DRN-4823373

The complaint

Mr W complains National Westminster Bank Plc (NatWest) are refusing to refund him a series of unauthorised transfers and payments.

What happened

Mr W contacted NatWest to report a series of unauthorised transfers in early January 2024. These transactions were from his NatWest account and totalled over £3,000.

Mr W also reported a series of unauthorised card payments totalling over £600 in early February 2024. Both parties to this complaint are aware of the disputed transactions so I will not repeat them in detail here.

Mr W explained he had been unwell and in hospital from late 2023. He also explained he had not had access to his most recent mobile phone device with his NatWest app on it, an iPhone 8, during this time but it was secure in the hospital. He confirmed his debit card had remained in the possession of a trusted family member. Mr W said he thought the disputed transactions had been completed by two associates of his.

During calls to our service, Mr W explained the transfers had possibly occurred on his old mobile device, an iPhone 7. He explained he thought he had misplaced this phone in his home and hadn't realised it had been stolen. He said one of the associates knew the passcode to this phone explaining it had his banking details stored in the *'notes'* section of it. He also explained once you had access to this phone with the passcode, you could change the fingerprint biometrics and this would allow access to his banking app. He said one of the named associates had used this mobile phone for his own internet banking in the past.

Mr W explained one of these associates also knew the code to the key-safe outside of his home so could have gained access whilst he was in hospital that way. He described these individuals as colleagues who he had loaned money to in the past.

NatWest did not uphold Mr W's complaints. It said the payments were made using a mobile device registered for internet banking. It explained Touch ID had been used to login and the transfers were to existing payees who Mr W knew. NatWest also explained the transactions did not score high enough to trigger any restrictions or to stop the payments.

After speaking with Mr W, NatWest wrote a second response letter. NatWest said it thought Mr W wasn't keeping his account safe and secure, explaining he had delayed reporting some of the transactions as fraudulent for a significant period. It also explained one of the merchants had provided information to NatWest which matched the personal information NatWest held about him. NatWest explained the bank transfers had gone to existing payees who Mr W had set up and sent money to many times before.

Our investigator didn't think NatWest needed to refund the disputed transactions. They explained they couldn't see how someone else could have accessed his registered mobile device to make these transactions. They also explained the evidence suggested recipients of the transfers, the two associates, were known to Mr W and he had made numerous previous transfers to these payees, including over 100 previous payments to one of them.

With regards to the disputed card payments, our investigator explained the correct card details were recorded to make the payments via Apple Pay, with one transaction using full card details and the three digit security code printed on the debit card.

Our investigator explained the last time the card details were viewed in the banking app was in September 2023, so did not think there was a clear explanation of how a fraudster could have used access to online banking to get the details to make these payments as Mr W had explained the card was kept safe at the time the transactions occurred.

Mr W responded to our investigator's recommendation explaining the associates could have seen a letter left on the floor of his flat showing when loan payments were due into his account.

As Mr W rejected our investigators recommendation, his complaint has been passed to me to make a final decision.

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.

Where evidence is incomplete, inconclusive or contradictory, I have to make decisions on the balance of probabilities – that is, what I consider is more likely than not to have happened in light of the available evidence and the wider surrounding circumstances.

I appreciate how strongly Mr W feels about his complaint and I was very sorry to hear about the ill health he recently suffered. Although I may not mention every point raised, I have considered everything but limited my findings to the areas which impact the outcome of the case. No discourtesy is intended by this, it just reflects the informal nature of our service.

The relevant regulations here are the Payment Services Regulations 2017 (PSRs). In general terms, the bank is liable if the customer didn't authorise the payments and the customer is liable if they did authorise them. So, the issue for me to determine was whether it was more likely than not Mr W carried out the transactions himself. If he authorised someone else to carry out the transactions for him, this would also be considered as carrying out the transactions himself.

The transactions fit into three categories, firstly there are what appear to be regular subscription payments made to an online service provider, secondly there are several transfers, all made on the same day to two existing payees for over £3,000. Finally, there are several payments over a short period of time to a takeaway service and two hotels.

<u>Subscription transactions</u>

The first four transactions Mr W complains about are to the same online content provider. They appear to be a subscription as they are for the same amount of money taken at the beginning of each month in October, November, December 2023 and January and February 2024.

NatWest have provided our service with details from the merchant for these transactions. This evidence shows the purchases were made by entering the correct details for Mr W's debit card online. The name, address and email from the merchant all match the contact details Mr W has provided our service with. It also shows the first payment was agreed to on 1 August 2023, several months before Mr W complained about them.

Mr W would have received notifications for a significant period of time before he reported these transactions as unauthorised. I also note Mr W withdrew this complaint with NatWest on one occasion stating he had recollected what these transactions were for.

I therefore think, on balance, as the details held are correct and show Mr W's details, there was a delay in reporting the transactions, and the inconsistency of Mr W's view of whether the transactions were disputed, it is more likely than not Mr W authorised this payment.

For these reasons, I am not persuaded these transactions were unauthorised and NatWest does not need to refund these payments.

Bank transfers to Mr W's associates

Turning now to the disputed transfers, I have carefully considered the data NatWest has provided our service regarding logins to Mr W's banking app throughout the period in question.

As Mr W has suggested, the evidence supports there were indeed two mobile devices active over this period. I will refer to the two phones used as phone 1 (which I believe, on balance is consistent the 'lost' iPhone 7 Mr W described) and phone 2 (which I believe on balance is likely to be the iPhone 8 Mr W says was retained in his possession in hospital).

Phone 1 was registered on Mr W's NatWest banking app on 28 June 2023, phone 2 was registered on 25 September 2023.

The data shows both phones were actively used to maintain Mr W's NatWest accounts through online banking until 6 November 2023. This was the last time phone 1 was used until just before the disputed transfers were made.

From 6 November 2023 onwards, phone 2 was exclusively used for mobile banking, with regular logins from this device. Phone 1 then logs in again for the first time since 6 November, on 22 December 2023.

At the same time, phone 2 appears to stop logging into the account. Between 22 December and 2 January, the only phone to log into the account is phone 1. It regularly logs in during this period, until 2 January where phone 1 is then used to make the disputed transfers. It then ceases to log in again during the data set I have seen.

On 9 February phone 2 is used to login. This is the first time phone 2 has logged in since 20 December 2023.

Mr W has told us he misplaced or lost one of his phones, the iPhone 7, in November 2023. This appears to be his older phone and is consistent with the lack of usage of phone 1 after this date. Mr W said he thought he may have lost it in his home and it didn't have SIM card in it, which corroborates why he didn't report it to a network provider.

Mr W says he went into hospital on 6 December and has said he had limited access to his newer phone 2 during this period. Although this does not strictly concur with the usage we can see, it does not appear that any disputed transactions occurred from any logins this phone made whilst he was in hospital.

Mr W said he was still in hospital when phone 1 reactivated on the account in late December 2023. When it first logged into his account there was only just over £100 in Mr W's main account. Phone 1 then logged in regularly, without making any transaction until Mr W received a maintenance loan payment in of over £4,000 on 2 January, in the early hours of 2 January, soon after these funds had been credited, this money was transferred out by phone 1 over four separate transactions apparently to the associates he has named, leaving just over £700 in the account.

Mr W explained in response to our investigator's view, as his associated had access to his home whilst he was in hospital, they could have seen correspondence which would have indicated he was due the maintenance loan payment. This would accord with this phone regularly checking the account and making these withdrawals in the early hours of the morning after the payment had been credited.

I carefully considered all of this evidence and what Mr W has said about his associate's ability to access both his home address and potentially find his iPhone 7 and the circumstances surrounding the loss of this phone.

I have also considered the comments Mr W made about this associate using his phone for their own mobile banking and having placed his banking details in the unprotected *'notes'* app on this mobile phone.

I presented the above evidence to NatWest to ask whether this evidence changed its positions regarding the transactions and for any further evidence or comments it wished to make.

In response, NatWest said Mr W had continued to make payments to one of the associates he was claiming had taken the funds from him. NatWest provided evidence of at least a further 10 transactions made by Mr W to this individual using the same account details, in autumn 2024.

NatWest also considered the circumstances Mr W explained about how he may have lost the iPhone 7 and how he had given the associates access to both his banking app and home address.

NatWest said it would decline Mr W's claim under its terms and conditions. It specifically pointed out section 5.1 which state customers should take all reasonable steps to keep security details safe and keep debit cards and mobile devices secure at all times and not to let let anyone use them to make payments.

NatWest also explained it had reviewed the technical data related to the 'image' used for its Biometric authentication for the app. It said the current image had been registered on 19 May 2023 and had not been changed since.

Because NatWest suggested Mr W had not complied with its terms and conditions, I must now consider this case in line with intent and gross negligence principles under Regulations 72 and 77 of the PSRs. These state customers must use payment instruments in accordance with the terms and conditions, notify the bank without undue delay if a payment instrument is lost or stolen, and take all reasonable steps to keep personalised security credentials relating to payment instruments safe.

Gross negligence is a high bar. There is no singular definition of gross negligence within civil law and it is often for the Courts to decide the threshold and whether the acts or omissions has breached that determined threshold.

For the purposes of this decision, I am satisfied gross negligence can be defined as:

- An act or omission to exercise reasonable care in performing or failing to perform an obligation where such party demonstrates indifference to, or a serious disregard for a reasonably foreseeable risk.

In other words, doing or failing to do something which they reasonably ought to, to avoid something happening that had a reasonable chance of occurring.

Mr W has told us he apparently had to go into hospital at short notice for an extended period. The evidence he had presented shows this was sadly not a choice he made and it seemingly happened at short notice, but it presented an opportunity to the associates to gain access to his property and apparently find the lost phone, which they knew how to access and use.

If we accept Mr W's testimony, he has confirmed he allowed access to his phone by the associates he identified as making the transfers. He also allowed access to his home by providing associates with potentially unrestricted access to a key-safe and he has said he stored his banking details on his phone unrestricted.

I accept the evidence Mr W has provided could account for how these third parties were able to access his banking app and make the transfers.

In circumstances such as this I need to consider whether there was an obvious risk which a reasonable person would have considered and should have mitigated against. In the circumstances described, I think on balance, there is some evidence to suggest gross negligence.

Losing a phone with banking details stored on it, whilst knowing third parties could access his home and his device, appears to be risk a reasonable person would have realised and taken action to mitigate. I do appreciate the circumstances Mr W has described, but the test I must apply is what we would expect from a reasonable person.

For these reasons, I think there is, on balance, evidence of gross negligence. Mr W allowed access to secure banking details, did not report a lost, registered device and allowing third parties access to it when it was out of his control.

If we accept Mr W's evidence, it suggests for each of the transactions a detailed knowledge and access was required to Mr W's online banking. This could only have occurred had Mr W provided security information he should not have to a third party, which he accepts.

I am minded that Mr W has explained he knows the individuals who have benefited from the transfers. Furthermore, it is clear Mr W has made many transactions previously to both parties which have not been disputed.

An important development is Mr W has continued to make payments to one of these associates after the disputes were raised. On balance, despite the evidence Mr W has provided regarding the loss of his phone, I also do not think this activity is consistent with the claims he has made.

For these reasons, I do not think, on balance, it would not be fair or reasonable to expect NatWest to refund these transactions. I am persuaded by both arguments, that for the reasons I have given, Mr W was grossly negligent and that continuing to authorise payments to one of the beneficiaries after raising a disputed transaction, is inconsistent with the fraud claimed.

Debit card and Apple Pay transactions

Now moving to the disputed debit card and Apple Pay transactions. These all occurred on the same day in early February 2024. There are several transactions to an online takeaway provider, a small transaction to a scooter hire service and two transactions to hotels.

NatWest had blocked Mr W's account after he had reported the previous disputed transfer transactions. Mr W also asked NatWest not to block his debit card as he needed to use it to make payments whilst in hospital.

These transactions are again subject to the PSRs and I therefore need to consider evidence in line with what I have described above.

The evidence suggests one of the payments to one of the hotels was made using the full card details including the CVV, this is the three digit code printed on the back of the card. Mr W has said this card was retained in the secure possession of a relative whilst he was in hospital. He also explained he had a copy of the card written down with him in hospital, so he could make online purchases for his everyday needs. The options for these card payments are:

1. he provided the full card details to a third party, including the CVV, who made these transactions,
2. he made the transactions himself,
3. someone obtained his card details in some other way,
4. someone used his online banking details to obtain his debit card details.

Dealing with the last option first, I understand from the evidence, there is a function within the NatWest app for customers to view both their card number and CVV. NatWest has provided an audit of this facility explaining the last time these details were viewed was on 23 September 2023.

Bearing in mind the above, that Mr W claims a third party had access to his NatWest app, I have considered carefully whether I think this is where the compromise could have occurred. Having done so, I am persuaded this is unlikely on balance, as someone would have had to obtain these details, recorded them, then wait four months to make a series of purchases.

I am also mindful the evidence shows Mr W still had both phones in his possession until November, and if we accept the associates had unfettered access to his banking app and used this method to obtain the details, it seems unlikely they would not have looked at these details to check in the period.

I am also satisfied this is not in line with fraud our service often sees and would be unusual for a fraudster to wait this length of time to use such details.

Dealing with points one and two, Mr W has said the card remained secure whilst he was in hospital with a trusted relative, but explained he had a copy of the card details with him.

It may also be the case a third party obtained the details via another unknown method. Mr W provided evidence of unrestricted access to his address, has explained he provided this card to a third party and had written his card details down at least once, for use in hospital.

In line with the issues above, I am persuaded this again demonstrates Mr W was not complying with the terms and conditions NatWest set, specifically here for the use of his debit card.

I appreciate there is possibly a good reason for the card being placed in the care of a trusted third party in the circumstances.

There is a lack of evidence to base my decision on here, but looking at the broader picture and circumstances, including the evidence above, I think on balance it is likely Mr W has again been grossly negligent in providing these details to a third party. I therefore do not think NatWest need to refund these transactions.

Finally, I have considered the Apple Pay payments made to the takeaway, hotel and scooter service providers on the same day. The evidence suggests these payments were made by using Apple pay on a registered device. Due to this NatWest has explained it is limited in the detail it has about the device or devices used for these transactions.

NatWest's records show it advised Mr W when he contacted it to block his account after the transfers, if he wanted to remove Apple Pay from a device he would need to contact Apple, as this service was outside of NatWest's control where the associated debit card remained live. Mr W has not provided any evidence he did contact Apple, suggesting he thought NatWest had been able to block his account on Apple Pay.

Having considered the advice NatWest provided, which was correct, I do not think it did anything wrong here. There had not been any disputed purchased via Apple Pay at that time, the disputed transactions had been transfers and Mr W was reasonably requested his card remain active.

I do not think NatWest did anything wrong by placing a block on the account but allowing the debit card to remain active, especially as Mr W s explained he would have not been able to get a new debit card from his home address.

Furthermore, Mr W has regularly made undisputed payments to the same takeaway service soon afterwards and there have since been further, undisputed transactions to the scooter service.

For these reasons, and for the reasons I have already provided in relation to the other disputed transactions above, I do not think, on balance, these transactions were unauthorised.

I appreciate Mr W will be disappointed with my decision, but I trust I have fully explained it.

My final decision

For the reasons I have given, I do not uphold Mr W's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 5 December 2024.

Gareth Jones
Ombudsman