DRN-4619810

The complaint

Ms N is unhappy that Revolut Ltd ("Revolut") won't refund payments she says she didn't make.

What happened

Ms N explains that on 23 June 2023, she received contact from someone claiming to be from Barclays, who she banked with, saying a standing order had been set up on her account. She called the number she was provided and got through to someone who she believed worked for Barclays. The person she spoke to knew her account and sort code, her name and address, and said they would assist her in protecting her from fraud. She was told to open an account with Revolut and move her funds into that account to keep her money in a safe place. She was led to believe that Revolut was part of Barclays.

Ms N said throughout her conversation with this person, they prompted her at points to either share information or take steps to keep her account safe. She recalls being asked to provide a one-time passcode ("OTP") that she was told she would receive, but as there was a lot going on with her personally at the time this happened, she said she didn't read the message within the OTP, rather shared the code as prompted. At the time she was speaking to this person, she was teaching, fasting and was going to prayers.

After transferring money from her Barclays account to her Revolut account, she was told to delete the Revolut banking app to keep her funds safe, so it could keep track of any attempted fraud. She could then access it again the next morning. After the initial call ended, the person she was speaking to called her back saying they needed her to download the app again to make sure the account was safe. On that occasion she noticed a payment for just over £300 had been attempted from the account that she questioned this person about. She said she was told they were testing the security of the account and gave assurances her money would be safe. She was also told that her card came blocked and that she needed to unblock it. She then deleted the app again as instructed.

Ms N noticed direct debits didn't leave her account as expected the next day from her Barclays account. She then came to realise she'd been scammed after speaking to someone genuinely from Barclays about what happened, and also after seeing that payments had debited her Revolut account using Apple Pay totalling £804.83. I've set out the disputed activity below:

Date (2023)	Time	What happened	Amount
23 June	6:28pm	Declined payment to Boots	£311.49
23 June	6:55pm	Successful payment to Boots	£449.60
23 June	7:03pm	Successful payment to Tesco	£200

23 June	7:08pm	Successful payment to Tesco	£100
23 June	7:22pm	Successful payment to Nisa Local	£45.49
23 June	7:25pm	Declined payment to Nisa Local due to insufficient funds	£17.50
24 June	11:20am	Successful payment to Westfields	£3
24 June	8:33pm	Successful payment to Westfields	£3
24 June	8:47pm	Declined payment to Sv Retail Ltd due to insufficient funds	£43.73
24 June	8:47pm	Successful payment to Sv Retail Ltd	£3.74

Revolut declined to refund Ms N. It said because the payments were authenticated in person through Apple Pay, there wasn't a valid chargeback claim.

Unhappy with Revolut's decision to decline a refund, Ms N referred her complaint to our service. One of our investigators looked into her complaint and upheld it. In summary they said that as the payments were unauthorised, and Ms N hadn't failed with intent or gross negligence, Revolut was liable to refund her loss in full.

Revolut didn't agree. It initially provided a comprehensive response, however I've summarised below what I understand to be its outstanding points:

- The first attempted transaction was identified as high risk. Ms N confirmed the transaction as genuine which then allowed further payments to debit the account.
- Ms N was grossly negligent by confirming the first attempted transaction as genuine.
- The payments couldn't have been made without Ms N's consent or negligence.

As Revolut didn't agree, the matter has been passed 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 have reached the same conclusion as the investigator for similar reasons.

The starting position in line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, is that Ms N is liable for payments she's authorised, and Revolut is liable for unauthorised payments.

For these payments to have been authorised, the PSRs explain that Ms N must give her consent to the execution of the payment transactions and that consent must be given in the form, and in accordance with the procedure, agreed between her and Revolut.

To establish the agreed form and procedure, I've reviewed the terms and conditions that Revolut has referred us to. However, these don't set out in detail how Ms N consents to

make payments using Apple Pay, which is how the payments were made here. The technical data Revolut has provided us shows these payments were 'present' meaning they were carried out in person. So I've thought about what practical steps were needed to have made these payments.

It appears accepted that it wasn't Ms N's device that was used to make the payments as she has an Android phone (which does not support Apple Pay). Meaning Apple Pay was set-up on the fraudster's device, with Ms N's card details, to then make these payments.

From what Revolut has told us about how the Apple Pay was set up, it does appear Ms N would have either needed to have taken steps in her app or share secure information. She says the caller already had secure information about her and that's part of why she believed it was her bank that she was dealing with. She can't remember the specifics, but I'm satisfied she was coached heavily as part of the scam and didn't realise at the time she was sharing anything sensitive or putting her account at risk.

I've considered Revolut's comments that the payments couldn't have been made without Ms N's consent, referring to the set-up of Apple Pay. But I'm mindful here that when Ms N shared the OTP, which was needed to complete the set-up of Apple Pay, she didn't read the message in full and so didn't appreciate what the OTP would be used for. And she's been consistent in saying that she was following the steps given by the fraudster in keeping her money safe within the Revolut account. It doesn't seem to me that she had an understanding that money would leave her account or that she was enabling someone else to make payments.

Taking all the above into account, and the PSRs, I consider these disputed payments to be unauthorised.

The PSRs set out that Revolut can hold Ms N liable for unauthorised payments if she failed in her obligations with intent or gross negligence, which is what Revolut asserts. Of most relevance here is the obligation to take all reasonable steps to keep safe personalised security credentials and to use the payment instrument in accordance with the account terms and conditions.

When I'm considering if Ms N has failed in her obligations with gross negligence, I need to consider that the test isn't simply whether someone was careless. For someone to fail with gross negligence they would need to have seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person. So I've considered whether Revolut has been fair in determining this by assessing the circumstances of the scam and Ms N's actions.

Ms N received contact from someone claiming to be her bank Barclays. The fraudster she spoke to knew her personal information such as her name, address, and account details. She was told there were attempts to set-up payments from her account and that a new account needed to be created with Revolut so she could move her funds into a safe account. With this level of information, I'm persuaded why she believed she was speaking to her bank and why she trusted that her account with Barclays wasn't safe, so she needed to then follow the instructions to keep her money safe. Where Ms N was tricked into believing that Barclays and Revolut were in some way linked, I don't consider that unreasonable given she didn't appear to have much knowledge about how Revolut operated. I think a lot of people would have been persuaded like Ms N was here.

Revolut argues Ms N shared the OTP which contained a warning saying it ought not be shared. But as I mentioned earlier on, Ms N explained she didn't see the content of the message and only shared the code. She also explained that the fraudster pre-empted her

that she was going to receive a message, which she appeared to soon after.

In doing so, Ms N was tricked into sharing details with the fraudster which they used to make these payments. But I consider she took this action without understanding she was breaching the account terms, or failing to keep her personalised details safe. Instead she thought the actions she was taking was to safeguard the funds in her Revolut account.

In the circumstances, where Ms N trusted the caller and the message came through from Revolut as expected, I'm persuaded why she focused on the code she was told to share, and not on the warning. Particularly given she was tricked into believing she was acting to safeguard her money, under a false sense of panic. I think it's likely a lot of people would have done this in a similar situation, having been told they were at risk of losing their money.

Revolut also argues Ms N was aware a payment had been attempted and declined, yet took steps to unblock her card that otherwise confirmed the payment as genuine. Ms N explained she asked about what appeared to be an attempted payment with the fraudster at the time who told her they were making sure her account was secure and that this would be returned to her. She was also told that her card came blocked so she needed to unblock this so they can ensure the account was kept safe.

While Ms N may have been careless in unblocking her card, that isn't the relevant test here. The fraudster used social engineering to create a sense of panic that her money was at risk, and that she needed to act to protect it. Given her explanation as to why she followed the fraudster's instructions, I don't consider she fell so far below what a reasonable person would have done that her actions amount to gross negligence.

Ms N explained that after downloading the Revolut app a second time, she deleted it again on the fraudster's instruction. This appears to be consistent with the banking reports Revolut has provided us where the account wasn't accessed until the following morning. It appears she was still in her app for around a minute after the first successful payment, but it doesn't appear Ms N saw this. So I don't believe she was aware that money had started to successfully leave her account, and therefore hadn't identified any obvious risk to her account.

Taking everything into account, I'm not persuaded Revolut has shown Ms N failed in her obligations with intent or gross negligence. So in line with the PSRs, it needs to put things right by refunding her losses alongside interest to compensate her for the time she's been without her money.

As a final point, I've noted Revolut has also raised several arguments in its initial response that I consider to be relevant to authorised payment scams. As I've concluded these payments are unauthorised, I don't think it's relevant to address these.

My final decision

For the reasons I've explained, I uphold Ms N's complaint. Revolut Ltd must:

- Pay Ms N the total of the unauthorised payments, less any amount recovered or refunded.

- Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms N to accept or reject my decision before 19 July 2024.

Timothy Doe
Ombudsman