complaint

Mr F complains that Nationwide Building Society (Nationwide) allowed over £51,000 to debit his account without his authority or consent. He's unhappy that Nationwide has refused to refund these disputed transactions.

background

Mr F opened a current account with Nationwide on 15 May 2017. Mr F confirms he held a genuine account with a gambling company - J. He says that in the early hours of 30 May 2017 he requested withdrawals of his winnings from J to be paid to his Nationwide account. £51,836 was credited into Mr F's Nationwide account from J.

After the deposits into Mr F's Nationwide account, funds totalling £53,221.99, were spent with J. Mr F disputes all of the transactions to J from his Nationwide account that occur on 31 May 2017.

Below are the timings of the transactions and online banking activity which took place on Mr F's Nationwide account:

- Mobile and online log-ins to Mr F's Nationwide account:

Date	Time	Place/location	Type of transaction
30/05/17	*21:50 – 23:56*	*Online banking log ins*	*Mobile device & computer*
31/05/17	*00:41 – 04:29*	*Online banking log ins*	*Mobile device & computer*
31/05/17	*07:27 – 14:48*	*Online banking log ins*	*Mobile device & computer*
31/05/17	*17:00 – 23:45*	*Online banking log ins*	*Mobile device & computer*
01/06/17	*02:59*	*Online banking log in*	*Mobile device & computer*
01/06/17	*12:02*	*Online banking log in*	*Mobile device & computer*

- Transactions to J from Mr F's Nationwide account

Date	Time	Value range	Type of transaction
31/05/17	*12:55 – 22:18*	*79 successful payments ranging between £25 - £2k*	*Card payments to J*

Mr F says the transactions and mobile/computer log-ins during this time were not made by him and that his details were compromised by a scam HMRC text. He says his computer was remotely accessed during a cold call where he was told he had a virus on his laptop. He says his phone was cloned as well.

He says his accounts with various other companies have also been hacked and he's taken up disputes with them. Mr F has provided a range of emails, screenshots and receipts to show how he thinks this could have happened.

Mr F also complains about the way Nationwide treated him throughout the investigation of the disputed transactions.

In its final response Nationwide said its records show that Mr F accessed his account on both his computer and his mobile device (using finger print ID) during the period of the disputed transactions and didn't report the spending on his account at the time. It also said the IP addresses used for the disputed transactions matched that of Mr F's genuine use with J. Nationwide held Mr F liable for the transactions on the basis that he would've been aware of the transactions when logging into his mobile banking and didn't report them.

Nationwide also commented that it didn't feel it had been rude or treated Mr F unfairly when dealing with his calls about the disputed transactions.

Nationwide gave Mr F two weeks' notice and closed his account in July 2017.

Unhappy with Nationwide's final response Mr F brought his complaint to our service. One of our investigators looked into things and concluded that Nationwide hadn't made any error in holding Mr F liable for the transactions. He said that whilst Mr F had provided a lot of information about his laptop, internet connection and mobile phone this didn't evidence that they had been hacked in order for these transactions to have occurred. He concluded that on balance it was more likely than not that Mr F carried out these transactions himself and so he felt Nationwide's conclusions weren't unreasonable.

Mr F didn't accept these findings and asked for an ombudsman to review his complaint. So the complaint has been passed to me to consider.

my 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've decided not to uphold the complaint, for broadly the same reasons as the investigator.

Mr F is adamant that he didn't carry out these transactions and I can see he has gone to great lengths to provide as much information as possible about what he thinks might've happened. I've looked at that evidence, the evidence from Nationwide and the circumstances surrounding the transactions to reach my conclusions.

In short, Nationwide is required to refund the amount of an unauthorised transaction. The relevant regulations, to this effect, are the *Payment Services Regulations 2009 (the PSRs 2009).* Mr F says he didn't make any of these payments to J from his Nationwide account and is seeking a refund of £53,221.99. So my primary concern is to come to a view about whether or I not I think Mr F authorised the payment.

the evidence Mr F has provided

I agree with the investigator that the evidence provide by Mr F to demonstrate his laptop and phone were hacked is inconclusive. Mr F explained that his phone had a fault but that doesn't show it was hacked. Mr F has provided evidence he took his laptop for assessment but this again doesn't show that the laptop was compromised only that he took his laptop to be assessed and there was evidence of some malware on the laptop.

I accept that there is evidence of malware on Mr F's laptop but I have to balance that against the other evidence and this doesn't show what the malware was used for, how long it had been on the laptop and whether it coincides with the timing of the disputed withdrawals.

Mr F has also reported the incident to the police and action fraud and feels he has provided everything he can.

I appreciate all the evidence Mr F has provided and the lengths he has gone to provide as much as he can. But I can't consider this evidence in isolation and having considered everything I don't think that these transactions were carried out without Mr F's consent or authority.

the disputed transactions with J

Mr F confirms there are genuine payments on his account to J on 30 May 2017 and many others before this date. Mr F opened his account with J a month prior to these transactions. Overall he deposited over £54,000 into the account and made bets and wagered significant sum before the genuine withdrawals to his Nationwide account on 30 May 2017. As an example Mr F accrued winnings of £32k on 27 May and then placed bets using these funds and depleting his balance to zero on the same day.

J has provided evidence of the gambling transactions on Mr F's account. This evidence shows that the type of bets Mr F was making throughout April and May were similar to those that he is disputing on 31 May 2017. The transactions are also at a similar time that Mr F has made genuine gambling transactions and at a similar frequency. The pattern of spending on the account with J doesn't look unusual and is similar, in my opinion, to Mr F's usual use of the account.

Mr F withdraws the funds from J at approximately 2.50am on 30 May. Then there is activity on the account with J at approximately 12pm on 30 May. This continues until approximately 1pm that day. Then there is activity on the account again at midnight on 31 May. There is further activity on the account with J using a mixture of "free plays" and very low level wagers until a deposit of £25 at approximately 1am then this is depleted to a zero balance at around 1.30am. At 5.40pm on 31 a £100 deposit is added to the account with J and play continues then until 10pm that same day. This is when the disputed deposits increase as bets are placed, almost continually through this time. Having reviewed this activity, as I've said, it looks very similar to Mr F's genuine pattern of activity on his account with J.

In addition to the above evidence I have also considered some of the events around the transactions which can't be explained by Mr F's version of events.

- Mr F had just deposited over £50k into his Nationwide account. There's no explanation how an unknown fraudster would've been aware that this money had just been deposited into his account. And it seems unlikely that a fraudster decided to hack his accounts at this time to gain access to these funds when previously there had only been a maximum of almost £600 in his account.

- If someone other than Mr F did gain access to his account there's no benefit to a fraudster or someone else to spend this money back with the same gambling company. It would be unusual for a fraudster to do this rather than try to withdraw the money or attempt to transfer it or spend it on goods or services to gain the most benefit, especially if they have access to his online banking log information and access to his mobile app. And the types of games played with J would be of no benefit to a fraudster – either the house wins or the funds return to the same account they were deposited with.

- Mr F's phone, laptop and gambling account all needed to be hacked at the same time in order for this to be successful. Whilst I accept this is possible, I don't think this is the most likely explanation, especially as the spending was back to a gambling website with no obvious benefit to the fraudsters (any winnings would go back to the same account which the fraudster already has access to – if Mr F's version of events is correct).

- There is no explanation how the finger print authorisation was used on Mr F's phone – by someone other than Mr F - to log into his mobile banking during the time of the disputed transactions. Even if I were to accept that Mr F's devices were remotely access or hacked in some way this doesn't explain how Mr F's fingerprint was used to authenticate the mobile log-ins, which happened during the time of the disputed transactions. I think it's more likely this was Mr F logging in during this time.

Nationwide's investigation and contact with Mr F.

Mr F says he feels he was "attacked" by Nationwide during the calls he had with them and that this caused him stress.

I've listened to those calls and I can hear Mr F is frustrated but I think that's about the situation he found himself him rather than Nationwide being at fault with the way it handled things with him.

Mr F says Nationwide had a duty of care when allowing this amount of money to leave his account. The investigator said it's not for us to comment on Nationwide's fraud systems and what transactions may trigger it. Nationwide has provided evidence that these transactions were carried out on the same device and using the same IP address that Mr F had genuinely used. The transactions were also made to a gambling account with J that Mr F used previously and confirmed with Nationwide as being genuine – which is perhaps why Nationwide didn't detect these transactions as being suspicious. I agree that these transactions do appear out of character in terms of the other spending from Mr F's Nationwide account (although it hadn't been open for long so it's difficult to determine what he usual spending would have been). But ultimately I don't agree that Nationwide did anything wrong in allowing these transactions to leave Mr F's account as I believe they were genuinely made by Mr F.

Summary

Whilst I accept its possible Mr F's laptop, mobile and gambling account could've all been hacked in order for a fraudster to spend this money. Weighing up everything, I don't think this is the most likely explanation for what happened. I think it's more likely that Mr F carried out the transactions himself and therefore Nationwide's conclusions to hold Mr F liable for the transactions isn't an unreasonable one.

my final decision

For the reasons I've given I don't uphold Mr F's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 22 September date 2019.

Sophia Smith
ombudsman