

## The complaint

Mr R complained because MBNA Limited refused to refund him for transactions he said he didn't make.

## What happened

On 15 January 2024, there were two debits to Mr R's MBNA credit card. One was for £1,998.60 and the other for £799.44. There were two further attempts, but Mr R's credit limit had been reached and these were rejected.

Monthly statements were issued on 14 February and 14 March. Mr R had a direct debit set up which made credits in February and March.

On 27 March, Mr R requested a PIN reminder from MBNA. It sent him a text in reply, and he saw there had been texts from MBNA in January, asking him to confirm two January transactions. Mr R contacted MBNA and said that he hadn't authorised the two transactions.

MBNA declined Mr R's claim. He complained. In MBNA's final response letter, it said that the IP address (a unique computer identifier) used to make the disputed transactions matched the IP address which Mr R used to log in to his MBNA account. And it said it had contacted Mr R to verify the transactions and had received a text response to confirm it had been genuine. It also said that it hadn't been able to identify any SIM-swaps on Mr R's phone, for anyone else to have been able to respond to the texts it had sent him asking for authorisation for the transactions.

Mr R wasn't satisfied and contacted this service. He said MBNA's statement that he had received a text confirming the transactions had been a lie. He'd never sent text messages confirming these, and he'd only become aware of them on 27 March, when he'd requested a PIN reminder from MBNA. He sent photos of his phone, showing messages on 15 January providing a six-digit code, and one text saying *"You will shortly receive a text from MBNA to confirm recent activity on your card ending ..... If you don't respond to the text we may decline future card payments."* The photos sent by Mr R went on to show the communications about his PIN request on 27 March.

Mr R also told us that he'd been the victim of an investment scam in January 2024. This had been with another bank, which had refunded him after investigating. He said he had downloaded suspect software at that time, but his laptop had since been reset and the download removed. Mr R suspected that the individual who had scammed him through his bank in January had also been responsible for the MBNA transactions. He said that the regulator, the Financial Conduct Authority (FCA) had told him that he'd been dealing with a cloned account for an investment trading platform.

Mr R told us that his phone isn't password protected, but he lives alone and keeps his phone with him at all times.

Our investigator asked MBNA for more information. The technical information it provided showed that the transactions had been authenticated by text, and it showed the IP address from which they'd been made.

Our investigator didn't uphold Mr R's complaint. She said this was because the transactions had been verified using an IP address which had previously been used for a genuine log-in. Also, a text had been sent to Mr R which had allowed the transactions to be authorised. She noted that the transactions were out of character for Mr R, but as he'd said he hadn't received any suspicious calls, emails or suspicious links, that meant he hadn't been the victim of a scam.

Mr R didn't agree. He said that even if the transactions had been verified using his IP address, he hadn't made them. He said that in January he'd been startled to see his cursor wandering about his laptop screen without him having anything to do with it. His laptop had then been remotely operated when he'd been scammed out of what a fraudster had said would be an investment for £4,250, which his bank had since refunded. Mr R also pointed out that the texts he'd received on 15 January had been to let him know of the transactions, not to authorise them – and he'd only seen them on 27 March.

Mr R said that after the January 2024 scam he'd discovered that software allowing remote transactions had been put on his machine, and the FCA had advised him that that had been done by a cloned firm. So he believed that it was the same fraudster who had hacked his way into his MBNA credit card and was responsible. He said that at that time, the only person who could access his laptop then had been the fraudster.

Mr R asked for an ombudsman's decision.

### **My provisional findings**

I issued a provisional decision on this complaint. This was because I'd come to a different conclusion to the investigator. Issuing a provisional decision gave both sides the opportunity to comment on it, by the date set, before I issued a final decision

Before issuing the provisional decision, I considered all the available evidence and arguments to decide what would be fair and reasonable in the circumstances of this complaint.

#### *What the Regulations say*

In my provisional decision, I explained that there are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. So what determines the outcome here is whether Mr R, or a third party, is more likely than not to have authorised the disputed transactions.

#### *Who is more likely to have carried out the disputed transactions?*

I looked in detail at what had been said, and the technical evidence.

The information provided by MBNA confirmed that online banking activity only started on Mr R's account in January 2024. It sent us the information relating to the IP address for:

- the two successful disputed transactions, which took place at 16:07 and 16:41 on 15 January;

- the two unsuccessful ones which failed at 16.52 and 17.07 the same day, after Mr R's credit limit was exceeded; and
- the only previous login which used the same IP address. This was for a log-in only and took place at 14:59, just over an hour before the first disputed transaction.

So I found that the IP address didn't provide conclusive evidence here. There was no evidence to show that the IP address used had been previously used for any genuine transactions. MBNA also confirmed that online banking activity only started in January 2024, though it provided statements going back to April 2020.

It also appeared from the account history, and MBNA agreed with this, that the disputed transactions were out of character for Mr R.

The disputed transactions also went to the same investment business name which Mr R had said were the subject of the transactions where he suffered a £4,500 scam against his bank account.

I looked at the codes for the payments. They were coded as "*continuous payments*." These are usually created online or on the phone, and don't usually have a paper trail. The recipient can claim different amounts at different times without giving notice to the payer. I thought that the payment type here, especially when I hadn't seen others on Mr R's MBNA account, made it more likely that they were fraudulent.

I also looked carefully at the text messages. Mr R had sent us photos of what he'd received, though he said he didn't see them till he contacted MBNA in March. The evidence from MBNA showed that the disputed transactions were authenticated following receipt of a text confirmation. The phone number which sent the authorised transactions wasn't given on MBNA's spreadsheet, though the six digit code would have been sent to the phone number on MBNA's existing record for Mr R's account. And Mr R's phone did show that the code had been received on his phone.

I can't know whether or not Mr R's phone's SIM was cloned when he was scammed out of £4,500 from his bank account. But it must be a possibility.

The fact that there were two further attempted transactions, which failed because Mr R's credit limit had been exceeded, is also typical of fraudster behaviour, trying to maximise their gain.

On the other hand, it's surprising that Mr R didn't report the disputed transactions for two months after they happened. Statements were issued in mid-February and mid-March, as I've set out. And as Mr R suffered a scam around that time on his bank account, I think most people would carefully check their other financial accounts to make sure there was no problem with those too.

On balance, however, I thought it was more likely than not that it wasn't Mr R who authorised the disputed transactions. Key factors in my decision were:

- the IP address was only used to log on an hour before the disputed transactions, and for the disputed transactions;
- the transactions were out of character for Mr R's account;
- online banking hadn't been used on Mr R's account before, although he'd had the account since 2020;
- the disputed transactions were continuous payments;
- there were further attempted transactions after the two successful ones.

So my provisional decision was that I intend to uphold this complaint. I said that subject to responses to my provisional decision, I intended to order MBNA to refund Mr R for:

- the two disputed transactions on 15 January 2024 for £1,998.60 and £799.44;
- charges debited the same day in relation to these two transactions, for £99.93 and £39.97;
- interest at 8% simple on the total of £2,937.94 for the transactions and charges, from 15 January 2024 to the date of payment; and
- the interest which MBNA debited to Mr R's account in relation to these sums.

### **Responses to my provisional decision**

MBNA agreed with the proposal to refund Mr R's account with the two disputed transactions, and to ensure that any debit interest incurred in relation to these sums would be refunded to the account.

But it pointed out that Mr R had never paid off the transactions. So MBNA didn't agree to pay 8% compensatory interest on that basis. I asked MBNA to provide Mr R's statements which showed this. MBNA sent Mr R's statements which evidenced that he hadn't paid off the disputed transactions.

Mr R sent information about the separate scam which he said he'd suffered in January 2024. This included emails with the FCA about that separate incident. He also said that he had no reason or need to check his MBNA account which was why he only realised about the transactions on his MBNA account when he had a text from MBNA about his PIN reminder. He asked whether the fraudster could have seen his MBNA account and phone number during that separate January 2024 fraud. He also asked about continuous payments and how one can prevent these.

Mr R also queried the 8% interest I mentioned in the provisional decision. He said he believed he'd been charged at the usual MBNA rate of 29% or 30% for the fraudulent 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.

I've looked carefully at both responses to the provisional decision.

The statements provided by MBNA show that Mr R didn't pay for the disputed transactions which were debited to his account. Interest was charged on them at MBNA's rates, which will be covered by the fact that I'll order MBNA to credit Mr R's MBNA account with those charges.

Normally, if a customer has paid for disputed transactions which we then order to be refunded, we award interest at 8%, as I set out in my provisional decision. This is to reflect the fact that a customer has lost the use of what they've paid, for that period of time. But here, MBNA has argued, and has proved, Mr R didn't pay MBNA any money towards the disputed transactions or charges. So he hasn't lost the use of that money, which means it wouldn't be correct to award him interest for it. When I wrote the provisional decision, I wasn't aware that Mr R hadn't in fact ever paid for the disputed transactions. It means that no 8% interest is payable.

Mr R asked other questions in response to the provisional decision. I can't know whether or not the fraudster could have seen his MBNA account and phone number during that

separate January 2024 fraud. Similarly, it isn't for this service to provide advice on how one can prevent continuous payments being set up on an account, but he can ask the various financial organisations with which he has dealings.

### **My final decision**

My final decision is that I order MBNA Limited to credit Mr R's MBNA credit card account with:

- the two disputed transactions on 15 January 2024 for £1,998.60 and £799.44;
- charges debited the same day in relation to these two transactions, for £99.93 and £39.97; and
- the interest which MBNA subsequently debited to Mr R's account in relation to these sums.

I don't award interest at the standard 8%, because Mr R didn't pay for the disputed transactions, so he hasn't lost the use of his money.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 26 December 2024.

Belinda Knight  
**Ombudsman**