DRN-5385890

The complaint

Mr W complains that National Westminster Bank PLC's (NatWest) facial recognition on his banking app worked during a robbery when he was held at knifepoint and his eyes were closed, allowing his attacker to gain access to his accounts.

What happened

Mr W reported an attack when he was beaten, making his eyes swollen and bloodshot, with facial bleeding, and said he was held with a knife to his throat. Mr W said his attacker wanted access to his mobile banking app, and throughout the incident held Mr W's phone in front of his face attempting to activate the facial recognition biometrics.

Mr W thought the facial recognition wouldn't work as his eyes were closed and his face was unrecognisable through the assault. However, the assailant eventually gained access to the mobile banking app via facial recognition. He stole Mr W's phone, made a cash withdrawal, paid for a taxi and set up a transfer for £3,000.

Mr W informed NatWest of the incident and to suspend his accounts. He said an agent told him his mobile phone had been blocked which delayed him reporting the theft to his mobile phone provider, but this proved not to be the case. NatWest returned the stolen money to Mr W but he said an agent was extremely rude to him and made him feel like a scammer.

Mr W complained as he wanted to understand how the facial recognition had worked, how many attempts had been made and why it wasn't disabled after so many attempts. He didn't understand how the attacker was able to withdraw cash from an ATM in the early hours of the morning, when he had never made a withdrawal himself with that card.

NatWest responded to say that it hadn't made an error. It said it only takes a split second for eyes to be open to allow facial recognition. NatWest said that during a call its agent told Mr W it would disable the banking app. It didn't say it would block a mobile phone as this was beyond account activity. It sent Mr W a copy of the call recording. NatWest apologised for a member of staff that Mr W had complained about and paid him £100 compensation.

Mr W wasn't satisfied with NatWest's response and referred his complaint to our service.

Our investigator explained how the biometrics system works and said NatWest told us there were 14 facial recognition attempts to access Mr W's banking app at the time of the assault. She said the biometrics system won't allow access after five failed attempts and facial recognition is disabled until the biometrics are removed and re-added. But the system still records the additional attempts to access the banking app. She said the banking app doesn't delete the biometric after five failed attempts, as the biometrics are stored in a secure server.

The investigator said NatWest wasn't at fault that the facial recognition allowed access to Mr W's accounts and had quickly refunded him. She said NatWest's response to Mr W was about resetting his biometrics, which was a misunderstanding of his questions. She said NatWest should have responded to Mr W's requests by explaining how account access had been possible using the biometric and should pay him further compensation of £100.

The investigator said NatWest wouldn't provide the image that accessed the banking app allowing the biometric to be reset, as it would breach data protection, but Mr W may be able to access this directly from NatWest. She said the assailant withdrew cash from an ATM using the correct PIN and Mr W's card and would have looked like a genuine transaction.

Mr W disagreed with the investigator and requested an ombudsman review his complaint. He agreed that five failed attempts locked customers out of the app, but he questioned the meaning of code references to failed attempts and NatWest's policy when 13 attempts are invalid. Mr W felt there's a failing within the app and asked if this is in line the regulations. He said the access of his account needs to be looked at, so it doesn't happen to anyone else.

Mr W said a successful attempt at biometric validation was not him as his phone had been stolen, and was out of his presence and must be evidence of a failing in the biometric. Mr W said it took almost two weeks for the biometrics to be re-added which he thought was due to his assailant having put his biometrics on his account, and that's why he couldn't register.

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.

Mr W has also complained about NatWest's response to his subject access request and its security around passcodes, and these issues are being considered separately.

I was very sorry to learn about the appalling attack on Mr W and the consequences of the robbery for his banking. I can see that he has raised questions to NatWest about the operation of its facial recognition on his banking app. My role is to determine whether NatWest's response to the impact on Mr W and his accounts was reasonable and whether it has followed the process correctly.

I've taken into account the relevant rules and guidelines along with good industry practice. There are general principles that say a bank should conduct its business with due skill, care and diligence and pay regard to the interests of its customers.

Mr W said NatWest's biometrics failed as it didn't block his account and allowed his attacker to add his face. Mr W wanted to know how the facial recognition worked while he was being assaulted and NatWest's security codes for account interactions. Our investigator has explained this in some detail which I won't repeat here.

Mr W is concerned about the number of failed attempts followed by three successful logins after his phone was stolen. NatWest has explained that the biometrics system will not allow access to the banking app after five failed attempts. When this happens, facial recognition is disabled until the biometrics are removed and re-added, but the system still records the additional attempts. The banking app won't then delete the biometric as this is stored in a secure server which is then used to match future authentication attempts.

NatWest explained that to reset biometric access, a successful authentication is required. NatWest has recorded a failed attempt to remove the biometric during the assault followed by a successful attempt and then re-adding. This allowed access to the banking app, as the face matched the image stored within NatWest's secure server. There are no security alerts if the facial recognition fails after five attempts, the user is blocked until the biometrics are removed and reset. As it was Mr W's image that was used to remove and re-add the biometric, and this image matched the image held on NatWest's server, access was granted.

After the first five failed attempts at facial recognition when Mr W was under assault there were nine further attempts recorded by NatWest. There was no access from these attempts as the system had blocked this, as it should, until the biometric had been reset. From what I have seen NatWest's biometric system worked as intended.

Mr W also complained that his assailant was able to withdraw cash from an ATM at a time of night inconsistent with Mr W's usual pattern of withdrawals, and he was given misleading information in a call when he was told that his mobile device had been blocked by the bank. When the assailant withdrew cash from an ATM in the early hours of the morning of the assault, he used the correct PIN and Mr W's card. I can understand why the withdrawals were allowed as there was no reason to believe they weren't genuine transactions.

NatWest said its systems picked up on the unusual activity of the £3,000 transaction, but although this was flagged the instruction was carried out. Ideally this would have been blocked but at that stage NatWest was unaware of the incident. I'm pleased that NatWest quickly refunded Mr W all fraudulent transactions, so he hasn't lost out financially.

From what we know of NatWest's security systems it appears that Mr W's attacker accessed Mr W's mobile banking app having guessed his passcode. The attacker probably added his biometric to Mr W's mobile banking app having deactivated Mr W's. This wasn't NatWest's responsibility or a fault of the system. The biometric system has to facilitate customers who wish to make amendments and NatWest's policy doesn't require it to call a customer for this reason or after failed attempts to log in.

When a biometric image is deleted, it's copied to NatWest's archive database where it's stored and then permanently deleted after six months, so unfortunately it no longer exists. NatWest are unable to retrieve an archived image to view it, but even if they could, it no longer exists due to the time frame. As I have said above, I don't think what happened to Mr W was as a consequence of the failure of NatWest's security systems. I haven't found any regulatory issue with the operation of NatWest's biometric system and I'm not aware of any similar complaint on this issue to our service.

Mr W said he had difficulty logging into his mobile banking app using his facial biometrics after the attack. NatWest has shown mobile banking payments on his account since then. Mr W spoke to NatWest about this at the time, but this wasn't part of his original complaint, and we haven't seen a response from NatWest about the issues Mr W has since raised around this and so it is not something we can investigate at this stage.

During Mr W's first call to NatWest after the robbery NatWest's agent told him, '*Your mobile device has been locked as well, so they won't be able to access the online banking on there*'. The next day an agent said, *'I've marked your mobile phone down as stolen, that will lock the device and they can no longer get into your online banking*.' The agent reiterated this, '*I've locked the device and marked it as stolen so they can't log in with that anymore.*'

In the next call, with NatWest Mr W was told '*your phone's completely locked down now, so that should help with that side as well*.' Clearly, it's beyond a bank's power to lock a customer's phone, but it's understandable that Mr W understood this differently at the time, particularly as agents said his phone has been locked. I agree with the investigator that the information was a little misleading and this led to a delay in Mr W reporting theft of his phone to his provider and allowing money to be stolen from another of his bank accounts.

NatWest apologised to Mr W and paid him £100 compensation in relation to poor customer service he received in a call, which was unrelated to the calls mentioned above regarding his mobile phone being blocked. I agree with the investigator that NatWest should have provided Mr W with an explanation and reassurance that the biometrics system had worked

correctly. He also received misleading information about his phone being blocked and this caused a delay in reporting the phone as stolen. I think a total sum of £200 to be a fair and reasonable sum and request that NatWest pay Mr W an additional £100.

Putting things right

I can well understand that Mr W has been deeply upset by the assault and robbery he suffered. I agree that he has been caused frustration and inconvenience by NatWest's service and that compensation of £200 is a fair and reasonable reflection that he didn't receive the customer service we would expect following such a traumatic incident. This compensation falls within our guideline for poor service resulting in some acute stress for a short period, with some inconvenience caused requiring a reasonable effort to sort out.

Our service investigates the merits of complaints on an individual basis, and that is what I've done here. I think it's important to explain that my decision is final. I realise that Mr W will be disappointed by this outcome and his unanswered questions though I hope he appreciates the reasons why it had to be this way.

My final decision

For the reasons I have given it is my final decision that the complaint is upheld. I require National Westminster Bank PLC to pay Mr W further compensation of £100 (totalling £200) for the distress and inconvenience he has been caused.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 23 April 2025.

Andrew Fraser
Ombudsman