complaint

Mr D complains that Bank of Scotland plc has held him responsible for a number of transactions that were debited from his account but which he says he not make or authorise.

Mr D is represented by his father in referring his complaint here.

background

The disputed transactions, for a total value of £7400, were for payments to an online gambling company and took place over just short of two hours. They were made using Mr D's own online gambling account and started within three hours of Mr D carrying out genuine transactions on the account, the last of which was the receipt of £3,200.

Our adjudicator established that, ordinarily, in order to carry out the disputed transactions, a person would need to have:

- knowledge of Mr D's own gambling account username and password;
- knowledge of the security number on the back of Mr D's card; and
- access to Mr D's home and laptop.

She noted that Mr D said that he did not keep a written record of his username and password, nor had he given them to anyone else. He said the same about the bank account card's security number. The gambling company's evidence was that all the disputed transactions were made from the same IP address and this was the same address as Mr D made previous genuine transactions from. This indicated that the disputed transactions were being made from the same location as the genuine ones. In addition, the game played in the case of the disputed transactions was the same as that Mr D had genuinely played just hours before.

The adjudicator took into account how the disputed transactions appeared not to be of the sort that she would expect a fraudster to make – an unauthorised third party with access to card details might be more likely to spend on items with lasting value rather than online gambling: especially as the available balance on the account was over £14,000 yet the first two disputed transactions were for £200; and winnings would be paid into Mr D's account, and while Mr D's father mentioned a way in which winnings could be diverted to an accomplice, this seemed unlikely to the adjudicator.

The adjudicator did not consider that password details were likely to have been released by the gambling company and the session containing the genuine transactions, as well as that with the disputed transactions, were both sessions which were properly initiated and logged out of. She also did not consider the card security code was likely to have been released by the gambling company to a fraudster.

Mr D has speculated about how his computer, or the online gambling system, could have been hacked in order to provide the fraudster with information to enable him to pass security. But the adjudicator was not persuaded that Mr D had adequately shown that his computer was hacked and the nature of the transactions did not suggest that this happened. And she did not consider that the copy telephone calls, between him and the bank – that Mr D complains he has not been provided with – are material to the outcome of this complaint.

On balance, the adjudicator considered that the transactions were, more likely than not, made by Mr D.

The bank attempted to charge back the transactions for Mr D and temporarily refunded the funds to Mr D's account. However, the bank considered that the charge back was successfully defended and re-debited the account. The adjudicator considered that the bank acted correctly in this matter even though there were errors on the document produced by the gambling company and it only later explained these were made as a result of human error.

Finally, as regards to Mr D's concerns that the bank's security systems had failed him – it did contact Mr D about a disputed transaction which Mr D claimed to be fraud and stopped further transactions being made; but the call came too late Mr D says – the adjudicator said that banks have security procedures in place intended to prevent fraud from occurring, but we would not indicate what procedures the bank should have in place. She did not consider that the bank's system itself failed or that the bank can be said to have been obliged to have identified the transactions as fraud.

In conclusion, the adjudicator did not consider that the bank had acted incorrectly in holding Mr D responsible for the disputed transactions; and she therefore did not recommend that it needed to refund the value of the disputed transactions. The bank had, though, offered Mr D £86 for some administration failures while dealing with Mr D and the adjudicator recommended that Mr D accept this payment.

Mr D has asked that his complaint be reviewed by an ombudsman.

my findings

I have considered all the available evidence and arguments to decide what is fair and reasonable in the circumstances of this complaint.

Having reviewed the evidence and arguments presented, I agree with the findings and conclusions of the adjudicator.

Mr D's father has presented detailed and lengthy evidence and arguments and I recognise that he and Mr D have strong feelings about this matter. It is understandably of great importance to them. And I should firstly say that I have looked carefully at everything that has been submitted. But I hope that Mr D will not consider the brevity of my decision, in relation to his submissions and his expectations as to the nature of the investigation he may be expecting, as a discourtesy to him or that it represents that I have inappropriately simplified my consideration of the complaint.

In short, Mr D's father reiterates that Mr D could not have made the transactions on his computer as he, and others, were in his company at the time they were made and he has explained the circumstances of them being together. And he also maintains that Mr D's computer was hacked and his email account has now been hacked in the same way.

First, Mr D has offered to present more evidence that Mr D is acting with integrity in this matter and that he is of good character. There is no need for further submissions of that nature.

I accept the evidence presented by, and for, Mr D and also that all members of Mr D's family say that he was not using the computer. But I cannot now know with certainty how the disputed transactions occurred and I have to take into account all the evidence available. And where evidence is incomplete, inconclusive, or contradictory, I have to reach a decision on the balance of probabilities; that is, what I consider is most likely to have happened, given the evidence that is available and the wider surrounding circumstances.

Mr D questions the validity of the gambling company's defence to the charge back claim. He asks how the gambling company came to mistakenly refer to details of the account used to make the transactions but I am not in a position to say that the errors, in its response to the claim, were not made other than by human error - in any event, regardless of the outcome of the charge back claim, I would not require Mr D to be held responsible for the disputed transactions unless I was satisfied, on balance, that he made them.

Mr D's father says that he has produced evidence that a virus existed on the computer. However, there is not persuasive evidence that a virus was on the computer at the time that the disputed transactions took place; nor is there evidence that a virus was on the computer that enabled a fraudster to take control of the computer and make the transactions – within three hours of Mr D using the computer for the same purpose – or to have taken the password and account card information from the computer and used that information on another computer, while making it look like Mr D's IP address was being used.

Mr D's father maintains that a fraudster could have accessed the gambling account for reasons that are not concerned with how they will access winnings in the victim's account. I accept the points made but, again, I have to weigh this consideration up with all others in deciding, on balance, what is more likely than not to have happened.

As regards the issues of the phone calls and the bank's security system, I agree that, ultimately, these are not relevant to the outcome of this complaint. Both issues are raised in the context of whether the bank ought to have done more to stop the transactions. But it is a matter for the bank to put in place appropriate security arrangements in order to try to prevent fraud – and indeed it will have such measures in place. And there is a balance to be achieved between the bank protecting their customer from fraud and it allowing customers to make the transactions they wish to make, where they are properly authorised. And, of course, those arrangements do need to accommodate that spending habits alter and unusual needs arise.

In this case, I do not consider that I may fairly and reasonably say that the bank has acted incorrectly in allowing the transactions to take place. On the face of it they would have appeared to have been properly authorised.

It remains that there is no compelling evidence that the transactions were made by a fraudster who had hacked into Mr D's computer. The evidence shows that the gambling was of the same nature as only recently played by Mr D and soon after he received significant winnings. There is evidence that the IP address used for the fraudulent transactions was the same as that used for Mr D's genuine transactions and the nature of the spending, generally, does not look obviously like that of a fraudster.

I recognise Mr D will be disappointed to receive my decision but, on balance, I do not consider that I can safely say that it was not Mr D who made the transactions and therefore require the bank to refund to Mr D the value of the transactions.

I leave Mr D to contact the bank directly, if he still wishes to accept the compensation offer of £86 and the bank has not already paid it.

my final decision

My final decision is that I do not uphold this complaint.

Ray Neighbour
ombudsman