

The complaint

T complain that Revolut Ltd failed to refund transactions they didn't recognise.

What happened

T are represented by Mr V. As he was the one who was involved with the disputed transactions, I'll refer to him where it's appropriate throughout this complaint.

Mr V had a business account with Revolut. During the operation of his account, Mr V reported that account details had been changed for some of his payees. Mr V noticed these changes and reported it to Revolut who were able to prevent the funds from leaving his account. Mr V experienced other difficulties with both receiving and sending payments.

Sometime later, Mr V believed his Revolut account had been compromised through a "hack" on his email account. He believed that whoever had done this was able to use the email to gain access to his Revolut account and amend payee details (to change the destination of the payments). Mr V noticed these changes and was able to change them back to the proper account details. There was no loss of funds at this point.

Mr V wanted to close his account but declined to provide identification details that Revolut had requested. This was because he believed the "chat" was being monitored by whoever had accessed his email/Revolut account. Revolut couldn't complete the account closure until they received these details, so they restricted access to the account and waited for the information they'd asked Mr V for to be sent to them.

Mr V explained that he had no intention of using his Revolut account and arranged for his invoices to be paid to a different bank, unfortunately the next payment was sent in error to the Revolut account. Mr V then sent the additional details Revolut had requested and asked for his email address to be changed, which Revolut amended.

Revolut also told Mr V to change his password and explained the process for doing so. Revolut carried out a "hard lock out" of the account to ensure that no other devices were logged into it. Once the account was re-opened, the incoming payment was still restricted and shortly after it was released, several payments were made from the account.

Mr V advised Revolut that his account had been hacked and all the outgoing payments (over £36,000) weren't authorised. Mr V believed that an unauthorised third party had gained access to his account. Revolut blocked the account and attempted to retrieve the funds. Revolut were able to retrieve about £6,000 and paid this back into the account.

Mr V sought a refund for these transactions, but Revolut didn't think that the account had been compromised and they thought that Mr V was negligent by not changing his password when he'd first notified them about his account's security. They declined to make a refund to T. A complaint was raised and Revolut again looked into what had happened but didn't change their position. During the investigation, it was found that two other devices (mobile phones) had previously been registered for use with the account. These registrations took

place some months before the disputed transactions, but Revolut didn't believe they were linked to the disputed transactions.

Evidence from the chat logs showed that Mr V had asked for different phone numbers to be updated on his account at various stages due to his work locations. The number used at the time of the disputed transactions was previously changed by Mr V some months prior to the disputed transactions.

Mr V brought T's complaint to the Financial Ombudsman Service for an independent review. It was looked into by one of our investigators who asked both parties for information about the complaint. Mr V explained what he believed had happened. He was generally unhappy with how Revolut's security had functioned and believed that an unauthorised third party had been able to access his account through a compromise of his email address.

Revolut provided details of their chats with Mr V and information concerning the transactions. Revolut's data indicated that the disputed transactions were carried out by logging into their internet portal, rather than their app.

After considering the information provided by both parties, our investigator didn't uphold T's complaint. She thought there wasn't enough evidence to show someone else had been responsible for the transactions. She also thought the pattern of transactions wasn't indicative of usual fraudulent behaviour.

T disagreed with the outcome and wanted a further review of the complaint. Mr V continued to believe that Revolut's security had been responsible for the loss of his funds and he'd relied on Revolut's confirmation that his account was safe. Mr V believed that further attempts to take the remaining funds from his account occurred some time after the original disputed transactions.

Mr V didn't think that the pattern of transactions was relevant to the complaint, he said that he emptied his account shortly after funds were received.

T's complaint has now been passed to me and I issued a provisional decision where I said:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Revolut can hold T liable for the disputed payments if the evidence suggests that it's more likely than not that they made them or authorised them.

Revolut can only refuse to refund unauthorised payments if it can prove T authorised the transactions, but Revolut cannot say that the use of the internet banking details conclusively proves that the payments were authorised.

Unless Revolut can show that consent has been given, it has no authority to make the payment or to debit T's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to T. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold T responsible for the disputed transactions or not.

I'm very aware that I've summarised this complaint above in far less detail than it may merit. No discourtesy is intended by this. Instead, I've focussed on what I think are the key issues here. Our rules allow me to do this. This simply reflects the informal nature of our service as

a free alternative to the courts. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual argument to be able to reach what I think is the right outcome. I will, however, refer to those crucial aspects which impact the decision I'm making.

Essentially, Mr V on behalf of T, believes that Revolut's security was so poor it allowed an unauthorised third party to gain access to his account to amend payment details, resulting in the loss of his funds.

So, in order to determine if T are due a refund, I have to be satisfied that there's a plausible and likely explanation for how someone could obtain the necessary details to allow them to gain access to T's account.

Principally that involves knowledge of T's password, without which it's not likely anyone could access the account. Mr V confirmed that he never gave anyone else the password or allowed anyone else to use his account. Mr V also believes a compromise of his email account was, in part, responsible for the breach of his Revolut account.

Accessing the email account linked to the Revolut account wouldn't, on its own, provide the necessary details to allow someone to login to the Revolut account. It may allow someone to force a password change on Revolut's account. The process would send an email to the relevant email address and allow someone to change the password. But, if that was the case, then Mr V himself wouldn't then have been able to access his own account which wasn't the case here.

Whilst a compromised email account is a risk for security on other accounts linked to it, it doesn't answer the question of how someone could obtain the necessary password to be able to login to the Revolut account.

I appreciate that Mr V was trying not to use his Revolut account prior to the final invoice being mistakenly paid into it by T's employers. I can also see on the chat he attempted to close his account before this happened. But reading through the chat, Revolut required additional information before they could action such a request and Mr V had decided at that point he wouldn't supply it because he was concerned about security on his account.

Revolut's position is that they couldn't detect any other access to his account and their assessment is that an account take-over was unlikely. Once Mr V had notified Revolut of the change to his outgoing payee details, they restricted his account until he provided details they'd earlier asked for. At this point, Revolut also confirmed they completed a "hard lock out" of all logins to the account and changed the email address. Revolut had previously advised Mr V to change his password and Mr V asked how this was done. Revolut explained how to change it and Mr V then asked for his account to be opened.

Some further administration was needed which was completed and Revolut advised that the funds would be released within a few hours. The incoming payment landed in T's account just after midnight and the disputed transactions took place around 10:00 am that morning. About ten minutes after the final disputed transaction left the account, Mr V notified Revolut about the unrecognised transactions. So, whoever was using the account was able to transfer the funds within hours of them being released into the account – which seems to indicate some knowledge about what was happening with the incoming funds.

Revolut's data doesn't show which device made the transactions because the login details were used through their internet portal rather than their app. What that means here is that it's not possible to identify if a previously registered device was used to access the account.

I understand the frustration that Mr V experienced when he believed his account was being accessed and persons were amending his payee details, but I haven't been able to determine how someone could have obtained the details necessary to access the account in the first place. Without that, I can't make a finding that Revolut were responsible for sending the payments without appropriate authority.

I don't think that Revolut necessarily served T well here, as they notified Revolut on several occasions about their concerns. It's not apparent that Revolut conducted any form of investigation for the earlier notifications by T. But when T notified them of the latest issue, Revolut did lock out all other devices, changed the email and gave T the appropriate advice to change their password. Revolut don't believe the password was changed prior to the disputed transactions.

If that was the case, then I find it unusual for an account holder who believes there's an issue with someone logging into their account - who wouldn't change their password immediately.

Taking everything into account, I think it's implausible to conclude the transactions weren't authorised without stronger evidence to the contrary. That means I currently think it's more likely than not that Mr V on behalf of T carried out these transactions themselves – or that someone else with consent did so.

I invited T and Revolut to give me any more evidence and information they wanted me to consider before issuing my final decision.

Mr V on behalf of T disagreed with my provisional decision and in summary said:

- He believed that unauthorised access to his funds was through Revolut's app and this didn't require either a password or knowledge of the correct email address.
- Revolut's failure to secure the account enabled others to access it and to read the private chats.
- He did change the password after some difficulty, but it didn't make any difference because unauthorised third parties didn't require it.
- He was told that someone else had access to his phone.

I asked Revolut to comment on the assertion that access to the account could be done without either the correct email address or password. Revolut confirmed that both of these details are required to access the account.

I also asked for additional enquiries to be made regarding the beneficiary accounts used to receive the disputed transactions. Further information was received which, in summary said:

- Payments from T's account were sent to a number of other accounts.
- The funds were utilised in a variety of ways.
- Of the three accounts that received funds, all were subsequently closed by their respective banks.
- One of the accounts had received a report about it but no further details were provided.
- Two of the accounts had no other reports made about them.

Revolut were asked to comment further about the complaint and in summary said:

- The "account takeover" was fully investigated when it was reported by T.

- They believed that they'd done everything in their power to protect the account.
- They were confident that there was no breach of their systems.
- Steps were taken to provide the appropriate advice to secure the use of the account.
- The circumstances of the complaint remain "one of a kind".

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.

I'd like to thank both parties for their patience while I've investigated the complaint. Additional enquiries have been carried out to try and establish the best possible evidence upon which to make a fair and reasonable decision about T's complaint.

The complaint is finely balanced and there are some aspects to it that indicate unusual activity, such as repeated concerns about unauthorised access to the account and the use of other accounts to receive funds which were soon utilised. But here I have to make my decision based on the available evidence and where there's a dispute about what happened, and the evidence is incomplete or contradictory, I must reach 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.

Mr V believed their account could be accessed without the email address or password. I asked Revolut about this as it's a fundamental part to the complaint. If the account could be accessed in such a way then it would be very difficult for Revolut to show that it was T who authorised these payments because anyone could just open up the account. Revolut confirmed that both the login details (email address and password) are required to gain access to the account. I'd be surprised if this wasn't the case and Mr V's belief isn't supported by any specific evidence to reflect that this was what happened in the individual circumstances here. So, whilst I've considered this point made by Mr V, I don't think it's plausible that someone could access T's Revolut account without the necessary login credentials.

Mr V reported that he was told someone else had access to his phone by a Revolut employee and I've specifically asked them about this. Revolut told me the comment wasn't backed up by their investigation and believe it was a poorly phrased assumption from the call handler at the time they were still gathering information about the incident. Revolut's investigation didn't detect any other party accessing the chat and couldn't find any evidence of third-party interference and they described the circumstances of this complaint as "one of a kind". What that means for my considerations here is that there is no other evidence of unauthorised access to the account that I've been able to consider.

Revolut supplied details of the various accounts that were set up to receive payments from T's accounts. Mr V didn't recognise them and believes they were set up by unknown third parties to divert his funds. I've considered how these details could have been changed and in the case of the disputed transactions linked to this complaint, how they could have been authorised. None of these details could have been changed without access to the account which required the password and email address to login. I accept that Mr V had a situation some time before these events that resulted in the changing of an account, but this was linked to a separate scam, and it was Mr V in that instance who made the changes (although it didn't result in any loss).

As I've previously mentioned, the issue here is how anyone other than Mr V could have known the password, without which the account couldn't be used, or payments authorised. I also think it's relevant that Revolut changed the email address shortly (less than a day)

before the payments left the account. Prior to the clearance of the payment into the account, Revolut confirmed they locked out any device using the account – that means that only new logins would be successful, so to log back in, the new email address and Mr V's password would have been required. Mr V confirmed he eventually changed his password (although Revolut don't believe that happened prior to the disputed transactions).

Revolut believed that Mr V was negligent by not changing his password when he believed his account had already been compromised. I've thought about this and whilst I don't think there's a case that Mr V was (grossly) negligent, I do think it unusual that Mr V didn't immediately change the password on the account when he believed his account security was at risk. But, as I've mentioned already, both the correct (new) email address and password would have been required and there's no evidence to show how someone could have obtained those details.

Mr V later reported to Revolut that further attempts to empty his account had been made and the remaining balance sent to one of the accounts that had earlier received his funds. Revolut couldn't establish what happened to this transaction as no funds were actually sent, so it remains unclear how the account was accessed, but it remains that access to the account would have required the new email account and the password.

The use of different accounts to send the funds to remains an aspect of the complaint that's not fully explained. The funds were utilised once they were received from T's account. This is often seen in fraudulent attempts to steal money from other bank accounts. Whilst this part of the complaint can be interpreted as unusual, it remains that the security credentials were still required to access the account in the first place.

I haven't seen any evidence or a plausible version of events that would give me reason to think that the password was obtained by unauthorised third parties or that the new email address was compromised. Having considered the additional points raised by Mr V, and whilst I'm sure he'll disagree with me, I see no reason to reach a different conclusion. So, this final decision confirms the findings set out in my provisional decision.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 30 March 2023.

David Perry
Ombudsman