DRN-3429300

The complaint

Mr P complains that Barclays Bank UK PLC debited his account with a series of payments totalling approximately £8,000 which he says he didn't make or otherwise authorise.

What happened

Between January and August 2020, a series of approximately 625 payments were made from Mr P's account to a specific gambling merchant. These transactions totalled around £18,500 – though Mr P told our service there were about £8,000 of disputed transactions. There were credits in which were winnings from the gambling merchant which totalled approximately £11,000. Mr P strongly denies that he has any relationship with the merchant, and disputes making or otherwise authorising any payments to them. He said he hadn't noticed them on his account as he hadn't been keeping an eye on it during the period of the disputed transactions. He explained this was as he was unemployed, so he wasn't expecting any money to come into the account. Mr P said he noticed the transactions in September 2020, when he checked his account as he was working again and expecting his salary to be paid in.

Mr P said he doesn't know who completed the transactions, and he doesn't think it is someone known to him such as his family, whom he lives with. He said he hadn't given his card or details to anyone. Mr P advised Barclays that around December 2019 both his email and WiFi had been hacked after he clicked on a link from an email, and that he believes this is how his details were compromised and how someone was able to fraudulently transact on his account. He said he contacted the gambling merchant, who confirmed to him that there was no account held with them in his name or address.

Mr P raised numerous complaints with Barclays to dispute the transactions. Barclays raised numerous chargeback requests with the merchant. Some of these went undefended, so were refunded to Mr P's account. But they did defend some and provided details from the gambling account used to make the transactions. When Barclays completed their investigation, they declined to refund the disputed transactions on the grounds that they believed he had authorised them. They said this was because:

- There was no clear point of compromise for his card and details;
- When defending the chargebacks, the gambling merchant provided compelling evidence of an account held by Mr P with them, which included his correct name, mobile number and address. They explained there was no clear point of compromise for these details either;
- Mr P accessed his online banking often during this period, using their PIN Sentry device to do so. This required Mr P's card and PIN, which again there was no clear point of compromise for. Moreover, this would have meant he was aware of the payments but didn't report them until August.
- He moved winnings from the gambling merchant between his current and savings account, which implies that he was fully aware of the transactions.
- There were no further attempts to use Mr P's card from September 2020, when he had contacted them to dispute the transactions. This implied whoever was using his

card details knew the debit card had been cancelled and was no longer of use to them.

- There were a lot of matches between the IP address used to complete transactions, and the IP address used to access his online banking.

They also decided that they no longer wished to do business with Mr P, so they closed his account in November 2020.

Mr P wasn't happy, so he complained to our service. One of our investigators looked into what happened and didn't recommend that this complaint be upheld. They said the payments were most likely completed by Mr P himself as there was no clear point of compromise for all the personal data required to make the payments, no clear explanation for how they went unnoticed for all those months despite the online banking logins, and no benefit to an unknown third party in possession of the details needed to transact on Mr P's account to do so on a gambling website where the winnings would, and did, return to Mr P's account. Mr P didn't agree. So, it has come to me to decide.

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 am reaching the same conclusion as our investigator previously set out and for broadly the same reasons.

Generally, Barclays can hold Mr P liable for the disputed transactions if the evidence suggests that it's more likely than not that he made or authorised them himself. I'm satisfied from the bank's technical evidence that the payments were properly authenticated - Mr P's genuine card details were used to make the disputed transactions.

But the regulations relevant to this case say that is not, on its own, enough to enable Barclays to hold Mr P liable. So, I need to think about whether the evidence suggests that it's more likely than not that Mr P consented to these transactions being made.

From what I've seen, I think its reasonable to conclude that Mr P authorised the transactions. This is because:

- The disputed transactions were made using Mr P's genuine card details, but Mr P said he had the card with him during this period. Whilst I accept its possible, I'm not persuaded that it is the most likely explanation here that an unknown third party took Mr P's card and then returned it to him without him noticing or obtained the details by hacking his email and WiFi;
- I say this because the gambling merchant provided Barclays with evidence that the account was set up using Mr P's genuine details including his name, date of birth, phone number, copy of his legal identification (namely a passport or driving license), and a recent household bill. This causes me concern over the truthfulness of Mr P's account of what happened as he hasn't provided a plausible explanation for how an unknown third party would have obtained these details – but further, I can see no benefit to an unknown third party to use genuine details such as the phone number or email address. The gambling merchant use these to contact their customers – and if Mr P were not one then I would have expected him to have been alerted to the scam sooner – or an unknown third party would have likely seen this as a risk that could be easily avoided.
- Further to this, Mr P said that he hadn't checked his online banking during this period, which is why he hadn't noticed the transactions. But the technical evidence from Barclays showed that there were around 155 successful online banking logins during this period. Some of these logins used 'PINsentry' – a device which the

person logging in would put the genuine card and PIN into in order to access online banking. There was no clear point of compromise for his card and PIN which were required for these logins, so it seemed most likely that they were completed by Mr P. And if Mr P was logging in throughout this period, but wasn't making these transactions, I would find it very unusual that he didn't notice and report them more promptly.

- The same IP address was used to make the gambling transactions as Mr P used to check his online banking as far back as 2017, so the transactions were most likely completed on one of his devices or at least through his internet connection – and Mr P hadn't provided a point of compromise for these. Whilst he said his WiFi had been hacked, he hasn't provided any evidence of this and I think really this implies that the transactions were completed on a device owned and operated by Mr P.
- Any winnings from the gambling merchant are refunded to the original bank account the bets were paid from – indeed Mr P's account received approximately £11,000 in winnings. I cannot see a benefit to a fraudster making these transactions, as they couldn't have accessed the benefits of winning. If a third party had accessed all of the details required to make these payments, as well as access to online banking details, legal identification documents and recent bills, it seems highly unlikely that they would simply use them to gamble when they may not even be able to access the winnings – as Mr P could have noticed the transactions and cancelled the card at any time. I suggest that an unknown third party in possession of such valuable personal information would be more likely to have ordered goods or services that they could benefit from, spent as much money as quickly as possible, or even taken out credit in Mr P's name – rather than gamble frequently over many months. There were also other actions on the account during this time, such as moving winnings to and from his savings account, done on online banking. If a fraudster had this much access to his account, they could have simply emptied it.
- There were credits into the account during the period of disputed transactions, including payments from the Department of Work and Pensions, refunds, and cash deposited in branch. These payments were used in part to fund the gambling – yet Mr P didn't notice or question where his funds were going until August. This also undermines his statements that he wasn't checking his account further, as he said that the reason for this was that he wasn't receiving any income – and whilst this wasn't necessarily income from a job, he was receiving incoming funds.
- Mr P's account shows other history of gambling, so the activity was not unusual for his account.
- No further attempts were made to use Mr P's account after he cancelled the card – which implies whoever was using it knew it had been cancelled. I don't see how an unknown third party could have known this.

Based on everything I've seen, I think it's fair and reasonable for Barclays to refuse to refund the disputed transactions because I think it's more likely than not that Mr P made or otherwise authorised the transactions that he disputes.

My final decision

I don't uphold this complaint.
Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 2 June 2022.

Katherine Jones
Ombudsman