DRN-2669214

Complaint

Mr T is unhappy that Barclays Bank Plc is holding him liable for a series of transactions he says he didn't authorise.

Background

In January and February 2020, a series of transactions were made from Mr T's account to a gambling account that had been set up in the name of his fiancée. The total value of those payments was over £30,000. In the course of our investigation into his complaint, it has also come to light that there are other transactions on the account which Mr T says he didn't authorise – but the bulk of the payments in dispute are to the gambling website. Mr T told us that he does have a historic relationship with this company. However, he had contacted the gambling company some time ago to ask that he be prevented from placing bets in the future. This is a process known as self-exclusion.

Mr T says that these payments weren't authorised by him. At the time he referred the complaint to us, he thought the payments might have been a result of an iPhone he sold in late 2019. He says this phone had enough information on it to enable a fraudster to set up a gambling account in the name of his fiancée and make payments to it. However, he has since provided screenshots of a text message exchange between him and his fiancée in which she concedes that it was her who carried out the transactions.

Mr T first noticed the suspicious transactions on his account in January. He called Barclays and explained that, as he'd self-excluded - the payments must've been a mistake. There were further payments to the bookmaker a few days after this call. Around two months later, he called Barclays to say that he was a victim of fraud and that the transactions should be refunded.

Mr T didn't tell Barclays that he'd been a victim of fraud in this first call. He assumed that this was most likely a mistake on the part of the bookmaker. He didn't tell Barclays what had happened until April, but he says that in reality many of the payments had gone unnoticed because he'd not checked his bank account on his online banking app during the period of disputed account activity. He'd logged on to the app – but he'd only done so to check his business accounts, not his personal one.

Barclays is holding Mr T liable for the transactions because it thinks it's likely he authorised them. It says that the Internet Protocol (IP) address from which Mr T's online banking app was accessed was the same one from which payments were made to the gambling website. It also thinks the fact that Mr T took so long to notify it of the disputed transactions suggests that he had intended to make them after all.

Evidence provided by the bookmaker suggested the account was created in the UK – or at least via an IP address that was in the UK. However, Mr T's fiancée was overseas throughout the period.

Mr T was unhappy with Barclays' response and so he referred his complaint to this service. It was looked at by an investigator who didn't uphold it. In summary, the investigator thought that:

- Mr T's phone didn't leave his possession throughout this period. But some of the transactions were authenticated using ApplePay. This was set up for Mr T's account in mid-January and was associated with a phone with his number. As part of the registration process, the fraudster would've needed access to Mr T's phone to get a One-Time Passcode (OTP). The investigator felt that this showed that it was his phone that had been used in connection with the transactions.
- There were transactions made from the account which the investigator thought were likely legitimate payments made by Mr T. The technical evidence provided by Barclays showed that these payments were carried out using the same device as the disputed transactions. The investigator concluded that this meant it was likely that whoever made the payments must've been in possession of his phone.
- There were additional payments made in London on things such as food and taxi fares. This coincided with a time that Mr T was in London. However, the geolocation of the IP address from which the gambling payments were made suggested they were made in a town over fifty miles from London which was close to where Mr T lived. The investigator thought that it was unlikely that a fraudster who'd acquired Mr T's phone would've made the same journey before making any gambling payments.
- The gambling company had told us that only one device had been used on Mr T's account.
- Barclays provided evidence showing regular log-ins to Mr T's online banking app throughout the period of disputed activity. The investigator thought it was likely that Mr T would've seen the transactions on his account. And if he'd done so, he would've told Barclays about them much sooner if they'd been unauthorised.
- It wasn't clear why a fraudster who'd come into possession of Mr T's account details would choose to set up a gambling account, since any winnings would necessarily be repaid into his account. The investigator didn't think it was obvious why a fraudster would be motivated to do this, rather than (for example) using the account details to purchase goods online.

Overall, the investigator concluded that it was more likely than not that Mr T had authorised these transactions.

Mr T disagreed with the investigator's opinion. He said:

- He didn't immediately think that the payments were fraudulent because he had been a genuine customer of this business in the past. It was still possible that they related to genuine bets he'd placed before his self-exclusion or perhaps they were the result of an administrative error on the part of the bookmaker.
- It's not true that, in order to register a Barclays account with Apple Pay, an OTP needs to be sent to the phone number associated with the account. He says that it's possible to register without this validation process taking place.
- The gambling website's claim that only one device was used for these transactions is false. Furthermore, he didn't log on to that site at all in March or April. If the IP address evidence suggests otherwise, someone must have done so without his knowledge.

- The disputed transactions were not made from his IP address. The IP address is for a shared wi-fi facility. He doesn't know who it was who authorised these transactions, but he's certain that it wasn't him.
- He didn't notice the suspicious activity on his account for two reasons. First, the email notifications that were sent by the gambling firm didn't go to his main email address. It was an email account that he'd set up to receive junk emails. And although he might have logged in to his online banking during this period, this was only to check his business accounts – he didn't check the account these payments were made from and so wouldn't have had any reason to think anything was wrong.
- His historic betting pattern with this gambling company suggests it's highly unlikely that these bets were placed by him. He also says it's not obvious why he would go to such lengths to create an account with this particular website. As he'd excluded himself from using their services, it would be simpler for him to just register with a different bookmaker entirely rather than attempt to circumvent the self-exclusion in the way that has been suggested.

Since then, Mr T has provided us with screenshots of a text message exchange between him and his fiancée in which she admits to being responsible for the transactions. He says that this evidence shows that he didn't authorise the transactions and so Barclays shouldn't hold him liable for them.

Because Mr T has disagreed with the conclusions of the investigation, the complaint was passed to me to consider.

I issued my provisional findings in December 2020 and said the following:

> *The basic position is that Barclays can hold Mr T liable for the disputed payments if the evidence suggests it's more likely than not that he made them or authorised them. For each transaction, Barclays has been able to provide evidence to show these payments were appropriately authenticated but that isn't enough to hold Mr T liable. I also need to consider whether the evidence suggests he consented to these transactions.*
>
> *The evidence I must consider has changed quite significantly since the investigator issued her view. At that time, Mr T had speculated that these transactions were carried out by an opportunistic fraudster who had used data found on his old phone. He now says that they were carried out by his fiancée and has provided text messages from her as evidence. I've considered this explanation carefully and I'm afraid I'm not persuaded by it.*
>
> *At the time Mr T made this complaint, he still believed that the sale of his old phone may have been the way that the security of his account had been compromised. It's now clear that the transactions were made using his iPhone. Each payment to the gambling website was authenticated using Apple Pay. Information provided by Barclays shows that the type of device used for the transactions was a mobile phone and that the facility was connected to a specific phone with Mr T's number. This is also supported by records provided by the gambling website. These show that each device used to access the online account is assigned a unique ID and that the same device was used to place each bet.*
>
> *Mr T's fiancée was overseas at the time and in a country where access to gambling websites is prohibited. However, he's told us he had a paid subscription to a Virtual Private Network (VPN) provider and gave her access to it. This enabled her to bypass local restrictions. He says he set this up to allow her to use various streaming*

services and social media that is prohibited in that country. But he says it would also enable her to access banned gambling sites. He's also told us that the bookmaker confirmed to him that it had spoken directly with his ex-fiancée and that she claimed that she was placing bets with her own money, but he's not provided any further information about this.

It might have been possible for Mr T's ex-fiancée to access the internet via his local internet connection. Mr T says that this would mean that the IP address would match his own and it would appear that the transactions had taken place in the same geographic location as Mr T. But this wouldn't explain how she was able to gain control of the device that was used to place the bets.

The transactions were made using an iPhone running the iOS operating system. In the exchange of message with his ex-fiancée, he mentions the Remote Desktop Protocol (RDP) which would've enabled her to access and remotely control a Windows computer. I'm not aware of any straightforward way of using this technology to remotely control another person's phone. And to manage to do so without their knowledge is even more unlikely. There may be more esoteric ways of remotely controlling an iPhone, but I understand that these would only work if the iPhone had been jailbroken and Mr T has already confirmed that was not the case here.
I also think it's significant that there was a series of other transactions around the time, including taxi fares, payments for food and so on. Mr T didn't initially dispute these. The evidence suggests they were made using the same device as the gambling transactions. However, he's since claimed that they were carried out by his ex-fiancée. She was out of the country at the time, but Mr T says that she could've made these payments online.

I don't think there is a straightforward way of paying an Uber fare or a restaurant bill remotely – and I'm not sure why Mr T's ex-fiancée would've felt it necessary to take control of his phone in order to do so. I also understand that these payments were all made in London and that Mr T was in London at the time. This is too much of a coincidence and, on balance, I think it's likely that these payments made in London were authorised by Mr T.

I also find it significant that, in the first call Mr T had with Barclays, he didn't suggest that these payments were unauthorised. Instead, he focused on the fact that he'd self-excluded from placing bets with this particular bookmaker and so thought it shouldn't have allowed the payments to go through. I find it unlikely that Mr T would've placed his focus on that if he genuinely believed these transactions were fraudulent.

If Mr T's ex-fiancée had intended to place these bets without him being aware of it, I think it's unlikely that she'd have registered the account with his email address as the main point of contact. This seems like too great a risk for someone who wanted to avoid detection. It's also not clear what benefit she could expect to receive from placing these bets. I say that because the bookmaker has been clear that any potential winnings could only be paid into Mr T's account.
I know Mr T has since said that the bookmaker confirmed they'd spoken directly with his ex-fiancée about the bets and that she'd claimed they were being placed using her own earnings but I'm afraid I've not seen any evidence to suggest this conversation took place.

Mr T responded to explain that he disagreed with my provisional findings. In summary, he said:

- He never suspected his fiancée because he still trusted her at that point and naturally assumed it must have been someone else.
- It's not true that an iPhone needs to jailbroken in order for it to be accessed and controlled remotely. The most important point is that Mr T's fiancée knew the password for his banking app.
- He didn't question the smaller payments made from his account because they often appear on statements later than the date the service is provided and he trusted the merchants that had billed him.
- He also mentioned correspondence from the bookmaker explaining that it had been in contact with Mr T's fiancée. A letter it sent to Barclays said that she *"was registered as a priority client and frequently contacted her account manager seeking free bet tokens. We also have contacted with [her] over the phone …"*
- The bookmaker shouldn't have accepted any of these bets, and Barclays should've carried out further security checks before allowing any of the payments to go through.

Barclays didn't respond to my provisional decision.

Findings

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 not persuaded to change from the position I set out in my provisional decision. Mr T has said that it's possible to place an app on an iPhone to allow it to be accessed and controlled remotely, and that this can be done without first jailbreaking the phone. I'll take that claim at face value. Mr T hasn't specifically claimed that his fiancée was able to access his phone in this way. Furthermore, he shared messages between them in which she appears to concede having accessed his account using the Remote Desktop Protocol – a specific application used for remote access to a PC using the Windows operating system. It wouldn't have enabled her to access his iPhone. So overall, I'm not persuaded that's what happened here.

I understand that why Mr T might not have queried the smaller transactions that were made to businesses in the UK from his account. But I still can't see any plausible explanation for how his fiancée would've been able to authorise these payments remotely. I also find it an unlikely coincidence that she would've done so throughout the same period Mr T was visiting the city in which those payments were made.

Finally, I accept what Mr T has said about the correspondence from the gambling company. This does suggest that there was some contact between the company and his fiancée. It doesn't, however, suggest that she said that she'd been spending Mr T's money.
It's impossible for me to know with complete certainty what happened here. With many of the cases that come to this service, the evidence is unclear, incomplete or contradictory. And when that happens, I must decide the case on the balance of probabilities. And with Mr T's case, the overwhelming weight of the evidence suggests that he authorised these transactions.

I'm sorry to have to disappoint Mr T, but I think it's fair and reasonable for Barclays to hold him liable for these disputed transactions.

Final decision

For the reasons I've set out above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 7 April 2021.

James Kimmitt
Ombudsman