

## **Complaint**

Miss L complains Nationwide Building Society (Nationwide) won't refund a cash withdrawal and an online bank transfer which she disputes to authorising.

## **Background**

I sent Miss L and Nationwide my provisional decision on this matter on 5 March 2021. In my provisional decision - which forms part of this final decision and is attached below – I said that I wasn't planning to uphold Miss L's complaint.

Broadly I said that because I thought it was implausible – based on what Miss L had told me and the information we had - that someone unknown to Miss L:

- stole her debit card and reader
- travelled thousands of miles to another country
- registered on her online banking using her personal memorable data
- accessed her genuine email account with her personal security credentials
- and then returned her debit card to her within a few days after committing fraud against her

I went onto say that without stronger evidence, I wasn't persuaded someone carried out the disputed transactions without Miss L's knowledge. So I thought it was more likely Miss L consented and therefore authorised the transactions she disputes.

I also considered some other events that suggest Miss L may have been the victim of fraud. But I found they didn't explain how a potential fraudster knew so much about Miss L's personal information without her being involved in some way.

I then invited both parties to submit any further evidence or comments they would like me to consider before I reach my final decision by 26 March 2021. That time has now passed.

Both Miss L and Nationwide haven't responded. So I will now decide this matter.

## **My findings**

I've re-considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. And having done that, and for the same reasoning that I set-out in my provisional decision, I've decided not to uphold this complaint.

As neither party has raised any new arguments, or sent me new information to consider, the reasons for reaching this decision are summarised above - and set-out in detail below in my provisional decision.

## **My final decision**

I've decided to not uphold Miss L's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss L to accept or reject my decision before 30 April 2021.

Ketan Nagla  
**ombudsman**

### **COPY OF PROVISIONAL DECISION**

#### **Complaint**

Miss L complains Nationwide Building Society (Nationwide) won't refund a cash withdrawal and an online bank transfer which she disputes to authorising.

#### **Background**

Miss L says that £500, withdrawn from an ATM in the UK, on 19 September 2017 from her Nationwide Flex account was done so fraudulently. She adds that an online payment from the same account sent the following day, on 20 September 2017 for £10,000, was also not authorised by her.

An amount of £900 was also credited into Miss L's account on the 19 September 2017. These funds were confirmed as fraudulent and returned to source by Nationwide.

Miss L says she'd been living abroad for some four to five years around this time. She adds that she'd put aside considerable funds in her Nationwide Flex account which she used infrequently to top-up another of her UK accounts.

A personal loan application in Miss L's name was also made around this time with Nationwide for around £13,500. Nationwide cancelled this before any funds were released.

Miss L says she was unable log into her Nationwide account on the 24 September 2017. This prompted her to call Nationwide. Miss L says she then discovered someone had called Nationwide pretending to be her on the 21 September 2017. Nationwide asked her to attend one of its branches in the UK with proof of identity so that it could be satisfied she was its genuine customer.

Miss L says she had the debit card for the account at this time. And, as far as she was aware, it had always been stored in a suitcase in her bedroom along with all her UK banking cards and associated items.

In October 2017, Miss L attended a Nationwide branch in the UK to show she was the genuine customer. Following this she made a claim for the two transactions she disputes. Nationwide raised an indemnity with the bank the £10,000 transfer was sent to.

Nationwide was able to recover £180 of this from the bank. This amount has been credited to Miss L's Nationwide account.

After Nationwide declined Miss L's fraud claim, she complained. Nationwide didn't uphold her complaint, so she referred the matter to this service.

One of our investigators then looked into the matter and they didn't recommend the complaint be upheld. In summary they said:

- Both transactions were authenticated as they'd seen evidence the correct process was followed by CHIP and PIN and a One Time Passcode (OTP).
- It's most likely Miss L gave her security details to someone but did not give them authority to make the transactions. They said that because there was unusual activity on Miss L's account which they didn't think she was involved with. Specifically, a £13,500 loan application, £900 fraudulent credit, call from an unknown third party and an attempted online login from an IP address not associated with the UK or the country where Miss L resides.
- So they didn't think Miss L authorised the two transactions of £500 and £10,000.
- As someone would have needed the bank card, PIN number, access to Miss L's email account, a Nationwide card reader and Miss L's memorable information used for online login, our investigator said it was unlikely they could have got this information all on their own. Because of this they went on to say Miss L most likely gave someone her personal security information that enabled these transactions to happen.

Our investigator then said Miss L failed with gross negligence. But they later amended this and said she had failed with intent and *not* gross negligence. That is, Miss L most likely gave her personal details to someone else which is in breach of the account's terms and conditions.

So they concluded that Nationwide had not done anything wrong and it doesn't need to refund the transactions to Miss L.

Miss L didn't agree with what our investigator said. Some of the key points she made are:

- She never shared any banking or personal details with anyone – not even her closest family.
- Whilst living abroad, she had at times lived in shared dwellings. Her UK banking cards and anything related to this were kept in luggage in her bedroom. Both the bedroom and luggage weren't locked.
- Why was Nationwide only able to recover £180 from the bank the £10,000 was sent to, and why did the fraudster leave that amount behind.
- Why didn't Nationwide pick up on the unusual transfer of £10,000 and ask her questions and/or block the account before sending it. Especially as she'd previously only sent £2,000 from her Nationwide account to her other UK bank.
- She uses similar passwords and PIN numbers for everything. In the notes section of her phone, she has a list of her accounts with the corresponding username and passwords. Miss L says she may previously have given a housemate access to her phone.
- The only explanation Miss L can think of is that someone she shared her house with accessed her details from her phone, and either used her card themselves or gave it to someone who travelled to the UK, and then put it back.

As Miss L didn't agree with what our investigator said, the complaint has now been passed to me to decide.

### **My provisional findings**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. And having done that I'm planning to not uphold Miss L's complaint.

I know this will disappoint her, so I'll explain why.

I'm satisfied from the bank's technical evidence that Miss L's genuine card and PIN were used to make the disputed transaction relating to the £500 ATM withdrawal. I'm also satisfied the £10,000 bank transfer was authenticated using the genuine card, PIN and OTP.

But the regulations relevant to this case say that is not, on its own, enough to enable Nationwide to hold Miss L liable.

The relevant regulations, to this effect, are the Payment Services Regulations 2009 (the PSRs 2009). Under the regulations, a payment transaction is regarded as having been authorised by the payer only if the payer has given their *consent* to the execution of the payment transaction.

So, I also need to think about whether the evidence suggests that it's more likely than not that Miss L consented to the transactions being made.

I'm satisfied Miss L's card wasn't cloned. Based on what our service has seen and the industry guidance available to us, we have yet to see a complaint where the CHIP on a card has been cloned. So I'm satisfied Miss L's genuine card – the one she had in her possession – was used.

I'm also persuaded that both transactions were most likely carried out by the same person, given the genuine card was needed for both transactions and they were done a day apart.

Both transactions Miss L disputes required the genuine CHIP to be present. As I've already said, Nationwide's records show that the ATM transaction was done so with the genuine card. Similarly, in order to carry out the online transfer the CHIP had to be read by a Nationwide card reader after which an OTP was sent.

Miss L says she was at home and not in the UK at that time. And to her knowledge her Nationwide card was always in her possession. It follows then that if somebody else had carried out these transactions without her knowing, then they would have to take the card, travel a substantial distance to the UK, and then have returned it a few days after using it. This is also the only explanation Miss L can put forward herself.

Miss L says it could have been someone she shared her house with, who then accessed her account username and passwords from her phone, and either used her card themselves or gave it to someone who travelled to the UK, and then put it back.

I've thought about this, and it seems implausible given the risk someone had to go through in order to pull this off – especially returning the card within a few days of the fraud before Miss L could know it was even gone. I accept however that it's not impossible.

Carrying out the ATM transaction required only the card and knowledge of the PIN number. But in order to carry out the online transfer a lot more had to be known about Miss L's personal information. Having closely reviewed Nationwide's records relating to Miss L's online banking activity, I note the following key events occurred between 12 and 24 of September 2017:

- A OTP was generated and sent to Miss L's email address for her internet banking registration and then was entered successfully
- A card security reader was used to verify the customer
- There were successful logins on four separate occasions, in which Miss L's memorable data questions were answered correctly

Having given this careful thought, I find it too implausible that someone unbeknownst to Miss L:

- stole her debit card and reader
- travelled thousands of miles to another country
- registered on her online banking using her personal memorable data
- accessed her genuine email account with her personal security credentials
- and then returned her debit card to her within a few days after committing fraud against her

So, on balance, I'm persuaded Miss L either knew what was going on – or she had given all of this to someone for another intended purpose. If they then went onto carry out transactions she didn't agree to or instruct, that would still mean she consented to them.

In considering this matter, I'd asked Miss L if anybody close to her and with access to her room had travelled to the UK and returned within a few days of her logging into her account. Miss L hasn't said anything specific about any individual.

She says it's possible someone she knew did this - or that they gave her details and card to somebody else to do so. But given how close someone needed to be to her in order to effect the fraud, I'd expect Miss L to know more about who specifically could have done this.

So, without stronger evidence, I'm not persuaded someone carried this out without Miss L's knowledge. So I think it's more likely Miss L consented and therefore authorised these transactions.

In coming to this conclusion I'd like to assure Miss L that I've thought very carefully about all the irregular and suspicious events surrounding her account at this time. This includes

- Miss L's online banking being re-set on 12 September 2017

- a fraudulent payment of £900 being paid into her account the same day the ATM transaction was carried out which was later returned to source.
- A personal loan of £13,500 being applied for in Miss L's name - albeit the funds were not dissipated by Nationwide.
- Someone calling Nationwide on the 21 September 2017 purporting to be Miss L and saying the £10,000 was a loan to a friend, and confirming they'd made the loan application.
- Once logged in, Miss L's online banking email address being changed to a different one to the one we know as genuine.
- A failed login on Miss L's account from a country other than the UK and where she resides.
- An application for a substantial overdraft limit.

I accept that all these activities, especially in the context of what Miss L is complaining about, raise serious questions about whether there was someone – or several people - conspiring to commit fraud against her.

But the reasons I explained above, I'm not persuaded these activities explain how a fraudster knew so much about Miss L's personal data - and how they had possession of her card and reader without her being involved in some way

For the sake of completeness, I've also looked into whether there was a possibility another card was ordered and then used to carry out these transactions – especially as Miss L's registered address with Nationwide is still here in the UK. Nationwide have given me records to show that there was only ever one card issued for this account up until the disputed transactions took place.

I note Miss L questions why Nationwide didn't take more action to prevent the £10,000 transfer by blocking it as unusual activity given her previous behaviour and spending pattern. Nationwide say it didn't need to as the transfer was verified by the genuine CHIP being read by its reader, and the OTP being correctly entered.

I think this would be a valid consideration, and something I'd have to give more thought to if I didn't think Miss L likely authorised these transactions. But I've already said I find it most likely she did.

Miss L questions why £180 recovered by way of indemnity wasn't returned to her Nationwide account. But I've seen Miss L's banking records which show that it was.

So, after weighing everything up, I'm currently minded to not uphold Miss L's complaint

### **My provisional decision**

For the reasons set out above, I'm intending to not uphold Miss L's complaint.