DRN-5665335

The complaint

Mr S complains that Ulster Bank Ltd won't refund a transaction he didn't make or otherwise authorise.

Mr S is being represented by Miss D in bringing this complaint. For ease of reading, my reference to Mr S in this decision includes his and Miss D's submissions.

What happened

Mr S unfortunately fell victim to an impersonation scam. He received a call purportedly from Ulster Bank's fraud team about suspicious activity on his account. Under the belief that the individual was assisting him in securing his account, Mr S followed the caller's instructions and installed a remote access software on his phone. At the time of reporting the scam to the genuine fraud team at the bank, Mr S said the scammer also made him download an app for, and create an account in his name with, an online money remittance firm, "R". He also confirmed he transferred funds between his savings and current accounts with Ulster Bank while on the phone with the scammer.

Ulster Bank said there were two transfers attempted to R – £3,490 and £4,951.99 – through the Open Banking payment system. Both transactions were initially held, and the bank sent a text message to Mr S's registered mobile number to check it was indeed him making the payment. The first transfer was processed after the bank received a response from Mr S's registered number that the transaction was genuine. The second transfer, attempted around 40 minutes later, was ultimately rejected after Mr S notified the bank that he'd fallen victim to a scam. Ulster Bank declined to refund the successful transfer (£3,490) and asked Mr S to contact R to recover his funds.

Unhappy with this response, Mr S made a complaint to Ulster Bank before referring it to our Service. Our investigator concluded that as Mr S granted remote access to the scammer and understood that funds would leave his account (albeit temporarily), it was fair for Ulster Bank to treat the disputed transaction as authorised. The investigator also thought it wasn't unreasonable for the bank to have processed the transaction. And it acted fairly in attempting recovery once being made aware of the situation, but there were no funds left to be recovered.

Mr S disagreed with the investigator's findings and asked for an ombudsman to review the 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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

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

I'm sorry to hear of the circumstances that have led to this complaint. It's very unfortunate that Mr S has lost money in this way. But Ulster Bank doesn't automatically become liable to reimburse him.

As Mr S says the disputed payment is unauthorised, the relevant law here is the Payment Services Regulations 2017 (PSRs). The starting point is that Mr S would generally be liable for an authorised payment, and, with some exceptions, Ulster Bank would generally be liable for an unauthorised payment.

Is it fair for Ulster Bank to treat the disputed transaction as authorised?

From the technical evidence that Ulster Bank has provided, the transaction was correctly authenticated in Mr S's banking app. The log-in data shows Mr S logged on to the app from his registered device.

But authentication alone isn't enough to consider a payment authorised. To consider a payment authorised, the PSRs explain that Mr S must have given his consent to the execution of the payment transaction – and that consent must be in the form, and in accordance with the procedure, agreed between him and Ulster Bank.

In other words, consent happens when Mr S completes the steps agreed for making a payment. It's also possible for someone else to act on Mr S's behalf and complete some or all of the steps involved. And for the purposes of whether a payment is authorised, it doesn't matter if Mr S was deceived about the purpose or amount of the payment.

Ulster Bank hasn't provided us with the applicable terms and conditions from when the disputed transaction happened to determine the agreed form and procedure. So, I've considered the practical steps that needed to happen for the transaction in question.

The transaction was made using the Open Banking payment system. In simple terms, it was initiated on R's platform and completed once it was approved on Ulster Bank's platform. In other words, Mr S would have then been required to log on to his Ulster Bank app to approve the transaction before it was processed.

Mr S says it was the scammer who made the disputed transaction from his account after he allowed remote access to his device. However, in its submission, Ulster Bank has shown that its system didn't detect any remote access when the disputed transaction was authenticated in Mr S's banking app. The bank says its systems would be able to tell if remote access software was in use at the time.

This suggests it's unlikely that remote access was in use when the transaction was authenticated in Mr S's banking app. That said, I acknowledge that remote access may have been in use during part of the payment journey, i.e. when the transaction was initiated on R's platform.

I note Mr S told Ulster Bank it was him who transferred the money from his savings to his current account, which was then used to attempt a further unsuccessful transaction. So, although he doesn't recall doing so, it's possible that Mr S also approved the disputed transaction in his banking app. I acknowledge that he might not have fully understood what was happening at the time. But that's not a consideration under the PSRs in whether the transaction was authorised.

Even if I were to accept that remote access was used during the entire payment journey, i.e., the scammer approved the transaction by controlling Mr S's device, I'm satisfied that it would still be fair and reasonable for Ulster Bank to treat the transaction as authorised. This is because according to his testimony, Mr S was aware that funds would be leaving his account – albeit he was tricked into thinking they would be returned. This is supported by the fact that he agreed to move the money out of his savings account and into his current account.

As I'm satisfied that the transaction was authenticated correctly and that Mr S consented to it, it is fair for Ulster Bank to treat it as authorised. And that means the starting position is that Mr S is liable for the payments.

Is there any other reason it would be fair for Ulster Bank to be held liable for the disputed transaction?

Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. There are some situations in which a bank should reasonably have taken a closer look at the circumstances surrounding a particular transfer. For example, if it was particularly suspicious or out of character.

The transaction in question did trigger Ulster Bank's fraud detection systems and it sent a text to Mr S's registered number to check that it was him making the transaction. It has shown that it received confirmation from the same number that the transaction was genuine. And so, the bank processed the transaction.

I recognise Mr S says the scammer responded to the bank's text when they had control of his phone. But the bank wasn't to know that – as I've mentioned it didn't detect any remote access. I've given due consideration to Ulster Bank's duty to make payments promptly, as well as what I consider to have been good industry practice at the time. In the individual circumstances of this case, taking account of the value of the payment, when it was made and the payee, I consider checking that the transaction was being made by its genuine customer was adequate intervention on the bank's part.

I've also thought about whether Ulster Bank could have done more to recover the funds once it became aware of the situation, as in some circumstances it might be possible to recover some or all of the money. Here, the payments were made to an online money remitter, and it's a common feature of the scam Mr S has described that the remitter will have acted on the instructions received and transferred the funds to the recipient. Indeed, this is what appears to have happened on this occasion as R told our Service there were no funds left to return.

In conclusion, I know that Mr S will be disappointed with this outcome. Not least because of how long this complaint has been ongoing. Despite my natural sympathy for the situation in which he finds himself due to the scammer's actions, for the reasons given, it wouldn't be fair of me to hold Ulster Bank responsible for his loss.

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 Mr S to accept or reject my decision before 28 October 2025.

Gagandeep Singh
Ombudsman