was received, he noticed a number of transactions had been taken from his account that he didn't recognise and called Barclays about them.

Mr M couldn't get through on the phone, so he went to a Barclays branch and reported the problem where a fraud claim was logged. Barclays issued a temporary credit to Mr M whilst they looked into the claim. Barclays later took the temporary credit back from Mr M.

Barclays declined to make a refund, believing Mr M responsible for the transactions. Barclays said that there were matching IP addresses* and the payments were either made with Mr M's registered mobile device or were "card not present" (CNP) transactions. CNP means that the card holder and the merchant aren't physically together when the transaction is carried e.g. when done via the phone/internet. Barclays also told Mr M that because there were no further attempts to use the cancelled card after it was reported, this was an indication that whoever made the disputed transactions knew it had been cancelled and was unlikely to be an unknown third party.

*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.

Mr M disagreed with Barclays and made a complaint about their handling of the claim. Barclays investigated the complaint and declined to change their position. Mr M remained unhappy with Barclays and brought his complaint to the Financial Ombudsman for an independent review.

Mr M provided a list of messages and calls he'd received on his phone at the time of the disputed transactions and explained that this showed how the fraud had operated and that it wasn't him who'd carried them out. He confirmed that he hadn't lost his card or his phone and hadn't given anyone else access to them or his security details to allow someone else to use them.

Barclays supplied evidence to show Mr M's use of his online banking and how the payments were made, either through the use of the card details or mobile payments using Mr M's registered mobile phone. Barclays also recorded that a new mobile phone was registered on Mr M's account using his same phone number. Shortly after, the disputed transactions were made using his e- wallet. Barclays noted a large number of different devices had been registered by Mr M to use his mobile banking facility, which they thought wasn't typical.

Mr M's complaint was looked into by one of our investigators who thought it was reasonable for Barclays to hold him responsible for the transactions. She couldn't find a point of compromise that would allow an unknown third party to use Mr M's card details and his

mobile device to make the payments. She thought the timings of Mr M's use of his online banking and the disputed transactions pointed to Mr M having knowledge of them. She pointed out that the newly registered mobile wasn't responsible for the disputed transactions.

Mr M disagreed and asked for a further review of his complaint, he said he hadn't ever made such a large number of transactions together and this was out of character for him. Mr M didn't recognise the registration of another phone and couldn't understand some of the jargon – particularly the CNP reference. Mr M questioned the text message that Barclays claimed to have sent to his phone and speculated that it was an internal fraud issue within Barclays that was responsible for his loss.

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.

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

Authorisation is made up of two parts. Authentication and consent. Authentication is usually referred to as the technical evidence and in this case, Barclays have supplied evidence that shows the disputed transactions were authorised using a device registered to Mr M (e-wallet) or the correct debit card details. I'm satisfied the evidence shows the disputed transaction was authenticated.

Consent refers to the way in which Barclays and Mr M agreed to operate the account to allow Barclays to make payments on Mr M's behalf. For example, Barclays terms and conditions set out that if a payment is made using a registered device (e-wallet) or the use of the correct card details, then Barclays accept that the instruction to make the payment is authorised by the account holder. So, because the registered device was used to make contactless payments via its e-wallet and other transactions used the correct card details entered into a merchant's website, I'm satisfied that consent was given and the disputed transactions were authorised. But, there are exceptions where it wouldn't be appropriate for Barclays to hold Mr M responsible, for example if the mobile app or his card details were used without his permission.

Mr M has explained that he received suspicious calls that were intended to make him think it was Barclays calling him. When he spoke with the caller, they tried to obtain his debit card details including the three-digit security number from the back of the card. Mr M didn't give them this information and ended the call.

From this, it appears that Mr M was subject to some form of scam because a legitimate Barclays employee would be unlikely to ask for this type of information. I've examined the series of events leading up to the disputed transactions and the following table sets it out for ease of explanation.

Event	Date & Time
New phone registration for Barclays Mobile Banking with Speedy reg text to Mr M's	7/12/20 20:38

registered mobile phone.	
Card Not Present (CNP) transactions start	7/12/20 20:42
Mr M logs in to Barclays Mobile Banking from device previously used (and not disputed)	7/12/20 20:52
Mr M receives call from “Barclays” (believes suspicious)	7/12/20 20:53
Last CNP payment (total of four)	7/12/20 20:57
Anti-Fraud message to Mr M’s mobile related to CNP transactions	7/12/20 20:57
Mr M’s Mobile phone registered for (e-wallet)	7/12/20 21:02
First e-wallet payment using contactless facility on mobile phone	7/12/20 21:03
Anti-Fraud message to Mr M’s mobile related to e-wallet transactions.	7/12/20 21:36
Last e-wallet transaction (total of 12)	7/12/20 23:13
Mr M receives second call from “Barclays” (believes suspicious)	8/12/20 20:41
Mr M notices transactions and reports to Barclays	9/12/20 morning.

Mr M denied registering a different phone on the evening of the disputed transactions but the evidence from Barclays shows two devices were registered with the same phone number and used at different times on 7/12/20. The data also shows matching IP addresses for the use of the new device and previous devices. What that means is the newly registered device was used from the same location as other devices registered by Mr M. The registration of new devices requires a verification code to be entered that’s sent to the registered phone. Barclays records show only one phone number was used throughout this period, so I think any messages sent by Barclays would have gone to the devices used by Mr M.

Mr M sent information from his mobile phone supplier to show what messages he received, but they don’t cover the actual time period of when the disputed transaction occurred. Barclays provided evidence of their “Speedy Reg” system for new devices and this shows a new device was registered at 20:38 on 7/12/20. So, I think it’s likely that Mr M registered a second device using his registered number. Barclays records also show Mr M was logging in to his mobile banking account with a previous device during the evening when the disputed transactions were taking place. So, I think it’s likely he was aware what was happening with his account at the time, despite not notifying Barclays about it until a day and a half later.

Mr M explained that he’d not given out his debit card details to allow them to be used by any scammers. He also confirmed he was the only one who had access to his phone and cards. It’s difficult to find a plausible scenario to explain how an unauthorised third party could gain

access to Mr M's phone and card details without him being aware of it.

The disputed transactions started before any call was received that may be linked to an attempt at a scam, so I don't think that this is the explanation for how the authorised transactions started. The larger Card Not Present transactions were made using Mr M's card details and as he hadn't spoken with anyone about them before the first transaction took place, I think it's more likely than not that he was responsible for them.

The second set of disputed transactions used an e-wallet linked to Mr M's account that was used on a phone registered to him, so I don't think it's plausible for his phone to be used by anyone else when he's already confirmed he was the only one using it. It's unlikely anyone could obtain all the necessary information about Mr M's account to impersonate him and use his genuine phone number. I did consider the possibility of a "sim-swap" being responsible for the disputed transactions using the e-wallet, but I don't think it was likely because Mr M hadn't reported this and it would be apparent to the user because they'd lose control of their phone number. Also, anyone attempting to take control of the phone number would need to know all the other details of Mr M's account in order to log in to the mobile banking.

Mr M may well have also been subject to an attempted scam, but I don't think that's the explanation for how these transactions took place. That's because the disputed transactions started prior to the first suspicious call and the second suspicious call took place the next day, by which time the disputed transactions had finished. Barclays pointed out that no further attempts were made to use Mr M's account once he'd notified them about his losses. The logic behind this is that the user of the card, if not Mr M , wouldn't know if or when the card was cancelled and would keep using it after it was blocked – unless the user knew it had been cancelled.

I appreciate Mr M said the transactions were out of character for him and looking at his recent statements, I'd agree. But, the issue for me to consider here is whether it's fair and reasonable for Barclays to hold him liable for them. I think it was and I'd also note that they sent two messages to Mr M about the series of transactions at the time which he hasn't appeared to respond to. So, I don't think that Barclays needed to do anything further and I think that it's more likely than not that Mr M was responsible for making the disputed transactions or allowing someone to do it with his knowledge.

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 Mr M to accept or reject my decision before 28 March 2022.

David Perry
Ombudsman