DRN-3304667

The complaint

Mr W is unhappy Barclays Bank UK PLC ("Barclays") haven't refunded a series of transactions made from his current account which he says he didn't make or otherwise authorise himself.

What happened

Mr W contacted Barclays in 2018 and 2019 to report a series of gambling transactions made between August 2018 and May 2019. In total, Mr W has disputed more than 300 transactions to a series of different gambling companies totalling more than £53,000:

11 August 2018 to 21 September 2018	247 transactions totalling £39,870
13 May 2019 to 14 May 2019	58 transactions totalling £13,800

Mr W has said that someone else made these payments without his consent and he requested that Barclays refund them to him.

Barclays initially reviewed Mr W's claim in late 2019 – but it only considered some of the disputed transactions at this stage. It only considered the transactions made between 13 May 2019 and 14 May 2019. And it told Mr W it wouldn't be refunding him because it believed the transactions had been authorised by him. This stance was repeated in Barclays' final response after Mr W raised a complaint about how it had handled his fraud claim.

As Mr W remained unhappy with the situation, he brought his complaint to our service.

Our investigator noticed that Barclays hadn't addressed some of the transactions that Mr W had disputed by the time Mr W contacted our service. So, after some additional clarification, Barclays agreed for our service to consider the remaining disputed gambling transactions which took place between August 2018 and September 2018 as well as the ones they'd already responded to as part of this complaint which I have detailed above.

I'm also aware Mr W has complained about a third set of transactions to a series of e-money service providers. However, these are yet to be addressed by Barclays – so they will form the subject of a separate complaint and I won't be commenting on them further here. *What Mr W has said to our service and Barclays*

- Mr W has said he didn't make any of the gambling transactions.
- He's told us that he lives with his mother, and at the time of the disputed transactions, he was self-employed. So, he doesn't think anyone would've been able to access his personal belongings such as his wallet or mobile phone.
- He remembers not having a debit card for a number of months – but wasn't completely sure when this was.
- He has made some genuine gambling transactions previously – but with a completely different company.

What Barclays has said to our service

- All of the disputed gambling transactions were made online – meaning only the card details were needed to process them.
- Barclays made a series of data requests to four different gambling companies involved in the dispute. All of these companies (who I'll refer to as 'A'/'B'/'C' and 'D') responded to the requests and between them, provided the following information:

    - Companies A, B and C provided information which showed the accounts were opened using the same information (name, address, date of birth, email address and phone number) that Barclays held for Mr W. Barclays didn't think that a third-party fraudster intending to defraud Mr W would've have used his genuine contact details when opening these accounts as this risked Mr W becoming aware that accounts had been opened in his name. Company D couldn't provide any information outside of confirming the account was in Mr W's name.
    - All four companies also confirmed no withdrawals were ever made on the accounts. So, if fraud had been committed and Mr W's identity stolen, the third-party fraudster had received no benefit from their actions.
    - Company A also provided copies of a series of emails in which someone asks why they're unable to deposit more money into the gambling account. The emails stem from two different email addresses – one of which was the one used to open the account and is the same email address that Barclays holds for Mr W.

- Companies A and B were also able to provide evidence of the IP addresses used to access their websites/services on the following dates:

    - 20 September 2018 to 21 September 2018
    - 11 May 2019 to 12 May 2019

    Barclays has pointed out that these IP addresses are identical to the ones used to access Mr W's online/mobile banking during the same timeframes as listed above. Mr W hasn't made Barclays aware of anyone else being able to access his online/mobile banking.

- Barclays says that Mr W has accessed his online/mobile banking on multiple occasions during both periods of disputed activity. This access is all carried out from the device Mr W appears to have been using as far back as March 2018. However, Mr W didn't contact Barclays about the transactions at the time. Barclays says this suggests Mr W was aware of the transactions and didn't have concerns about them.
- Overall, Barclays believe Mr W has authorised the disputed transactions and so it wouldn't be fair and reasonable to refund them to him now.

Our investigator initially reviewed the transactions that took place between 13 May 2018 and 14 May 2018. Having done so, he agreed with Barclays that the most likely scenario was that Mr W had authorised them and so it wouldn't be fair for Barclays to offer him a refund now. Our investigator said:

- He didn't think a fraudster would've been able to obtain everything which was needed to make the payments without Mr W's knowledge. This included, but wasn't limited to, Mr W's bank card details and mobile phone.
- The type of transaction being disputed wasn't out of character for the account as Mr W had a record of making payments to gambling companies previously.
- The evidence he'd seen from the gambling companies showed the accounts were set up using all of Mr W's genuine details. The accounts were also accessed using either the same or similar IP addresses to the ones used to access Mr W's online/mobile

banking. He didn't think it was likely a fraudster would've used all of Mr W's genuine details to open the gambling accounts – as this would create a risk of being caught.
- He also highlighted that the email chain which had been provided by one of the gambling companies was sent from the same email address that Mr W has been using to correspond with our service. It's unclear how a fraudster would also have access to Mr W's email address in order to send such emails.

In a follow up view, our investigator then addressed the remaining disputed transactions which took place between 11 August 2018 and 21 September 2018. Again, he was persuaded the most likely scenario was that Mr W had authorised the transactions. This was for several of the same reasons that I've just highlighted above. But in addition to this, our investigator also said:

- There would've been no benefit to a fraudster in using Mr W's card details to process these transactions. This is because the gambling websites would've most likely paid any winnings back to the same account. And as there was no indication that anyone else would've had access to Mr W's bank card and/or banking details in order to access this money – he couldn't see how a fraudster would've financially benefitted from their fraud or why they would have gone to the lengths of stealing Mr W's personal information to set up accounts for no obvious gain.

Mr W disagreed with our investigator's view. In response, he provided some additional comments:

- He referred to a third party (a previous business partner) who has left him in debt. Whilst it's not completely clear if he's referring to the same person or not, he's also suggested that a third party may've carried out these transactions as an act of revenge. This is a newly introduced scenario as initially Mr W told us that he was self-employed and he lived with his mother and so he didn't think anyone else would've had access to his card, phone and wallet.
- Mr W pointed out that the IP addresses used to make the transactions don't appear to match with the IP address of his home address. He also doesn't think IP address evidence is enough to prove he authorised any transactions. He also asked that we review the entire account history for his online/mobile banking to show how the account was being run.
- Mr W has said neither this service or Barclays have been able to prove the transactions were made by him
- He says he didn't contact the gambling company – even though one of the email addresses used is associated with him. This leads him to think his email address has been compromised and someone else has been able to gain access to it.

Unhappy with the investigator's view, Mr W requested an ombudsman's decision, so the complaint has been passed to me.

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'm satisfied Barclays has acted reasonably when holding Mr W liable for the disputed transactions. I'll explain why in more detail below.

The regulations relevant to this complaint are the Payment Services Regulations 2017 (the PSRs). The PSRs set out when a customer should be held liable for transactions which happen on their account and when they shouldn't.

The starting position is that a customer is liable for authorised transactions and a bank is liable if they're unauthorised. And where there's a dispute about whether a customer has authorised the transactions or not, the bank would be expected to provide evidence as to why they're holding their customer liable.

As a result, my role is to weigh up the information made available to me and decide whether I think it's fair and reasonable for Barclays to hold Mr W responsible for the disputed transactions. The Financial Ombudsman Service is an informal dispute resolution service. It is not a court of law. And it is my role to decide what I think is *most likely* to have happened based on the evidence I've seen. It is not to conclusively prove that Mr W made the transactions now in dispute in order to allow Barclays to hold him liable for them – as Mr W has suggested. When deciding what's fair and reasonable, I've considered all the possible scenarios and decided on the balance of probabilities, what I think is most likely to have happened. Having done so, I'm satisfied that the most likely scenario here is that the transactions were authorised by Mr W. I'll explain why below.

- Firstly, I note Barclays requested information from the four gambling companies where the transactions were made. Companies A, B and C have provided documented evidence to Barclays which shows that the gambling accounts were all set up with the same information. This includes Mr W's genuine name, address, date of birth, phone number and email address. All of which mirror the details both this service and Barclays hold for him. Company D couldn't provide as much detail due the time that's elapsed. However, it was still able to confirm the account was in Mr W's name.

  I appreciate that Mr W has indicated that someone may've found a way to obtain his personal information, such as his business partner, and used it to set-up these accounts. But I'm not persuaded this is what's happened here. I'm not persuaded that a fraudster, having gone to the lengths of taking Mr W's bank card without him knowing, would've registered Mr W's genuine contact details when setting up multiple fraudulent accounts in his name as this would've significantly increased their risk of exposure. For example, it's not unreasonable to assume that once the gambling accounts had been registered; emails, or text messages would've been sent to the contact details each gambling company held on file to confirm any substantive activity on the account i.e each time a deposit was made. And so it's unlikely that a fraudster intent on keeping their activity a secret would choose to set up fraudulent accounts using Mr W's genuine contact details when they could've used their own.

- I also note that emails were sent to Company A from Mr W's email address in May 2019 asking why the account in question was no longer able to accept deposits. Again, I appreciate Mr W has said he wasn't the one to send these emails and that he thinks his email address may've been compromised. But I'm not persuaded that's the case either. I say this because I'm not sure why a third-party fraudster would take the time to 'hack' Mr W's email address to prevent Mr W becoming aware of what was happening. Firstly, it's unclear how Mr W's password for his email account could've been compromised and secondly, as previously mentioned, it would've been easier for the fraudster to have simply to have used a different email address when opening the gambling accounts in the first instance.

- All four gambling companies also confirmed that no withdrawals were ever attempted on the disputed accounts. I accept there could be different reasons as to why this is the case. For example, the bets which were placed may not have been successful. But, even if some winnings had been won, it's likely these would've had to have been paid back to Mr W's linked bank account. As a result, I'm not satisfied there would've been a clear or obvious benefit to a third-party fraudster carrying out this activity from the outset. I do appreciate Mr W has referred to someone perhaps having carried out these transactions to gain some form of revenge. But again, I'm not persuaded this is most likely what happened. I haven't seen any further information or evidence that supports this scenario. And Mr W initially told us that it wasn't possible for anyone other than him, and potentially his mother, to have access to all of the information they would need to place these transactions. I'm satisfied that had this been a significant possibility it would've been suggested sooner than it ultimately was. This is coupled with what I've already said above about it being unlikely that a third-party would've supplied genuine contact details if they wished their activity to remain a secret.

- Companies A and B were also able to provide additional technical information, such as the IP addresses used to either register or access the relevant gambling accounts. The IP addresses used are the same ones used to access Mr W's mobile banking over the same period. For example, Company B has shown the gambling account was accessed on one occasion at 11:30pm on 20 September 2018. Four minutes later, Mr W's mobile banking is subsequently accessed from the exact same IP address. I would add that this mobile banking access came from a device which I'm persuaded belongs to Mr W. Barclays' records show this same device had been used consistently in the year and a half leading up to the disputed transactions. This means that whoever was carrying out activity on Company B's gambling account was in the very same location as the person who was also accessing Mr W's mobile banking using his known device. And given the short turnaround time between both events, I'm satisfied that it's most likely the same person carrying out both sets of activity. I've not seen any evidence that anyone other than Mr W had access to his mobile banking details (such as his passcode) nor had access to the mobile phone itself. As a result, I can't fairly say this is just a coincidence and so I'm satisfied that the most likely scenario is that this was Mr W.

  I understand Mr W has said the IP addresses in question don't match the ones in the area that he lives in. He has also mentioned that IP addresses can be mimicked – and so this issue doesn't prove he was the one carrying out this activity. I accept this is a possibility – but I'm not persuaded it's the most likely one. I've previously questioned why someone would go to such great lengths as to 'hack' Mr W's emails – and I think the same question is applicable here as well. There doesn't appear to be any logical explanation as to why a third-party would've tampered with things like IP addresses or 'hacked' Mr W's mobile banking – especially when the same third-party would've already had Mr W's card details and therefore could've chosen to make purchases if they'd wanted to do so rather than place gambling transactions which they could not benefit from.

- Mr W's mobile banking is also continually accessed throughout the period of disputed activity. For example, between 11 August 2018 and 21 September 2018, Barclays' evidence shows Mr W's mobile banking was accessed on 68 separate occasions. I find it unlikely that all of these separate logins could be associated with someone other than Mr W – he himself initially told us this wouldn't be possible.

The volume of transactions as well as the total amount being spent during this same period was substantial. And so I'm also satisfied it would've been noticeable each time the mobile banking account was accessed. However, there's no indication that Mr W ever reported what was happening on the account to Barclays until each period of disputed transactions had come to an end. And given Mr W has told our investigator that no-one else had access to his mobile phone I'm therefore satisfied that it could only be Mr W who was accessing the mobile banking and consequently authorising the transactions as well.

- Whilst the values might differ, I can see Mr W has made noticeable amounts of undisputed transactions to similar merchants which indicates this type of merchant/transaction type wouldn't be unusual for his account.

In summary, for me to be persuaded by what Mr W has said, I'd have to be persuaded that a third-party (either known or unknown) to Mr W:

- obtained Mr W's card details
- gained knowledge of all of Mr W's personal details – such as his address and date of birth
- gained access to Mr W's email account
- gained access to Mr W's mobile banking credentials as well as gaining access to his mobile phone itself; and,
- completed all of the above without Mr W noticing, and exposed themselves to the real prospect of discovery by Mr W for no obvious benefit to themselves

So overall I don't think it's plausible that someone other than Mr W would've been able to access all of the things need to complete these transactions or take this level of risk for no benefit. Instead, I'm satisfied the most likely scenario here is that Mr W has made the transactions himself and now regrets them.

For the reasons above, I'm satisfied Barclays have acted reasonably in holding Mr W liable for the transactions and I won't be asking it to take any further action here.

My final decision

My final decision is that I don't uphold Mr W's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 25 April 2022.

Emly Hanley
Ombudsman