DRN-3753747

The complaint

Mr R complained that Barclays Bank UK PLC didn't take enough care to protect his account, after there were fraudulent attempts to use his credit card.

What happened

On 2 November 2021, Barclays received several calls about Mr R's credit card. The caller passed security using the account details, but Barclays was suspicious and it blocked the account and contacted Mr R, asking him to get in touch.

Mr R rang Barclays on 3 November. He confirmed transactions on his account, and the card was unblocked.

Mr R received paper statements, and by 25 November this was overdue, so he rang Barclays again. Barclays said Mr R had asked for his statements to be online – but he hadn't. So Mr R was put through to Barclays' fraud team.

Barclays told Mr R that someone had phoned Barclays and had passed security on Mr R's account. The caller had then changed the postal address on the account on 7 November; had asked for a replacement card the next day; and a few days later had registered the account for online services and had changed the phone number. Mr R's personal details were provided to pass security on all three occasions.

Mr R hadn't made any of these calls, which were fraudulent. So Barclays' fraud team:

- changed back his address and phone number;
- agreed an additional password for extra security;
- blocked Mr R's card and posted him a new card and, separately, a new PIN;
- recorded a protective marker with an anti-fraud organisation; and
- disabled the online registration. But as I've set out below, it later turned out this hadn't been fully implemented.

On 27 November, Mr R sent Barclays a Signed For letter about the issues. He asked a number of questions about what had happened, and asked for his paper monthly statement urgently so he could verify transactions.

On 14 December, Mr R hadn't had a reply, and he also still hadn't received his November statement, which he'd asked for during the 25 November phone call and in his subsequent letter. He rang Barclays and was again told that he'd asked for statements to be online. Mr R said he hadn't, and said it appeared Barclays hadn't corrected this from the previous call.

On 15 December, the mobile banking app was used to change the phone number on Mr R's account. The app was used the next day to apply for a balance transfer of £4650. Barclays' systems blocked the balance transfer. Both of these attempts were carried out by the fraudster.

On 23 December, Barclays sent Mr R a voicemail asking him to get in touch. Mr R rang Barclays straightaway, and was told about the change to his phone number and the balance

transfer attempt. Barclays changed the number back, confirmed the blocked balance transfer as fraudulent, and blocked the card. Mr R asked how this could have happened when an additional password had been set up on 25 November following the fraudster's earlier actions. He said Barclays didn't reply about that, but it appears it was because the additional password would only have covered phone calls not online transactions.

By 9 January 2022, Mr R had received a new card but not yet the new PIN. He wrote again to Barclays, setting out the latest events and pointing out that he'd continued to have issues. He asked questions, including how the latest attempts could have happened given the additional password. He said he was very stressed and anxious about the security of his account, and Barclays had failed to provide any response.

Mr R contacted this service the same day. We got in touch with Barclays, as the rules set for us say that financial organisations have to have an opportunity to provide a final response letter, before we can consider a complaint.

Barclays sent Mr R a final response letter on 26 January. It upheld Mr R's complaint, saying it appeared Barclays hadn't done enough to protect his account when it was first made aware he'd been the victim of fraud. It said that after Mr R's confirmation that he hadn't authorised the changes in early November, it had corrected his account details, including deleting the online facility. But Barclays acknowledged this didn't appear to have worked, as the fraudster changed the details again and attempted a balance transfer. It told Mr R that wherever possible, it referred known suspects or viable leads to the police.

Barclays also said that it couldn't determine why Mr R hadn't had a new PIN or his November statement. It enclosed statements for November, December, and January. Barclays apologised for the delay but said it hadn't received Mr R's November tracked letter. Barclays said it had put additional measures in place to protect him, including adding a password of Mr R's choosing to the account. Barclays paid Mr R £50 compensation.

Mr R wasn't satisfied and on 15 February wrote back to Barclays. He'd had another email confirming his online statement was ready, so he'd decided to close the account. Mr R had similar emails confirming his online statement was ready, on 21 January, 18 February, and 18 March.

Barclays didn't reply to Mr R's 15 February request to close his account. So he confirmed to us that he wanted this service to investigate.

Our investigator didn't uphold Mr R's complaint. She said she thought Barclays had taken the necessary precautions to keep Mr R's account safe. The fraudster had known Mr R's personal details when he rang up Barclays. She agreed Barclays had made an error by not blocking the internet banking, but she thought £50 was fair for that, as Barclays had blocked the balance transfer and there had been no financial loss.

Mr R didn't agree. He said it seemed a whitewash, and he said he still wasn't clear how the fraudster had been able simply to call Barclays and change his details. He said that given the history of fraudulent activity, he felt Barclays should have been more diligent, and he couldn't accept there hadn't been a data breach. He also said Barclays had been very slow to respond, and in some cases had failed to reply at all to his correspondence.

The investigator replied that Barclays wouldn't be able to explain how Mr R's details had been compromised, as it wasn't responsible for giving away any of his personal information. The fraudster had already known the details and passed security during the calls. She suggested Mr R might have clicked a link in a text message or email and input his details, or given information to a suspicious caller.

Mr R said he was insulted by the investigator's insinuation that he'd compromised the security of his account. He'd never clicked on links, or provided details to a caller, and he was more than aware of how to maintain a secure account. He asked whether Barclays had provided any evidence about what security questions it had asked, and asked about the call recording. Also, having told Barclays that the online facility had been set up by the fraudster, it still took Barclays more than three months to delete the online access to Mr R's account, during which time he kept getting notifications that his statement was available online. This failure and the security breach had caused him much anxiety, and he'd had to close the account, which was much to his detriment.

Mr R asked for an ombudsman's decision. He also asked for the recording of the fraudster's call to Barclays. The investigator asked Barclays for the call recordings, but Barclays wasn't willing to allow Mr R to have these under the data protection GDPR rules.

Mr R also said that although he'd received confirmation that his account had been closed on 24 March, he was still (late July 2022) receiving messages from Barclays saying his statement was available online. The investigator asked Barclays about this, and Barclays replied that when the account was closed on 24 March, there had been £50 credit on the account from its compensation payment. On 11 July it had sent this as a cheque to Mr R, which would have generated a statement. Barclays said Mr R might receive a further statement showing a nil balance – and it said it allowed access to an account online for up to 60 days after closure.

Mr R's complaint was referred to me for an ombudsman's decision.

My provisional findings

I issued a provisional decision on this complaint, as I had come to a different conclusion from the investigator. Our process in such instances is for a Provisional Decision to be issued, so that both parties have an opportunity to comment before a Final Decision. Before reaching my conclusions, I considered all the available evidence and arguments to decide what would be fair and reasonable in the circumstances of this complaint.

First, I said that I was sympathetic to Mr R for having been a victim of fraud. I could understand that he'd have been worried and upset by what happened, especially as there were repeated attempts. Unfortunately, frauds do happen, and they are upsetting in themselves. I explained that my role is to determine whether Barclays acted fairly and reasonably in this situation.

Security

I accepted that Mr R was careful about security, and I didn't agree with our investigator when she said it might have been that he'd clicked a link, input his details, or given information to a suspicious caller. I didn't just base that on his recent assurances, but I could see that when he first received a voice message on 3 November, he took the sensible precaution of phoning Barclays not on the number left on the message, but on the number on the back of his card. He also checked his statements carefully, as evidenced by the fact that he repeatedly asked for these. So I thought it was unlikely that Mr R would have done any of the things suggested by the investigator.

Similarly, however, I'd seen no evidence that Barclays committed any data breach by disclosing Mr R's security information to a fraudster. Sadly, there are many fraudsters who do obtain an individual's data, and it's not always possible to find out how clever fraudsters have done so.

I also accepted that it was because of GDPR regulations that Barclays didn't disclose, either to Mr R or to this service, the full information about the fraudulent calls including what security information the fraudster passed. I appreciated Mr R's frustration about this, but Barclays had said that the fraudster would have provided Mr R's personal details. When I don't have full evidence on any issue, I take my decision on what I think is more likely than not to have happened. Here, I considered it was most likely that the fraudster did give correct answers to the security questions. In those circumstances Barclays didn't do anything wrong in that respect.

Barclays' actions after the first fraud attempt

After it became clear on 25 November that there had been attempted fraud on Mr R's account, Barclays didn't properly block the online facility which had been set up at the fraudster's request. This meant that the online facility, and the mobile banking app, remained accessible for the fraudster. This resulted in the fraudster's further attempts against Mr R's account, with the phone number being changed on 15 December and the attempted balance transfer on 16 December.

Barclays' systems did block the attempted £4,650 balance transfer on 16 December. So there was no financial loss. However, the further attempts against Mr R's account did lead to increased distress and inconvenience for Mr R.

After the fraudster's December attempts against Mr R's account, Barclays still didn't then fully block the online facility which had made that possible. That was evidenced by the messages which Mr R continued to receive. These continued not only in the first three months of 2022 up to closure on 24 March, but even in late July 2022. Barclays had explained why there was still activity on the account then, because of the outstanding £50 compensation payment – but that didn't explain why online access was still in place, when the online facility had only been requested by the fraudster, and this was one of Mr R's complaint points.

Barclays should have properly removed all online facility when the fraud came to light on 25 November. It accepted that it didn't do so, which enabled the further attempts on 15 and 16 December. But even then, the evidence indicates that the online facility wasn't properly removed. I considered the repeated failure to remove the online facility was a significant failing by Barclays in the circumstances of Mr R's complaint.

Barclays' customer service

Complaints which are solely about how a financial business conducts its complaint handling falls outside our jurisdiction under the rules set for this service by the Financial Conduct Authority (FCA). Here, however, the way Barclays handled Mr R's complaint relates to how it administered its business in providing the financial service. So I considered that I could look at the customer service which Barclays provided to Mr R.

I could see that Mr R requested a paper copy of his statement on multiple occasions. The fact that the November statement hadn't turned up was the reason he rang Barclays on 25 November, which led to the discovery of the fraud. I could also see that, in Barclays' final response letter on 26 January, it said it had sent the November statement and new PIN, and once issued, these were in the hands of the postal service. Certainly mail does sometimes go missing, but Mr R also didn't receive his December or January statements – and as I've set out above, in early 2022 was still getting emails saying his online statements were ready, when he'd wanted paper ones all along.

I noted that Barclays didn't reply to Mr R's 27 November letter, which he said he'd sent for by Signed For mail. I was also surprised that Barclays didn't contact Mr R about the 16 December attempted balance transfer until a week later, on 23 December. Also, Mr R wrote to Barclays on 15 February, about the fact he was still getting emails saying his statements were available online, and asking to close the account as a result of what had happened. He'd received no reply by the time he wrote again on 18 March. So Mr R had to close the account by phone. Although the account was closed on 24 March, he still had frustration over the next few months when he continued to receive messages to look at his account online. In the circumstances of this case, where the unwanted online facility had been requested by the fraudster, this would have been particularly galling.

So I agreed with Mr R that Barclays' customer service in sorting out the fraud was poor.

Compensation for distress and inconvenience

Taking into account all the factors I've set out above, I considered a fair and reasonable amount of compensation for Barclays to pay Mr R would be £250. I said that I intended to uphold Mr R's complaint and to order Barclays Bank UK PLC to pay Mr R a total of £250 compensation for distress and inconvenience. As it had paid him £50 already, that would leave a further £200 to pay.

Responses to my provisional decision

Barclays accepted the provisional decision, and said it was willing to pay Mr R the additional £200, making £250 in all.

Mr R also accepted the provisional decision. He said he was pleased that the provisional decision was to uphold his complaint. He said he was a little disappointed that Barclays hadn't revealed the full story about how his account had been hacked, and he thought it was very poor that it didn't let him have the recordings of the fraudsters' call, citing GDPR. Mr R said that what he'd been after all along was an explanation, and to highlight what he considered to be security failings by Barclaycard which put all cardholders at risk.

Mr R said he didn't have any further evidence and would abide by the decision as he'd now like to draw a line under the event.

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 do understand that Mr R would have liked to know full details about how his account had been hacked. I don't have that information – and sadly it's often the case that it's not possible for anyone to know how any particular account has been hacked by very skilful fraudsters. I do realise this is frustrating, but unfortunately Mr R is by no means the only person in this position, and not just in relation to Barclays.

Having reconsidered the evidence, and in the light of both sides' responses to my provisional decision, I consider that my provisional decision was fair and reasonable in all the circumstances of Mr R's complaint.

My final decision

My final decision is that I uphold Mr R's complaint.

I order Barclays Bank UK PLC to pay Mr R a total of £250 compensation for distress and inconvenience. As it has paid him £50 already, that leaves a further £200 to pay.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 11 November 2022.

Belinda Knight
Ombudsman