DRN-4486721

The complaint

Ms L complains that National Westminster Bank Plc ("NatWest") won't refund transactions she didn't make or otherwise authorise.

What happened

Ms L has held a current account with NatWest for several years. She moved abroad in 2017 but didn't update her postal address with the bank at the time. When the debit card she'd been using expired in 2020, NatWest sent a replacement card to the UK address it held on record. Ms L says she didn't receive the replacement card. In 2022, when she was unable to log in to her online banking, Ms L contacted NatWest using its digital assistant. Later, a member of staff contacted her and Ms L says they helped restore access – although they didn't explain why she'd lost access in the first place.

Ms L says when she managed to log on, she discovered several transactions had been made from her account since the start of that year which she didn't recognise. She reported this to the member of staff she'd been in contact with, before going back to the digital assistant to raise concerns. Ultimately a complaint was made about the lack of response. NatWest said it was sorry Ms L didn't receive a response to her correspondence with the concerned member of staff. It also informed her of the steps she needed to take to log a fraud claim. Unhappy with NatWest's response, Ms L referred the matter to our service.

Our investigator concluded that NatWest didn't need to refund the transactions as, on balance, they were authorised. The investigator explained that several of the disputed transactions required a one-time passcode (OTP) to be inputted on the merchant's website before the payment could be completed. So, it wasn't just the debit card information that was required for the payments.

Ms L didn't agree with the investigator's findings and said she didn't receive her replacement debit card and the OTPs. The complaint was then passed to me to decide and, as the rules the Financial Ombudsman Service operates under allows me to, I attempted to resolve the dispute through mediation by sharing my thoughts informally with Ms L. I gave further reasoning for why I intended agreeing with the overall outcome investigator had reached. Ms L remained adamant that none of the OTPs were received and so she couldn't have been involved somehow in the authentication of the disputed transactions.

After carefully reviewing Ms L's response, I requested further technical evidence from NatWest. Specifically, further evidence that the additional verification (3DSecure or 3DS) that was required to approve most of the transactions was initiated through an OTP. NatWest explained that the 3DS authentication request – which it had previously evidenced did happen in this case – could be completed in a number of ways:

(i) through its mobile banking app if the customer is enrolled to mobile banking and the app is set up to receive payment approval requests,
(ii) a six-digit code sent to the customer's mobile as a traditional text if the customer doesn't use mobile banking but a mobile number is held on file,

(iii) a six-digit code provided via an automated call if the customer doesn't use mobile banking and hasn't provided a mobile number but has provided a landline number,
(iv) a six-digit code sent to the registered email address if only an email address is held on file, or
(v) asking the customer to call the bank if no contact details held on file.

While it didn't provide evidence that 3DS verification was sent via an OTP, NatWest provided system screenshots which show that at the relevant time Ms L's mobile banking app wasn't set up to receive and approve payment requests. The bank said evidence shows that 3DS authentication was completed via an OTP which would have been sent to Ms L's mobile phone number held on its record since 2017 (and remains unchanged).

I wrote to Ms L again and explained that while reviewing the case file again, I had noticed that there had been a successful log on in between the disputed transactions. The log-in data shows that her account was accessed from the country she resides in. I said to Ms L that as there had been no suggestions that her security details were compromised, on balance, I was persuaded that the account was accessed by her at that time. As no concerns were raised when more than 20 transactions in dispute had already debited her account by that point, I remained satisfied that it was fair of NatWest to treat the transactions as authorised.

Ms L remained unhappy with my provisional conclusion. It's now appropriate for me to formalise my findings and issue a decision on this complaint.

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.

Firstly, I'm sorry to hear that this incident has left Ms L distressed. I'd like to reassure her and NatWest that although I've only given an overview of what happened, so not everything that has been submitted and argued is mentioned, I have read and considered everything we've been provided in its entirety.

When considering what's fair and reasonable, I'm required to take into account relevant law and regulations; the regulator's rules, guidance and standards; the codes of practice; and, where relevant, what I consider good industry practice at the relevant time.

Where there's a dispute about what happened, and the evidence is incomplete or contradictory, I must make my decision on the balance of probabilities. In other words, what I consider most likely to have happened in light of the available evidence.

Generally, NatWest can hold Ms L liable for the disputed transactions if the evidence suggests it's more likely than not that she, or someone acting with her authority, made or authorised the transactions.

From the information available, the disputed transactions – which took place between February and May 2022 – were made using a debit card which was issued to Ms L in early 2020 and sent to her registered UK address at the time. The technical data also shows that the transactions were made online/over the internet, and that several of these transactions were verified using the 3DS technology. Essentially, this is an additional level of authentication to complete the transaction.

In my informal correspondence with Ms L, I had explained that the debit card wasn't physically needed to make the transactions as they were not made in person. But a code was required which had to be entered on the merchant's website for most of the transactions. So, for a third party to have been able to make these transactions, they would have needed to know not just the replacement debit card details but also the OTP codes.

Based on Ms L's submissions, the only mobile number that the bank holds on record – which is the same number the OTPs would have been sent to – still belongs to Ms L. That means, even if the SIM card became inactive – as has been argued – the phone number wasn't recycled and assigned to another user due to prolonged inactivity. So, it's unlikely a third party could have received the OTPs when they were sent. As Ms L hasn't claimed someone else had access to her phone/SIM during this time, I can't see how the OTP information NatWest sent could have been compromised.

I recognise that Ms L feels very strongly about my findings about the bank sending OTPs to her phone number. But when I gave her the opportunity (and I know the investigator gave her an opportunity as well) to contact her mobile provider and forward any evidence to support her claim that her SIM/phone number wasn't active at the time the OTPs were sent, Ms L refused to do this.

As I've mentioned, I did go back to NatWest and requested more specific evidence that shows the 3DS process was completed using an OTP. NatWest's submission doesn't explicitly show that it sent an OTP to Ms L's registered number at the relevant times. But it has shown that 3DS authentication could not have been completed through the mobile banking app. And so, through the process of elimination, it asserts that an OTP was sent in the circumstances of this case.

Having weighed up the evidence before me, I'm more persuaded that the 3DS authentication was completed using OTPs which were sent to Ms L's mobile number. Given there's no suggestion that her phone was compromised during that time, I find it unlikely that the transactions could have been completed without Ms L's involvement.

Additionally, I note that the online log-in audit data also shows a successful log-in in March 2022 using Ms L's security credentials. The IP address for the log in can be traced back to the country Ms L lives in. Again, there's been no suggestion that Ms L's login details were compromised at some point. That suggests that it was Ms L who logged in on the day in question. By that point, over 20 transactions which are now being disputed had been made. I consider the activity on the account and the amounts debited ought to have raised concerns if the transactions were made without Ms L's knowledge or consent. But I can't see the matter was reported to NatWest at that time. Instead, subsequent transactions being disputed continued to be made for a few more months.

I put this finding to Ms L recently, and she said she wasn't interested in talking about when she last logged into her account. And that this wasn't the matter she had complained about. But as I explained to Ms L, it is an important consideration for me as the deciding ombudsman. The crux of her complaint is that NatWest is holding her liable for several transactions from her account which she says she didn't make or consent to being made. Where a customer doesn't recognise transactions and alleges that they were not authorised, reviewing the log-in and transaction authentication data (amongst other things) is crucial to the investigation to understand if a third party could have gained access which might explain how the transactions were made.

In conclusion, I know Ms L will be extremely disappointed with this outcome. But based on what I've found above, I can't fairly conclude that NatWest should reimburse the disputed transactions.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or reject my decision before 4 June 2024.

Gagandeep Singh
Ombudsman