

The complaint

Mrs K complains Revolut Ltd (“Revolut”) declined to refund payments she says she didn’t make.

What happened

On 23 August 2023, Mrs K said she and her husband received a call from someone claiming to be one of their banking providers asking if they’d made any payments from their account. After responding no, Mrs K’s husband – who the call started with – was told their account had been compromised. The individual explained he would receive a call from another of their banking providers and he was provided with a reference number that would be used to confirm the caller in the next call. Prior to this call, Mrs K’s husband was expecting a delivery and had responded to a request for a payment where he had provided details for the same provider that they later realised wasn’t genuine.

Mrs K said the next caller claimed to be their second account provider who after confirming the reference number they were provided with, told them there was a malware virus on the account so she needed to move her money to a safe account. She said this caused her to panic, and at the time she and her husband were rushing to catch a train.

After disclosing she held an account with Revolut, Mrs K and her husband followed instructions to move money into her Revolut account as she was told it was an online account where their money would be safe. She said she wasn’t asked for her card details and doesn’t recall approving anything in her Revolut app. Not long after, she realised she’d been scammed when she noticed the following payments to a merchant I’ll call “I”:

Payment number	Date	Time	Payment amount
1	23 August 2023	3:26pm	£4,000
2	23 August 2023	3:37pm	£2,700

Mrs K reported the scam to Revolut on the same day as the disputed payments. After declining to provide her a refund, Mrs K raised a complaint with Revolut and it issued its final response letter. In summary it said as the payments were authenticated in-app, it couldn’t raise a chargeback claim. Unhappy with Revolut’s response, Mrs K referred her complaint to our Service.

One of our investigator’s looked into the complaint and upheld it. In summary they considered the payments were unauthorised and so Revolut was liable to refund Mrs K. Revolut didn’t agree. Revolut has provided multiple responses to our Service, but its most recent position is that it considers Mrs K authorised the payments. Because Revolut didn’t agree, the matter was then passed to me decide.

I issued a provisional where I upheld the complaint in part. I explained that I was persuaded Mrs K approved the two disputed payments in her Revolut app and in doing so, she made a representation to Revolut that the payment instruction was made by someone acting on her behalf. And so it was fair to treat the payments as authorised. But Revolut ought to have intervened when the second payment was made and if it had, its likely the payment would have been stopped. So it was liable to refund 50% of the second payment taking into account Mrs K's contributory negligence.

Revolut didn't confirm if it agreed or disagreed, but Mrs K didn't agree. I've summarised her points below:

- Mrs K says she never made an online transaction on her Revolut account so that alone should have been suspicious. And overall given her prior spending this activity was very unusual and out of character for her account.
- She was told by the fraudster they would take out money from her Revolut account and put it into a safe holding account, and would then be returned once the malware virus was fixed.
- She was the victim of a remote account take over.
- Due to the call she received, that she believed was from her bank concerning the safety of her money, she doesn't believe she contributed negligently but instead acted to protect her money.
- Revolut has been negligent in providing any support, ignoring requests for help, support or advice.

I now consider it appropriate to issue my 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, and having considered the responses to my provisional decision, I still uphold this complaint in part. I'll explain why.

Were the disputed payments authorised?

The dispute here is around whether Revolut has acted fairly in treating the disputed payments as authorised. Revolut says this is because Mrs K approved the payments in her Revolut app and so therefore authorised the payments.

In line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, the starting position is that Revolut is liable for unauthorised payments, and Mrs K is liable for authorised payments.

For a payment to be authorised, it must be consented to by Mrs K or someone acting on her behalf. This consent must be given in the form and in accordance with the procedure agreed between Mrs K and Revolut. In practice this is set out in the applicable terms and conditions, though Revolut's terms and conditions at the time these disputed payments were made aren't clear on how consent is given for online card payments.

The technical data Revolut has provided shows the two disputed payments were made online using Mrs K's card details and were approved using the 3D Secure ("3DS") system. This is an additional security layer for online payments that prompts an additional authentication step such as approving a payment within the Revolut app or entering a one-time passcode into the merchant's website. So it was these steps that led to the payments being made.

It's unclear how the fraudster obtained Mrs K's card details as she said she didn't share this information with them. I consider it possible this information might have already been known by the fraudster prior to the call, but equally I consider it possible Mrs K shared these details whilst speaking to them. But given how the scam unfolded, I think it's most likely that it was the fraudster that initiated the payments on the merchant's website with Mrs K's card details.

I've gone on to consider Revolut's point that it considers the payments to be authorised on the basis that Mrs K confirmed the payments in her Revolut app. As part of this I've reviewed Revolut's technical data where Mrs K disputes approving the payments in her app, and what Revolut has shown the screens presented to Mrs K would have looked like.

Revolut has shown the 3DS method involved for these payments required confirmation within the Revolut app. The data it has provided shows each payment prompted a notification that required the payments to be approved, and that it was done using an iPhone X. Revolut has shown this device was the only mobile phone device registered to Mrs K's account at the time of the disputed payments, and it was this device that was logged into Mrs K's Revolut app at the time these payments were made. And it was this device that Mrs K confirmed as being hers. So given the evidence I have, I'm persuaded Mrs K approved the payments in her Revolut app. Whilst I appreciate she said she didn't, the technical data Revolut has provided doesn't support this. The evidence shows it was approved on Mrs K's device.

Further to that, I note Mrs K has said she was the victim of a remote account takeover. This is a scenario where a third-party has gained access to the victim's device where third-party software has been downloaded. Often referred to as 'remote software'. She's referred to an online report published by Revolut in support of this. And because of this, she thinks this is how the fraudster was able to move her money out of her account. However, in its investigation, Revolut asked Mrs K whether she downloaded a remote software programme, which she said she hadn't. So I don't consider it likely that the fraudster had remote access to Mrs K's device. And I've seen no other evidence that supports how someone else could have approved these payments from her device.

Turning to the payment screens, Mrs K was asked to go through a series of pages to authorise the payments. These showed the merchant's name, the payment amount, and Mrs K was then given the choice to confirm or reject the payments. Mrs K then selected 'confirm' on both occasions.

I think that by doing this, Mrs K made a representation to Revolut that the payment instruction was made by someone acting on her behalf. Further to that, in response to my provisional decision, Mrs K explains she was told by the fraudster they would take out money from her Revolut account and put it into a safe holding account, and would then be returned once the malware virus was fixed. So I consider that further supports that by selecting confirm, she was making a representation to Revolut that the payment instruction was made by someone acting on her behalf.

And the clarity of the page about what Mrs K was confirming meant that it was reasonable for Revolut to rely on this representation and process the payments. So, for these reasons I think that it's fair for Revolut to treat the payments as authorised.

Should Revolut have recognised Mrs K was at risk of financial harm from fraud?

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mrs K modified the starting position described in *Philipp*, by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with Mrs K and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately¹. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut

¹ The Payment Services Regulation 2017 Reg. 86(1) states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

should in August 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;²
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with “due skill, care and diligence” (FCA Principle for Businesses 2), “integrity” (FCA Principle for Businesses 1) and a firm “must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems” (FCA Principle for Businesses 3).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017, BSI Code³, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a

² For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/

³ BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Since 31 July 2023, under the FCA's Consumer Duty⁴, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"*⁵.

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in August 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does).

Considering the first payment, though it was the largest payment Mrs K had made on her account considering the recent activity, I don't think it was so significantly suspicious in its appearance that it ought to have concerned Revolut. And I don't consider it unusual that a customer might on occasion need to make a one-off larger payment like it may have appeared here for Revolut.

Mrs K argues that she hadn't made online payments before, so this alone should be suspicious. But I don't agree this alone means Revolut ought to have been concerned. I don't consider it unusual that someone may need to make an online payment for the first time. Given the overall circumstances I don't consider Revolut missed an opportunity to have prevented the first payment.

But I consider by the second payment, there was a pattern of behaviour developing that was out of character for Mrs K's account. In less than 30 minutes, there were multiple top-ups into her Revolut account for £6,700 with the same value spent across the two disputed payments to the same merchant. Considering the recent activity prior to these payments, Mrs K used her Revolut account infrequently for smaller value payments. So by the second

⁴ Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

⁵ The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

payment I consider there was a significant increase in spending on the account, and a sudden change to the operation of the account, that I consider ought to have given Revolut cause for concern that Mrs K was at a heightened risk of fraud.

What should Revolut have done and would an intervention have made a difference?

I consider the account activity was out of character for Mrs K and indicative of a heightened risk of fraud to the extent that it would have been proportionate for Revolut to discuss the activity in more detail with Mrs K.

Had Revolut asked about the payment purpose, I consider it more likely Mrs K would have provided an answer that would have concerned Revolut. Whilst Mrs K has said she didn't approve anything in her Revolut app, and I've otherwise set out that the technical information shows she did, given the overall circumstances I don't think Mrs K intended to send money out of her Revolut account. And the technical information supports that she approved the payment screens quickly. Had Revolut gone on to ask more around the wider circumstances, I think she would have explained that she was told by another of her banking providers to move money into her Revolut account to keep it safe which ought to have suggested Mrs K was falling victim to a safe account scam. I've seen no evidence that suggests Mrs K was being coached to not trust contact from Revolut or to be dishonest with Revolut.

With appropriate warnings around safe account scams, I'm satisfied it would have stopped Mrs K from proceeding further, and the scam would have unravelled.

Should Mrs K bear any responsibility for the loss?

Whilst I think Revolut failed to take sufficient steps to protect Mrs K, I also need to consider her own actions and whether it would be fair for her to bear some responsibility for her loss. In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

Mrs K and her husband received a call from someone claiming to be one of their banking providers, asking if they'd made any payments from their account. She said it all felt genuine because her husband had provided his details for a payment where he thought he hadn't received his package, and received a text from this banking provider asking if he recognised a payment. This was then followed by the scam call where they were again asked whether they recognised payments being made. She added that this provider was their main bank account and this felt similar to previous experiences where her banking provider had reached out to confirm if they recognised payments. She said when they then received a call from who they thought was their second account provider, who relayed back the reference they were provided, this further convinced her the calls were genuine. I appreciate why she thought she was speaking to her banking providers. I don't think she was negligent in not carrying out further checks.

But as I've considered Revolut's intervention could have positively impacted her decision-making on the second payment, I've also considered her actions at the point the second payment was made.

The second payment was carried out 11 minutes after the first payment. In between the payments, there were multiple account top-ups by Mrs K using Apple Pay. Because of how the payments were carried out, it shows she was actively in her Revolut app during this time, and this is further supported by the Revolut app login data Revolut has provided this Service. Given the first payment had utilised almost the entire balance at the time, and given Mrs K was in her Revolut app and carrying out actions within the 11-minute period, she ought to

have been on notice that the money she had added into her account prior to the first payment being made was no longer there. And while I appreciate Mrs K has described feeling under pressure because of what she was told by the caller, and I can see she was quick to approve the second payment, I consider there was enough time in between the payments for Mrs K to have realise something wasn't right.

While I note Mrs K's response to my provisional decision on this point, for the above reasons I still consider it would be fair to make a deduction in the circumstances to factor her contributory negligence. So I therefore consider it fair for Revolut to refund 50% of the second payment, and pay interest to compensate Mrs K for the time she's been without her money.

Recovery

I've gone onto consider whether Revolut could have done more to have recovered the first payment. As the disputed payment was an online card payment, a recovery option that would have been available to Revolut would have been through the chargeback scheme. This is a scheme run by the card scheme provider to resolve payment disputes between customers and merchants – subject to the rules they set. The scheme is voluntary and limited in scope.

I note the merchant's category code falls under 'automobile parking lots and garages'. We can't know for certain what happened after the payment was made to the merchant but given the evidence I have and the type of merchant involved here, I consider it more likely than not that it would have evidenced that it provided the goods/service expected, albeit for the benefit of the scammer. So I don't think it's likely that a chargeback claim would have succeeded and so Revolut couldn't have done anything more to have recovered the first payment.

Customer service

Following my provisional decision, Mrs K's raised that she felt Revolut was negligent in the support it provided her saying it ignored her requests for help, support or advice. And this was part of the complaint she made to Revolut about its handling of her fraud claim, which it considered when it issued its final response to her complaint. I appreciate it would have been a stressful and worrying time for Mrs K, and it would have been disappointing where Revolut didn't agree to refund her.

Having considered Revolut's handling of the fraud claim, I consider it reviewed the matter appropriately in line with the claim it received. I think ultimately here the concerns Mrs K has raised relate to Revolut's decision to not provide a refund. And I've set out my conclusions earlier on what I think Revolut needs to do to put things right considering both parties' liability for the second payment. But I also consider the majority of the distress that's been caused to Mrs K has been as a result of the fraudster's actions, for which I can't hold Revolut responsible for. So I don't think an award of compensation is warranted here, or that Revolut needs to do anything further on this part.

Conclusion

I appreciate my decision will likely come as a disappointment to Mrs K, having fallen victim to such a cruel scam. Having considered this complaint carefully, I consider Revolut was fair to treat these payments as authorised, but as I consider that an intervention on the second payment would have likely unravelled the scam, it would be fair for Revolut to refund 50% of the second payment factoring in Mrs K's contributory negligence.

My final decision

For the reasons I've explained, I uphold this complaint in part. My final decision is Revolut Ltd should:

- Refund Mrs K 50% of the second payment (£1,350).
- Pay 8% simple interest per year on this amount from the date of loss to the date of settlement (if Revolut Ltd considers that it is required by HM Revenue & Customs to withhold income tax from that interest it should tell Mrs K how much it's taken off. It should also give Mrs K a tax deduction certificate if she asks for one so she can reclaim the tax from HM Revenue & Customs if appropriate).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs K to accept or reject my decision before 8 July 2025.

Timothy Doe
Ombudsman