

The complaint

Ms K is unhappy Revolut Ltd (“Revolut”) won’t reimburse her for the money she lost when she fell victim to an ‘authorised push payment’ (“APP”) safe account scam.

What happened

The details and facts of this case are well-known to both parties and were clearly set out in detail by our Investigator – so I don’t need to repeat them at length here.

In summary and based on the submissions of both parties I understand them to be as follows.

Ms K fell victim to a safe account scam. Around a week before the scam, Ms K fell victim to a phishing text – which resulted in Ms K providing some of her banking details.

On 12 August 2022, Ms K then received a text from her other banking provider – whom I’ll call “N”. The text appeared as though it had come from the fraud team and advised Ms K that it had blocked her account due to irregular activity and that someone from the fraud team would call her. It also provided a fraud reference number.

Shortly after, Ms K was called from what she thought was a genuine N telephone number. Ms K says the lady she spoke to knew the reference number she had received by text, sounded professional and her interaction resembled previous interactions Ms K had had with N. Ms K says she was advised that her accounts with N were at risk as a result of the phishing scam and that she needed to move her money into an immediate account (her Revolut account) and then from there on to new accounts that were being set up by N in her name. Ms K was told that she needed to transfer into separate accounts due to her having a current account and a savings account and due to transfer limits. Unfortunately, and unknown to her at the time, Ms K was liaising with fraudsters.

Ms K, believing things to be genuine, ended up moving her funds (from her savings account) with N into her Revolut account. From there, Ms K made seven payments in around two hours to the beneficiary account details provided by the scammer. In total, Ms K transferred £19,000.

Ms K became concerned when the fraudsters tried to also get her to transfer over her current account including an amount for the overdraft. Realising she had been the victim of a scam Ms K reported the matter to Revolut to see if it could help stop the payments or recover her funds.

Revolut logged the matter that evening and contacted the Receiving Firms (the Firms where Ms K had sent the funds to) on 14 August 2022, to see if any funds remained that could be recovered.

Revolut also informed Ms K through its in-app chat function that it wouldn’t be reimbursing her for the payments she had made from her account. Revolut explained it had protections in place and provided adequate warnings before payment authorisation.

Ultimately the Receiving Firms responded to Revolut to advise that no funds remained that could be recovered.

Ms K formally complained about the matter and Revolut issued its final response to Ms K on 9 September 2022. Broadly summarised Revolut remained of the opinion it wasn't responsible for the loss. It advised that on each occasion Ms K set up the new payee it informed her whether the beneficiary account name matched (commonly known as Confirmation of Payee – "CoP"). It then explained it asked Ms K to confirm whether she trusted the beneficiary and also advised that she could potentially be the victim of fraud and could ultimately be deprived of her funds. Revolut explained that Ms K continued with the payments. Revolut also considered it acted in a timely manner in contacting the beneficiary banks to try and recover the funds.

Unhappy, Ms K referred the matter to our service. One of our Investigators looked into the complaint. Broadly summarised, she considered while Ms K had 'authorised' the transfers (albeit while being tricked); Revolut should have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud or financial harm.

She noted that Revolut, in its submissions to our service, advised that it had detected that the initial transfer Ms K made during the scam was high-risk, and that it could indeed be a scam. Revolut explained that it left the transfer at a "pending" state and through its app asked Ms K about the purpose. Ms K at the time was being guided through the payment journey by the scammer and selected 'something else' – with Revolut advising that the correct option was 'safe account' which would have given Ms K an appropriate warning. Ms K proceeded with the payment and didn't take the option to have a live consultation (through its in-app chat function) with a Revolut agent.

Our Investigator considered Revolut's action was proportionate in relation to the first transfer of £100. But she thought the second transfer of £3,000, made eight minutes later should have flagged. She said this because it was another payment made to the same beneficiary (of where there was a CoP no match) in quick succession and was of an increasing amount.

Our Investigator thought Revolut should have been on high alert that Ms K might be at risk of financial harm, and it should have done more to intervene on the second transfer. Our Investigator thought Revolut should have contacted Ms K about it. It was our Investigator's view that, had it done so, it was more likely than not the scam would've unravelled, and the loss would've been prevented. Our Investigator also considered that Ms K wasn't partly to blame and shouldn't bear any responsibility for the loss.

Our Investigator therefore thought the complaint should be upheld in part. She recommended Revolut refund Ms K her losses from (and including) the second transfer onwards. So reimburse Ms K £18,900. She also recommended Revolut pay additional interest on that amount at the applicable saving account rate that the funds had originated from. Our Investigator considered had the scam been prevented, Ms K wouldn't have moved her funds from that account – so this would return her into the position, as far as is possible, had the scam been prevented.

Ms K accepted the Investigators findings, but Revolut disagreed.

Broadly summarised Revolut considered that Ms K chose the wrong payment purpose – choosing 'something else' as opposed to 'safe account' – so it considered Ms K should share some responsibility for the loss as Ms K's responses led Revolut to believing the payments were genuine.

Revolut also considered that had it intervened further, as Ms K was being guided by professional scammers, then it was unlikely that Ms K would have been truthful. So it considered it wouldn't have been able to prevent Ms K from making the payment.

Our Investigator disagreed and remained of the opinion that had Revolut had better intervention the scam would have been revealed. She considered while Ms K had been guided through the payment purpose the scammer had given Ms K a plausible reason why. But importantly she thought Ms K hadn't been provided with a cover story or coached as to what to say by the fraudster if Revolut contacted her. So she considered Ms K, if she had been contacted by Revolut, would have explained what she was doing and why which would have put Revolut on notice that Ms K was at risk of falling victim to a scam. And had things been explained then Ms K would have likely questioned what was going on and wouldn't have made the transfer. The Investigator remained of the opinion that the scam would have unravelled at the point of Ms K making the second transfer and Ms K's losses could have been prevented by Revolut.

Revolut disagreed and asked for an ombudsman to make a determination. So as the matter hasn't been resolved, it's been passed to me for a 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.

Having done so I uphold this complaint in part. I'll explain why.

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 have been good industry practice at the time.

It is the case that Ms K authorised the transfers in dispute and that's accepted by all parties. And under the Payment Service Regulations 2017 (which are the relevant regulations in place here) that means Ms K is responsible for them. That remains the case even though Ms K was the unfortunate victim of a scam.

However, taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which payment service providers are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Taking the above into consideration, in this case, I need to decide whether Revolut acted fairly and reasonably in its dealings with Ms K when she made the transfers to new payees, or whether it should have done more than it did.

Did Revolut act fairly and reasonably in this case?

As I've explained, I consider that as a matter of good practice Revolut should have been on the lookout for unusual and out of character transactions.

I note what Revolut has said about how Ms K used her account. However, Revolut did identify the first transfer to a new payee (which had a CoP 'no match') as high risk. It set it to pending and asked Ms K the payment purpose – to which Ms K chose 'something else' and proceeded with the payment.

Given the value of the payment – I think Revolut acted proportionately here. But eight minutes later, Ms K made a further payment of £3,000 to the same details.

I am mindful that a common theme to a scam - especially a safe account scam – is that a scammer tries to gain as much money from unsuspecting victims as is possible. So where there are multiple payments or transfers made in quick succession, it is a possible indication to a bank or building society that their customer could be at risk of financial harm.

The first transfer Ms K made was for £100 and the second transfer was for £3,000. So it was another transfer to the same payee (with the beneficiary's name being Ms K's – which didn't match) and it was in quick succession and importantly the amount had also increased significantly. I think the second transfer, in light of the first transfer and the risk it had identified there, should have given Revolut a concern that its customer may be at risk of financial harm.

So I'm persuaded that when Ms K made the second transfer which was of an increasing amount to the same beneficiary details (in Ms K's name) and in a very short space of time her account activity was unusual and out of character. I think Revolut should reasonably have taken additional steps and made additional checks before processing the second transfer.

Revolut argues that it did identify the first transfer possibly meant Ms K was at risk and set the transfer to pending and asked Ms K about the purpose of the payment through its app. Revolut says Ms K selected 'something else' – which was the wrong option as there was an option to select 'safe account'. It considers that had Ms K selected the more appropriate option in 'safe account' then she would have seen a warning in relation to those types of scams.

When a risk is identified, the steps a Firm can take to intervene to satisfy itself that its customer isn't at risk of financial harm are its own commercial decision. So the question I must consider is whether Revolut took appropriate action in responding to the risk of financial harm it had identified?

Did Revolut take appropriate action in responding to the risk of financial harm it had identified?

I accept that a 'payment service provider' or 'electronic money institute' does have a duty under the Payment Service Regulations not to delay payments or transfers unduly. But it is not an unfettered duty to execute – and reasonable checks are also required as part of the broad regulatory landscape to treat customers fairly and to safeguard against the risk of fraud or financial harm. I accept there's a limit as to what it can reasonably do; and I still expect consumers to take responsibility for their own decisions – and possibly even bear a reduction in compensation if there is clear evidence of blame on their own part (see below). But when plain triggers of unusual or uncharacteristic account activity exist, it's not unreasonable to expect a Firm's fraud alerts to respond *proportionately* – and that might simply include, for example, a phone call, in app chat or discreet conversation for transactions in branch to check that things are okay.

First, I note Revolut has said that it has provided Ms K (and other customers) with information about scams in email communications. While this is certainly good practice and does raise awareness – from a preventative aspect, Revolut – where it identifies in real time that its consumer is at risk of possible financial harm – still has an obligation to step in and intervene or make additional checks to ensure that everything is ok, and its consumer isn't potentially falling victim to a scam.

When Ms K set up the new payee details, she received a CoP 'account name doesn't match'. I also note Revolut, when Ms K made the first payment to a new beneficiary, said it provided a review transfer screen / page and at the top of this screen / page it stated the following:

"Do you know and trust this payee?"

If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others and we will never ask you to make a payment."

However I'm mindful that Ms K was in a pressure situation, was under the belief that she was talking to her genuine bank, had been told that it was a pseudo account – where the details wouldn't match, and was also being helped through the making the payment. So I can understand why the CoP and the review transfer screen wouldn't have necessarily broken the spell for Ms K.

But and importantly – I think it should have put Revolut on alert that its customer was at potential risk of financial harm when Ms K made a follow up transfer minutes later.

I consider that following its concerns about the first transfer, when Ms K made a second transfer eight minutes later more intervention was required. I say this because it isn't uncommon in scams (such as a safe account scam) for the customer to be guided through the payment journey by a scammer. And without proactive steps to 'break the spell' of scammers, customers will often proceed with the payment they are making. They are unaware that they are caught up in the scam. And when sophisticated elements are involved such as the scammers utilising phishing texts and therefore knowing lots of information about a customer, then the scam becomes significantly more persuasive. A warning is unlikely to have the required impact on a customer that has been manipulated into action through a combination of sophisticated means and fear and who is being guided through the payment journey by a scammer.

So, when I take into account the risk Revolut had identified with the first transfer then it should have intervened when Ms K made another transfer minutes later to satisfy itself that its customer wasn't at risk of financial harm. It was a second transfer to the same details (whereby the payee details were again in Ms K's name – and wasn't an account match) and the amount had increased.

Direct contact with Ms K would likely have made the difference here. And I think that would be a proportionate response in the circumstances – given the risk it had identified. That intervention might have come in the form of Revolut contacting Ms K directly, or by requiring her to contact Revolut herself to speak to a member of staff before being able to proceed.

I've thought carefully about what would've happened had Revolut made enquiries with Ms K (such as an in-app chat or phone call) before processing the transfer.

There is obviously a balance to strike, and I'm not suggesting that Ms K should have been subjected to an interrogation by Revolut. But Revolut ought fairly and reasonably to have satisfied itself that Ms K hadn't fallen victim to a scam, and I'm persuaded it could've done this by asking a few questions of Ms K prior to processing the transfer.

Of course I can't know for sure what would've happened, so I've thought about what is more likely than not to have been the case.

Ms K wasn't given a cover story by the scammer and had only been guided through the payment journey and what payment purpose to select and why. So I disagree that Ms K wouldn't have been truthful in any direct communication with Revolut. I think had Revolut contacted Ms K to enquire what the payment was for – she would have explained what she was doing.

Revolut would, or should reasonably, have been aware that this scenario fits the characteristics of a safe account scam. Firms such as Revolut have actual or constructive knowledge of all the main scams, such as this. So it could have explained this type of scam to Ms K. If that had happened, I consider it likely that the 'spell' of the scam would have been broken and that Ms K wouldn't have proceeded with the transfer.

So I think Revolut could have prevented the losses Ms K incurred when she made the second transfer and Ms K wouldn't have made any further transfers.

Should Ms K bear some responsibility for the loss?

In reaching my conclusions about what is fair and reasonable in this case, I have also considered whether Ms K should bear some responsibility for her loss. Ms K has explained and provided evidence to show the text she received that she thought was from her bank. The text appears from the 'fraud team' and provided a reference number. Ms K has also provided evidence of the telephone numbers and calls she received which Ms K thought was N's number (it transpires there is a one-digit difference to N's genuine number – so very similar). Ms K says the adviser she spoke to knew details about her and her interaction resembled previous interactions she had with her bank – running through all the same processes. The scammer (as a result of the phishing text) was able to make everything seem genuine.

So I can see why Ms K thought she was liaising with her bank and was carrying out the instructions asked of her. The scammers provided plausible answers to Ms K about what she needed to do and why. Again, in a pressure situation such as this, with Ms K convinced she was talking to her bank and where the scammers instil a sense of urgency and panic, I can see why she took the actions she did.

All things considered, Ms K was the victim of a cruel and sophisticated scam. I am satisfied she believed she was liaising with her genuine banking provider at the time and didn't foresee the risk of this sort of harm and was not partly to blame for what happened. So, on the particular facts of this individual case, I don't consider it fair to reduce compensation for some of the loss due to any blameworthy acts or omissions by Ms K.

Did Revolut do enough to recover Ms K's funds?

I've also considered whether Revolut took reasonable steps to recover Ms K's funds once it was made aware she was the victim of a scam. Revolut could have reasonably acted sooner than it did here. Ms K reported the matter on 12 August 2022 and Revolut contacted the Receiving Firms on the 14 August 2022 (according to its records). However I am mindful that Faster Payments are often credited into the receiving account almost instantaneously and fraudsters typically withdraw / move funds on also in case they get frozen or withheld if the matter is reported. Our Investigator obtained information from the Receiving Firms that the funds had unfortunately been moved on / withdrawn almost instantaneously. So even had Revolut acted quicker than it did it unfortunately wouldn't have made a difference.

Summary

Overall, I consider when Ms K made the second transfer Revolut could have done more to prevent Ms K from the risk of financial harm. There was enough going on, in light of the first transfer, to suggest that Ms K may well have been in the process of being scammed and Revolut ought fairly and reasonably to have picked up on this. Had it done so and had Revolut contacted Ms K directly and asked some questions to challenge the purpose of the transfer, I'm persuaded it is more likely than not the scam would have come to light, and Ms K wouldn't have lost out on the £18,900 she ended up transferring.

Ms K has explained that money she lost originated from her savings account held at N. Had the scam not happened the funds would have remained in that account. So I think it is fair that in addition to refunding her outstanding loss, Revolut pay additional interest on that amount at the account rate the funds originated from. Ms K has provided evidence to show the savings account interest rate was 0.30%. I consider this fairly places Ms K back in the position, as far as is possible, that she would have been in had Revolut prevented the second and subsequent transfers – as I consider it should have done.

Putting things right

For the reasons given above, I uphold, in part, Ms K's complaint against Revolut Ltd.

I now direct Revolut Ltd to:

- Refund £18,900 (less any sums that have potentially been recovered and subsequently returned to Ms K).
- Pay additional interest on that amount at 0.30% (which was the rate of the savings account the funds had originated from) calculated from the date Ms K made the transfers until the date of settlement. *

**If Revolut Ltd deducts tax from this part of the award it should provide a tax deduction certificate to Ms K so she can reclaim the amount from HMRC if eligible to do so.*

My final decision

For the reasons given above, my final decision is that I uphold this complaint in part.

I direct Revolut Ltd to pay compensation, as set out above, within 28 days of receiving notification of Ms K's acceptance of my final decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms K to accept or reject my decision before 24 March 2023.

Matthew Horner
Ombudsman