

## **The complaint**

Mr R is unhappy Barclays Bank UK Plc (Barclaycard) allowed an unauthorised third party to access his account.

## **What happened**

On 31 July 2024, an unauthorised third party contacted Barclaycard, and on impersonating Mr R they accessed his account. They then went on to make two balance transfer requests, changed his password and increased the credit limit available to him.

Barclaycard was alerted to the irregular account activity on the same day, blocked Mr R's account and the balance transfer requests were stopped.

Barclaycard accepted that its agent hadn't picked up on the unauthorised access and apologised for the distress and inconvenience caused. It awarded Mr R £200 in recognition of this, which it later increased to £240 after Mr R prompted a further review of the complaint.

As Mr R felt this was still insufficient in addressing the subsequent stress and inconvenience that the event caused him, he referred the matter to this service.

Our investigator reviewed the concerns but didn't uphold the complaint. He felt that Barclaycard had acted fairly. But Mr R disagreed.

In summary, Mr R felt that Barclaycard had played a role in allowing the third-party access to his account and should do more to put things right.

Despite Mr R making a Subject Access Request (SAR) to Barclaycard, Barclaycard refused to provide this information and explained that it was not possible because of data protection considerations and Mr R was directed to the Information Commissioners Office (ICO).

## **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.

Having done so, I know this outcome won't be what Mr R hoped for but I'm not upholding his complaint. I'll go on to explain why.

I can see Mr R has submitted further considerations in support of his complaint which I've carefully reviewed. I'd like to assure Mr R that if I don't mention a particular point, it's not because I haven't considered it, but that I've focused instead on what I believe to be important to the outcome of this complaint.

I am sorry to hear that Mr R experienced identity theft and I can understand the level of worry that this matter caused. Based on the evidence that has been presented, it seems that an unauthorised third-party impersonating Mr R, contacted Barclaycard via a pre-authorised call and went on to make some unauthorised requests on the account.

Internal records provided by Barclaycard suggest that this initial contact was possible via their app which had either been registered for and set up by Mr R on his own phone, and then accessed using biometrics or a five-digit code. Or that someone that possibly had access to the five-digit code or Mr R's card information - that is required for app registration - registered for the app on another device and then used it to make the call to Barclaycard.

Mr R states he's never registered for the app, so that leaves us with the only possible alternative option – that Mr R has also suggested - which is that the third party set up the app using Mr R's already compromised information. As the verification process to get into the app identifies the card holder to be genuine, this allowed the third-party to bypass the scrutiny of further verification checks by Barclaycard when the call was connected to the agent. Access to further account details was granted after the third party correctly provided answers to two further security questions. In this instance this consisted of satisfying confirmation of Mr R's full name and the last four digits of Mr R's card number.

I'm glad to hear that despite the third-party gaining access to Mr R's account, Barclaycard's fraud detection system detected the activity to be suspicious on the same day, and it acted promptly to protect Mr R from suffering any further detriment with a block being placed on the transfer requests and Mr R's account being locked.

I can see that Barclaycard in its response to Mr R's concerns, accepted their error in not spotting certain warning signs that were presented during the call. And it confirmed that feedback had been provided to the agent. It reassured Mr R that its data breach team had also been notified to help prevent a repeat of the occurrence in the future. It made an award of £200 to Mr R in recognition of this failure, which after a further review of the complaint was increased to £240. Having reviewed this, I think it was reasonable.

Mr R doesn't consider this sufficient and although he accepts that his personal information had already been compromised before this event took place – and so is probably better placed than Barclaycard on explaining how access was achieved in the first instance - he feels that it was Barclaycard's security processes, and the agent's actions that enabled the third-party to access further account information. And had this unauthorised access been picked up sooner, then this would not have been possible. In particular, I appreciate the concerns Mr R raised about his online account, and I accept that a security oversight by the agent provided an opportunity for the third-party to re-register Mr R's online account which would not have otherwise been possible. But fortunately, Barclaycard's systems picked up on this discrepancy and took the appropriate action. Which is what I would expect.

To ensure there was no possibility of a further breach of the account, Barclaycard also requested that Mr R attend a branch with identification before account function could be fully resumed. But Mr R explains that having to visit a branch with his passport to verify his identity, despite Barclaycard's part in allowing account access, caused him unwanted stress and inconvenience and it took some weeks for everything to be rectified. I accept that it would have been frustrating, but as Barclaycard was acting to protect Mr R's account, I can't say this was not a reasonable request.

I can appreciate that Mr R is concerned as to how the third party was privy to information that allowed them to impersonate him, and that he believes this to be part of a wider hack of his personal information. And this is why he requested the call and any communication between Barclaycard and the third-party, because he felt that it would help in providing some answers to these questions - whilst also sharing the findings with Action Fraud and helping to identify any information that could be used by the unauthorised party to gain access to his accounts again in the future.

I can see that Mr R's SAR request was rejected by Barclaycard, and I can understand how frustrating this must be for him. However, because of the GDPR regulations banks have a duty to observe, I agree Barclaycard has been reasonable in refusing this request.

Sadly, a lot of the time, it simply isn't possible to identify where a fraudster obtains their information from. Barclaycard has already explained what information was exchanged during the call with the fraudster, so I can't see what else access to this information will provide, but Mr R is at liberty to follow up on his request with the ICO.

I have given great thought to Mr R's position, particularly the impact this matter had on him. I don't doubt this has been a troubling time for Mr R, especially considering he was a victim of identity theft. But on considering how Barclaycard responded to the situation and put things right, I do think that the offer of £240 it has made is fair and addresses the impact of its actions. And I do not hold it responsible for the actions of the fraudster.

Our website further outlines the awards made by this service for distress and inconvenience and explains that the awards made are intended to recognise the upset caused by an error. They are not intended to punish the business.

Once again, I'm sorry to disappoint Mr R and I appreciate that he won't be happy with my decision, but in this case, I think the award for compensation is fair and in line with what I would have awarded for the mistake that Barclaycard made. So, I do not require them to do anything further here.

### **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 R to accept or reject my decision before 28 April 2025.

Sukhdeep Judge  
**Ombudsman**