complaint

Ms A and Mr B complain that MBNA Limited has not refunded a number of credit card transactions that they say they did not make or authorise.

background

Ms A complained to MBNA that she did not recognise 11 payments made from her credit card account between February and March 2013, totalling £2,924. The card account is in Ms A's name and her husband Mr B is an authorised user. Most of the disputed payments were to gambling websites and two (for a total value of about £175) were to an online payment service. Ms A's online banking was also accessed during the time of the disputed transactions and she did not know who did this.

There were also two credits to the credit card account that Ms A and Mr B said they did not recognise. These totalled £1,400 and were transferred from a gambling website account. They reduced the net losses resulting from the disputed transactions to £1,524.

After an investigation MBNA declined to make a refund. It said that whoever made the transactions used Ms A's online banking security details, including the '3D Secure' password, and that there was insufficient evidence to suggest that a fraud had been committed.

Ms A and Mr B were unhappy with MBNA's response and referred their complaint to this service. They said they had never had accounts with the gambling websites or the online payment service. They pointed out that whoever set up the online payment service account used an email address that was slightly different from Ms A's, and that other transactions had been conducted through that account which were nothing to do with Ms A's real accounts. Ms A thought that her security information could have been obtained by some kind of software attack on her computer.

In the light of the available evidence, our adjudicator did not feel he could ask MBNA to refund the disputed transactions. Briefly, he said:

- The main gambling website said that the payments to it were made using the 3D Secure system. The larger payment to the online payment service also used 3D Secure. The adjudicator could not see how these details could have been known to a third party. MBNA confirmed that no changes were made to Ms A's 3D Secure details before or during the disputed transactions.

- To access Ms A's online banking the following were needed: her unique user ID and password followed by a 'sitekey,' in which the customer is required to confirm a scene/picture that was chosen on enrolling for the service. It was unclear how anyone could have acquired this information.

- The adjudicator had reviewed the IP addresses used for Ms A's online banking during the disputed period and a number of them differed from the addresses for her genuine online usage before and after. The pattern indicated that the same person had carried out the gambling site transactions and accessed her online banking.
  But in each case, Ms A's security details would still have been required.

- Ms A's card was not kept on her person and was accessible to others in the house, but she said that nobody in the household would have carried out the disputed transactions – no one would know the additional security credentials as described above.

- The disputed usage did not look like the work of an opportunist fraudster. The available balance of over £6,000 remained untouched. It was also strange that the two credits were made to the account. The adjudicator said he was unable see a reasonable explanation why someone intent on maximising monetary gain would do this. But whoever used the account appeared to have used a number of gambling sites, so financial gain may not have been the main motivation.

- There was no conclusive evidence of security details being compromised via a software breach.

Ms A and Mr B did not agree with the adjudicator's conclusions. In summary, they made these further points:

- They have always agreed that the events were not consistent with an opportunist fraudster or someone who stumbled on the cards while in their house. They felt the history of the events and directly related activity had not been explored adequately. This includes the IP address evidence.

- They did not think it was justified to regard the '3D secure' system as failsafe. They considered that the only plausible explanation was that covert key logging software had enabled the data to be harvested.

- The adjudicator referred to the credit limit not being approached and he questioned whether financial gain had been the motivating factor. But the further activity on the online payment service account, using the slightly altered email address, demonstrates that it was part of a wider sophisticated scheme motivated by financial gain.

- The disputed transactions were unlike their previous, genuine usage. The bank's protection system should have picked this up.

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 done so, I am sorry to tell Ms A and Mr B that I have come to the same conclusions as the adjudicator and for much the same reasons.

Where the evidence is incomplete or inconclusive or contradictory, as some of it is here, I reach my decision on the balance of probabilities – in other words, what I consider is more likely than not to have happened in the light of the available evidence and the wider circumstances.

I appreciate that Ms A says that no one known to her could have carried out the disputed transactions. But I cannot see how an unknown third party could have possessed all the personal security information that was required to make them. Ms A says that the information could have been gathered by fraudsters' software that had invaded her

computer, but there is no evidence of such a problem in her case, and her security software was up to date.

I note that the IP address evidence suggests that the disputed activity did not happen at the same location as the undisputed account use. But that does not necessarily show that the disputed activity was fraudulent. I must also take into account that whoever made the payments did not take full advantage of the credit limit and they then arranged for money to be paid back into the account. Ms A and Mr B agree that it was unlikely to have been an opportunist fraudster who made the transactions, but in my view the evidence suggests that it was not a fraudster at all. I do not believe that the other transactions on the online payment service account can explain why a fraudster would fail to take full advantage of the credit card account, or pay money back into it.

Ms A and Mr B feel that the bank's automated systems should have flagged the disputed transactions as suspicious events. But it is for the bank to decide how it scrutinises movements on accounts, and what balance to strike between security considerations and enabling customers to move funds freely. In the circumstances of this case I cannot say that the activity on Ms A's account was so unusual that MBNA was wrong to allow it.

Taking all the circumstances of this case into account, I do not believe the evidence shows that the disputed transactions were fraudulent, so I find that MBNA was entitled to hold Ms A liable for them. I do not require it to make a refund.

my final decision

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

Colin Brown
ombudsman