

The complaint

Ms F complains about Barclay Bank UK PLC's decision to not refund her transactions which took place on her account in 2019 which she says she didn't make or authorise.

What happened

Ms F opened an account with a betting website who I'll refer to as 'C' in 2018. She opened this to manage a syndicate she had going on at work in relation to a sporting event. Ms F confirms that once the sporting event had finished (in 2018), she stopped using C.

Ms F opened the account with C using her iPhone 7 and says this has been the only device she's used while accessing the account. Ms F says she didn't write down her log-in details, store them electronically or share them with anybody else. Ms F no longer uses the iPhone 7 and it's locked away in a cupboard and protected with a passcode.

Ms F confirms she now has an iPhone XS which she's had since June 2019. This phone is locked with a passcode which is only known to Ms F and isn't a code which could be easily guessed by anybody else. The passcode Ms F uses for her phone is the same passcode she uses for her Barclays mobile application. When Ms F isn't using her phone, she says it is left in the kitchen of her house which she shares with family members or in her bedroom while it is charging. Ms F takes her phone to work and sometimes leaves it on her desk. The phone case Ms F uses for her iPhone XS has a section to hold a debit card, and Ms F confirms she keeps her debit card in there which she mainly uses for contactless transactions.

Around 21 September 2019, Ms F purchased a cake using her phone. She tried to log in to her Barclays mobile application but noticed it wasn't working. She used a web browser and then used her phone again but once she was able to log-in she noticed her balance wasn't what she was expecting. Ms F called Barclays and they explained transactions had been made to C between 19 and 20 September 2019. Ms F couldn't see the transactions on the mobile application as they were 'pending'. Ms F told our service she thought Barclays should have sent her a text message when the transactions took place, but they didn't.

A few days later, Ms F received a phone call from C. They explained somebody had sent messages using Ms F's account threatening to end their life. C confirmed the messages were sent on 20 September 2019, but C weren't alerted until around 24 September 2019.

The transactions Ms F disputes started around 30 August 2019 and totals around £21,000. Ms F says on the day the transactions started she attended a funeral, and she was at home and work during the other disputed transactions throughout August and September 2019. Ms F confirms she doesn't live with anybody who also works with her.

Ms F confirms she was having a few issues with her Barclays mobile application and kept receiving error messages. Ms F didn't raise her concerns with Barclays as she thought the issues were due to internet connectivity issues. Ms F said she didn't notice anything

unusual when she did log in to her Barclays mobile application and thought her balances were normal.

Barclays held Ms F liable for the transactions she disputes. They relied on the matches they had for Ms F's IP address which they cross referenced with a mobile device ID they hold for Ms F. Multiple IP addresses have been used previously for genuine transactions which Ms F doesn't dispute. Barclays have confirmed the IP address was first used in December 2018 and the mobile device ID was first used in June 2019.

Ms F is unhappy with the way Barclays dealt with her fraud claim – she doesn't think they carried out a full investigation. Ms F also thinks Barclays should have contacted the Police and other organisations such as Action Fraud on her behalf.

Ms F made a Subject Access Request (SAR) in November 2019 once the bank had declined her claim. She's unhappy they exceeded the time limit to respond to her and said there were calls missing and blank pages included.

Barclays responded to Ms F's complaint and apologised for the level of service Ms F had received. They apologised for the time it took to respond to Ms F's SAR, and that they'd sent some information to the local Barclays branch instead of to Ms F's home address. In a follow up response, Barclays located another call which they sent to Ms F and offered her £100 for the inconvenience caused.

Ms F brought her complaint to our service where one of our investigators looked into

it. The investigator didn't uphold Ms F's complaint. She thought that;

- Ms F had authorised the payments because the card and CVV details had been input into C's website. And the electronic records show the correct passcode was provided when using the Barclays mobile application to make transfers between the accounts.
- Ms F consented to the payments because the same device ID and IP addresses which have been used for genuine transactions were used for these disputed transactions. The IP addresses also match the internet service providers for Ms F's home and workplace. The email address which was used to reset the password with C had been accessed and Ms F confirms nobody would be able to access that email address as it's never been used on a shared device.
- Barclays aren't responsible to tell Ms F about transactions on her account, and because Ms F was regularly logging in to her Barclays mobile application, she thought it was reasonable Ms F should have noticed any unauthorised transactions herself.
- It's the role of the Information Commissioner's Office (ICO) to deal with issues or concerns relating to non-compliance with SARs.

In conclusion, the investigator thought that Ms F had carried out the transactions. And therefore, she didn't think Barclays was unreasonable to decline the claims. She also thought Barclays offer of £125 compensation was fair.

Ms F disagreed. I've summarised the points Ms F disagrees with below.

- She said she didn't authenticate or authorise payments to C.
- And she disagrees with the devices Barclays hold for her as she has never

owned some of the phones listed.

- Ms F also says at the times the transactions with C took place, it would have been impossible for her to carry out the transactions due to her working hours.
- She thinks the security around email addresses and IP addresses can be easily compromised.
- Ms F thinks C has poor security measures in place, and it would be easy for somebody to access her information including her email address and bank card even though she's been careful with it.
- Ms F also had some concerns around Barclays handling of her SAR.

As an agreement couldn't be reached, the complaint has been passed to me to review.

The investigator helpfully included a list of relevant transactions, Barclays mobile banking log-ins and log-outs to the account held with C. I haven't repeated that list as I'm satisfied all parties are aware of the relevant transactions.

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 agree with the investigator for broadly the same reasons. I appreciate this will come as a disappointment to Ms F – so I've explained my reasons further below.

Firstly, I appreciate Ms F has provided a lot of information regarding this complaint and the reasons she disagrees with the investigator's view. While I haven't commented on every aspect, I would like to reassure Ms F that to help me decide what happened, I've looked at all the evidence of the transactions, as well as the information that Barclays and Ms F have shared.

When considering what is fair and reasonable, I'm required to consider relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

The Payment Services Regulations are the relevant law here. These primarily require banks to refund customers if they didn't make or authorise payments themselves. So, when considering whether Barclays has acted fairly in rejecting Ms F's fraud complaint, one of the things I have to consider is whether Ms F made the transactions herself or allowed them to be made. If Ms F did, then we generally wouldn't ask the bank to refund her.

From looking at the evidence, I don't think it's unreasonable for Barclays to hold Ms F responsible for these transactions. I say this because:

- The account with C where transactions on Ms F's card was credited was held in the name of Ms F. The account was opened in 2018 by Ms F herself.
- All the payments were made using Ms F's card details, rather than the card itself. It's possible of course that someone could have obtained those details without

Ms F knowing. But I don't believe that's what happened here.

- The only person who could have accessed Ms F's Barclays mobile application was Ms F herself.
- The device used for the mobile application is secured by a passcode which Ms F says she hasn't shared with anybody. And additional security is needed to open the Barclays mobile application. Ms F hasn't offered a plausible explanation about how someone could gain access to her bank details or be able to access her phone.
- Ms F says an old email address was used to change the password on the account held with C. But she's also confirmed the email address has never been used on a shared device so it would be impossible for anybody other than Ms F to access it unless she'd given them the details herself.
- The IP addresses used for the transactions are the same as IP addresses Ms F has used herself previously for transactions which aren't disputed. Whilst that's not conclusive evidence (it's possible to hide or disguise an IP address), it's a further piece of evidence that links Ms F to the gambling transactions.
- I appreciate Ms F says she doesn't own some of the devices used to make the transactions, but I don't think that's relevant. I say that because the person who carried out the transactions had access to Ms F's device to access her Barclays mobile application and knew her passcodes to log-in to her other accounts. The device used isn't relevant, but somebody knowing the information needed is.
- Ms F says the timings of the transactions mean it couldn't have been her as she'd attended a funeral during one of the transactions, and she would have been at work for some of the others. But the transactions are linked to IP addresses and the internet service providers both at Ms F's home and place of work. Ms F has confirmed nobody she lives with also works with her.
- Ms F checked her account regularly. I find it surprising if she didn't notice these payments being made especially as some included transfers from her savings account to her current account.
- I note too that significant sums were credited to Ms F's account from C. I note she hasn't suggested that money was paid to her in error.
- I've also kept in mind that there would be no financial gain for someone other than Ms F to place the bets which she disputes. Any profits from winning bets would have been paid directly into Ms F's betting account and transferring that money into a bank account would not have been instant. Taking all of this into account I think it's unlikely the disputed activity it was carried out by a third party.

In summary, the disputed transactions took place from an online gambling account that Ms F already used. The multiple banking app logins suggest that Ms F had her phone at the time of the disputed transactions and, as I've said, there would be no financial gain for someone other than Ms F to place the bets.

Based on the evidence I've seen, I'm not persuaded that the gambling transactions were

carried out by someone other than Ms F. And so it wouldn't be fair to require Barclays to refund them.

I note Ms F is also unhappy at the information Barclays left out when she made a SAR. The investigator suggested that Ms F raise these concerns with the Information Commissioner's Office, who are better placed than our service to investigate data protection concerns. I can't add anything further to this advice.

I have, however, considered Barclays offer of £125 compensation for the service issues Ms F experienced when they dealt with her fraud claim and SAR. In the circumstances I think £125 fairly recognises the inconvenience caused of sending information to the branch instead of Ms F's home address and the delays in responding to the SAR.

My final decision

For the reasons I've explained above, I don't uphold this complaint. Under the rules of the Financial Ombudsman Service, I'm required to ask Ms F to accept or reject my decision before 15 September 2020.

Hayley West

Ombudsman