

The complaint

Mr M is unhappy because Nationwide Building Society allowed transactions totalling almost £17,000 to leave his account which, he says, he didn't make or otherwise authorise and it has also unfairly recorded a CIFAS marker with the National Fraud Database.

What happened

The circumstances that led to this complaint are well-known to both parties, so I won't repeat them in detail here. But, in summary:

- Mr M says his mobile phone was lost or stolen on 21 December 2019, along with his Nationwide debit card and his logon details (including passwords) for his Nationwide mobile banking facility and an online gambling account. By the time he realised this – less than 48-hours later – and reported the matter to Nationwide, 38 payments had been made from Mr M's current account to the online gambling account and one debit card, contactless payment had occurred.
- Nationwide refused to refund the payments because it considered Mr M had acted with gross negligence in failing to protect his mobile device and security details and/or it didn't consider it likely a fraudster was responsible for the disputed payments. It closed Mr M's account and reported a CIFAS misuse of facility marker to the National Fraud Database.
- Our investigator thought it was more likely than not Mr M had made the payments himself. And he didn't think Nationwide had unfairly refused to refund the money or reported the matter to CIFAS.

Mr M didn't accept the investigator's findings, so the complaint 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've reached the same conclusion as our investigator, for much the same reasons. I'll explain why.

- In line with the Payment Services Regulations 2017 (PSRs), Mr M isn't liable for payments he didn't authorise, unless he failed with gross negligence or intent to comply with the terms of the account or keep his personalised security details safe.
- I've considered whether Mr M authorised the transactions that've been disputed – and so, in line with the PSRs, whether he completed the agreed steps to make the payments or gave consent for someone else to complete them. And where there's a dispute about what happened, I've based my decision on the balance of probabilities. In other words, on what I consider is most likely to have happened in the light of the evidence.
- All but one of the disputed payments went to an online gambling merchant and I'm

satisfied it's more likely than not they all went into the account Mr M set up a few days previously. But Mr M disputes having made, or consented, to these payments. He suggests he dropped his phone, without realising, and whoever found it was able to log into and pay money to his online gambling account because his debit card, gambling and mobile banking login details were all kept in his phone case. Mr M accepts Nationwide's suggestion that keeping all this information together amounts to gross negligence and I'm minded to agree. But, given everything I've seen, I don't think it's more likely than not a third party undertook the disputed transactions. I say that because:

- Given the size and weight of his phone (including the case) I have some doubts that Mr M wouldn't have noticed it being lost in the way he describes.
- Mr M says he has a passcode set on his phone and he hasn't said a record of which was kept with the phone. So it's not clear to me how a fraudster would have known, or been able to guess, the passcode in order to unlock and access Mr M's mobile banking and online gambling facilities. But the records provided by the society and the online gambling company indicate Mr M's mobile banking facility was accessed while the phone was out of his possession. The activity on the current account include checking the recent and pending transactions. But there were no apparent attempts to transfer money out in order for a fraudster to derive some benefit from having access to his current account. Mr M says this wouldn't have been possible because the fraudster wouldn't have had his card reader. But a fraudster, unfamiliar with Nationwide accounts and mobile banking facility, may not have known the process for setting up a new payee, before trying to steal Mr M's money – not all current account providers require a card reader when setting up a new payee.
- Mr M's online gambling account was accessed using the same IP address as was used to log into his mobile banking facility during the time Mr M says his phone was not in his possession.
- Mr M does not dispute having set up an account with the online gambling merchant less than a week before the disputed transactions occurred. And the gambling merchant has confirmed that a total of £20,000 was credited to his account using his Nationwide debit card between 16 and 23 December 2019. Also that £5,300 worth of winnings was paid back to this card – which show as two transactions on his account statements on 17 and 20 December. Online gambling merchants usually only pay winnings back to the account or debit card from which the credit payments originated, and that seems to be the case here too. In such circumstances, an individual who may have got access to Mr M's gambling accounts would have difficulty recovering any winnings.
- A fraudster could have used (or tried to use) Mr M's debit card to buy goods or services using the contactless facility and, thereby, derived a direct benefit from being in possession of his debit card. But Nationwide's records suggest there was only one contactless payment during the disputed period of time – a £4.80 travel charge.
- Mr M tried to use his replacement debit card but it was declined which, undoubtedly caused him some inconvenience. This was because, after issuing the new card, Nationwide finalised its investigation and decided to close Mr M's account without notice which would likely have resulted in his new debit card being blocked too. I think the society was entitled to end its relationship with Mr M in the way it did, as provided for in the account terms and conditions and given what I've said already above about the disputed transactions. I also note the society's record suggest it called Mr M on 31 December 2019 to try and share its findings, but left a message and sent a letter after

being unsuccessful in contacting him. The letter confirmed all of Mr M's accounts would be closed immediately – it looks like this eventually happened on 9 January, which was a slight delay, possibly to allow a direct debit to leave the account and Mr M's salary to be credited. It's unfortunate Mr M didn't receive the society's letter and instead had to be told about his fraud claim being declined and account being closed during a phone call that took place in branch when he, perhaps did not have the privacy he would have preferred. And I note he's suggested Nationwide's decisions about the disputed transactions and the account closure amount to discrimination. But, overall, for the reasons I've set out, I think Nationwide acted in a fair and reasonable manner.

Our investigator outlined the level of evidence required for Nationwide to load a CIFAS marker, so I won't repeat this in detail. But, in summary, Nationwide need to show there were reasonable grounds to believe that fraud or a financial crime has been committed or attempted and it has clear, relevant and rigorous evidence relating to this. Given everything I've already said about the disputed transactions, I'm satisfied Nationwide fairly reported the CIFAS marker and I can't fairly instruct the society to remove it.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 9 November 2021.

Ruth Hersey
Ombudsman