DRN-5645093

The complaint

A company, which I'll refer to as B, complains that Revolut Ltd won't reimburse it after it lost money to an impersonation scam.

Mr S, who is the director of B, brings the complaint on B's behalf via a family representative. For ease of reading, I'll refer to all submissions as being made by Mr S directly throughout this decision.

What happened

On 27 May 2025, I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any more evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

Mr S has explained that in September 2023, he was contacted by an individual purporting to work for the Financial Conduct Authority (FCA). Unfortunately, unbeknownst to Mr S at the time, this individual was in fact a fraudster. Mr S was told that there was advanced identity fraud against him. Mr S has explained that the fraudster knew of some of the accounts he held, including his Revolut business account. He was told this account was safer than his other accounts, as it was based online and had better facial recognition features. Mr S was therefore told to move funds from his other banks to this account.

Mr S moved funds from five other banking providers into his Revolut account. When questioned by other banking providers about why he was moving funds, he told them he was making changes to his business to expand, which required funding. After one branch meeting, the fraudster was able to accurately describe the appearance of the bank clerk that served Mr S, telling Mr S that clerk was under FCA surveillance. Another time after speaking to a banking employee by phone, the fraudster told Mr S he had used voice recognition and could confirm the employee was newly employed and also under surveillance. Mr S was told he could not speak to anyone about the investigation – to keep his funds safe.

Once funds were transferred to Revolut, Mr S was advised by the fraudster that they wanted to catch the criminal taking over his profile, so they were moving his funds temporarily to FCA controlled accounts. Mr S was told that once the individuals were caught, his funds could be returned. While Mr S sent funds to accounts in various names, he was told these were 'pretend' accounts. Below is a list of all transfers inwards and out of Mr S' Revolut account:

Payment number	***Date/time***	***Payment method***	***Value***
	06/09/2023 13:40	*Transfer in from account 1*	*+£4,900*
1	***06/09/2023 13:55***	***Card payment***	***£5,000***
	06/09/2023 14:17	*Transfer in from account 2*	*+£50*
	06/09/2023 16:03	*Transfer in from account 2*	*+£70,000*
	06/09/2023 16:08	*Transfer in from account 3*	*+£15,000*
	06/09/2023 16:33	*Transfer in from account 1*	*+£7,400*
2	***06/09/2023 16:34***	***Transfer to payee 1***	***£24,500***
3	***06/09/2023 16:47***	***Transfer to payee 1***	***£19,500***
4	***06/09/2023 16:48***	***Card payment***	***£5,000***
5	***06/09/2023 17:00***	***Transfer to payee 2***	***£24,500***
6	***06/09/2023 17:06***	***Transfer to payee 2***	***£19,500***
	06/09/2023 17:40	*Transfer in from account 4*	*+£50*
	06/09/2023 18:01	*Transfer in from account 3*	*+£8,000*
7	***06/09/2023 18:08***	***Transfer to payee 1***	***£8,000***
	07/09/2023 09:21	*Transfer in from account 1*	*+£6,500*
	07/09/2023 10:22	*Transfer in from account 4*	*+£20,000*
	07/09/2023 11:53	*Transfer in from account 2*	*+£25,000*
8	***07/09/2023 12:17***	***Transfer to payee 3***	***£24,500.20***
9	***07/09/2023 12:28***	***Transfer to payee 3***	***£19,500.20***
	07/09/2023 13:09	*Transfer in from*	*+£12,000*

		account 1	
10	***07/09/2023 13:19***	***Transfer to payee 4***	***£20,000.20***
	07/09/2023 16:26	*Transfer in from account 2*	*+£2,500*
	07/09/2023 17:02	*Transfer in from account 2*	*+£1,400*
11	***07/09/2023 17:33***	***Transfer to payee 5***	***£4,100.20***
	08/09/2023 07:59	*Transfer in from account 5*	*+£10,000*
	08/09/2023 08:21	*Transfer in from account 1*	*+£4,000*
12	***08/09/2023 08:33***	***Transfer to payee 5***	***£9,500.20***
13	***08/09/2023 09:45***	***Transfer to payee 5***	***£4,250.20***
	09/09/2023 07:58	*Transfer in from account 5*	*+£9,000*
14	***09/09/2023 08:06***	***Transfer to payee 5***	***£9,000.20***
	09/09/2023 11:33	*Transfer in from account 4*	*+£1,900*
15	***09/09/2023 12:51***	***Transfer to payee 5***	***£2,000.20***
			Total losses: £198,851.60

While Mr S recalls making all inward and outward transfers relating to the scam, he does not recall how the card payments were made. He's explained his Revolut bank card is left in his bedroom and wasn't moved throughout the scam.

During the course of the scam, Mr S also noticed unusual activity on his credit card, which he raised with the fraudster. The fraudster told Mr S that the fraud on his accounts appeared larger than they had expected and told Mr S to leave his credit card and some other specified cards outside his home for forensic examination. Mr S did as instructed and the cards were removed shortly after.

Several days into the scam Mr S tried to arrange a face to face meeting with the purported investigators. However, when these kept failing to materialise, Mr S realised he had fallen victim to a scam and contacted Revolut to raise a claim.

Revolut considered Mr S' claim but didn't uphold it. It said that it provided a scam warning when Mr S set up new payees as part of the scam and also asked Mr S to confirm on three occasions (payments 2,5 and 8) the payment purpose. Each time, Mr S selected 'goods and services', despite 'safe account' being an option.

Revolut also said that it attempted to recover Mr S' funds promptly after the scam was raised, but unfortunately, only £26.55 was recoverable.

Mr S remained unhappy and referred his complaint to our service. He also complained that Revolut repeatedly asked him for information during the claims process via the in-app chat, despite having disabled his access to this function, making communication stressful and difficult.

An investigator considered Mr S' complaint but didn't uphold it. She concluded, having considered intervention conducted by other banks when Mr S made inward transfers to his Revolut account, that when Mr S made payment two to the scam, Revolut ought to have done more to protect Mr S from financial harm from fraud, by questioning the payments with him to better understand them. However, she thought that even if Revolut had done so, the scam wouldn't have come to light. This was based on Mr S not being open with his other banking providers about the payment transfers he was making and the heavy coaching applied by the fraudster.

Mr S disagreed with the investigator's view. Among other points, to summarise, he said it was the investigator's view, and not fact, that intervention from Revolut would not have broken the spell of the fraudster. Mr S also set out why he should be considered a vulnerable customer and that in the least, Revolut would've been aware of his age as a vulnerability factor.

As Mr S disagreed with the investigator's view, the complaint has been referred to me for a final decision.

What I've provisionally 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, 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 Payment Services Regulations (in this case the 2017 regulations) 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 Mr S 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 Mr S 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 immediately[1]. 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 should in September 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*

---

[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).

[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_/

"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 Code[3], 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 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 Duty[4], 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 September 2023 that Revolut should:

- *have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;*

---

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

[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)

- *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).*

Did Mr S authorise all payments made during the scam?

Mr S has explained he doesn't recollect how the payments via card were made. He's said that his card was kept in his bedroom and doesn't believe he removed it to facilitate any payments. However, he has also accepted that, as a result of the scam's impact, his memory has since deteriorated, and he finds specific details harder to recall. I've considered all the available evidence to determine whether I think Mr S did authorise these payments or whether his account may have been compromised.

For a payment to be authorised, it must have been made by Mr S, or by someone acting with his consent. This consent must be given in the form and in accordance with the procedure agreed between Mr S 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 card payments were made online using Mr 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 would've obtained Mr S' card details, as he said he doesn't recall sharing this information with them. I consider it possible this information might have already been known by the fraudster prior to the scam beginning, but equally I consider it possible Mr S shared these details whilst speaking to the fraudster. 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 Mr S' card details.

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

Revolut has provided evidence that, as a result of both card payments, payment verification messages were sent – and that Mr S' phone was the only phone linked to his Revolut account at the time to receive the message.

The screenshots provided by Revolut demonstrate that when verifying the payments, Mr S would've been provided with the merchant name, the value of the payment, and asked to confirm or cancel the payments. I think that by confirming, Mr S made a representation to

Revolut that the payment instruction was made by him, or someone acting on his behalf. And the clarity of the page about what Mr S 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 that Mr S was at risk of financial harm from fraud?

It isn't in dispute that Mr S has fallen victim to a cruel scam here, and whilst I have set out in detail in this decision the circumstances which led Mr S to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr S might be the victim of a scam.

When Mr S made his first card payment towards the scam, this was notably higher than any other payment he'd made previously from his account, the highest before this being for around £1,000. Revolut went through 3DS checks with Mr S, which I think would've provided reassurances that it was Mr S making the payments. However, this didn't provide Revolut with any reassurance on whether Mr S was making this payment towards a scam, which I think was also necessary here given the higher payment value.

Additionally, when Mr S then made the second payment that day of £24,500, this was so out of character for the account that I think it also ought to have put Revolut on alert that Mr S was at risk of harm from fraud, particularly as Mr S had provided confirmation when setting up the account of maximum expected payment values (£3,000), as well as monthly transaction values (up to £10,000), and this one payment far exceeded both. Not only was this two out of character payments by this point within the same day, but Revolut would also have been aware that Mr S had made five transfers into his account that day as well (again, each account sending a higher sum than had ever been transferred in before in one transaction), from three different external accounts.

By transferring such large amounts into the account from a number of external accounts, followed by attempting large payments out to new payees, I think that by the £24,500 payment (payment 2 of the scam) a pattern was beginning to emerge indicative of safe account/impersonation scams that Revolut ought to have recognised as a potential risk.

What did Revolut do to warn Mr S?

As mentioned, when Revolut processed Mr S' first card payment, it took him through a 3DS process, which would've provided Revolut with assurances that Mr S was the individual making the payment.

Additionally, when Mr S made the payment transfer of £24,500, Revolut confirmed the account details provided matched the name on the account and provided Mr S with the following warning:

*'**Do you know and trust [account name]?***

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

After choosing to proceed following this message, Revolut has confirmed that its systems recognised this transfer as suspicious and it was put in a pending state. Revolut requested confirmation from a drop down of what Mr S was making the payment for and Mr S selected 'paying for goods or services.' As a result, Revolut provided the following warning:

*'**Stay protected from fraud and scams***

Before transferring money, please be aware that:

1. *scammers will typically offer a price below market value to attract your attention*
2. *scammers will often use social media to advertise their goods and services*
3. *you should avoid bank transfer payments when card payment options are available*
4. *you should research vendors when making first-time purchases and check for any negative reviews*
5. *you should validate payment requests through known communication channels*

If you're at all suspicious, please stop and read our scam guidance. By completing your transaction without knowing all the information, you risk losing money that we may not be able to recover.'

Revolut has confirmed this warning was also provided for payments five and eight.

Considering the value of payments being made here, the sudden increase in account activity and these payments coming in from multiple sources, then back out to a new payee, I don't think a questionnaire-based warning was proportionate in the circumstances, particularly given banks' awareness that customers can be told to conceal matters from them, and also given Mr S' age which I think ought also to have been factored into Revolut's considerations of whether he may be at risk of harm from fraud. This is particularly the case given that these payments post date the inception of the FCA's Consumer Duty, which emphasises the requirement for firms to act to deliver good outcomes for all customers, including those in vulnerable circumstances.

<u>What kind of warning should Revolut have provided?</u>

As mentioned, when Mr S made the initial card payment of £5,000, Revolut took steps to assure itself that it was Mr S making this payment. However, in order to also reassure itself that Mr S wasn't falling victim to a scam, I think Revolut also ought to have asked some proportionate questions, whether by dynamic warnings, or via in-app chat to understand the payment further. Based on the payment value and the perceived risk to Mr S at this point, as well as how Mr S answered subsequent questions posed by Revolut, I think Mr S would likely have been able to assure Revolut this payment was related to his business and passed through any proportionate questioning.

However, when Mr S made the £24,500 payment transfer, the risk was clearly much higher and I would have expected Revolut to be asking more probing questions before processing the payment. Additionally, by this time, there were further risk factors at play. Mr S was making a second payment in the same day towards a business seemingly unrelated to that which he was running, and he had transferred significant sums in from various other accounts. Additionally, as touched upon above, these payments were made after the inception of the FCA's Consumer Duty. Mr S was aged 85 when the scam occurred, and unfortunately impersonation scams of this nature are known to target older individuals.

I don't think it was sufficient for Revolut to asked Mr S automated questions about these payments, or to take first answers at face value, considering that we know that fraudsters will tell scam victims to conceal what they're doing from the bank for various reasons. Therefore, before processing this payment, I would've expected Revolut to have spoken to Mr S, either by phone or in-app chat to question in more detail the payment he was making.

Additionally, as I've referenced, I think the overall picture painted by Mr S' account activity was that the greatest fraud risk here related to safe accounts (based on large volumes of payments into one account and these then being quickly sent on to new payees). I would therefore have expected Revolut to provide questioning related to these scams.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Mr S suffered from payment two?</u>

While I think it's likely that Mr S would've initially tried to mislead Revolut as to why he was making the payment, I think there would've been red flags in what he was saying. Mr S' business appears to be run from his home address, and yet Mr S was attempting to make payments of nearly £30,000 in one day to roofing firms and chauffeur companies from his business account, which I think would have proved difficult to explain given the disparity between this and his business' function.

Having considered intervention by some of Mr S' other banks, I accept they did attempt to warn Mr S about safe accounts. Mr S doesn't recall these in detail - he remembers the primary aim in the calls or conversations being on where his money was going – which he knew to be an account securely held by him. However, in any event, Mr S has explained that the purpose provided by the fraudster for moving his funds to Revolut was that this was the most secure account and was considered safe. He says that if Revolut had therefore contacted him and warned him about moving his money, it would have impacted him differently, as he considered this account was already 'safe'.

Additionally, while other banking providers did reference the impersonation of banks and the Police, the FCA wasn't something that was raised. And as Revolut was the end point here for all other inward transfers, it had a much greater oversight of what Mr S was doing to identify primary fraud concerns. Having this awareness, I think Revolut ought to have covered impersonation scams in detail, including the FCA as a potential body that fraudsters may impersonate, given the prevalence of these scams, particularly in Mr S' age bracket. Red flags to cover could also have included (but aren't limited to) being told to conceal the 'operation' from banks and family, being told funds are being sent to accounts that are either 'safe', 'owned by staff' or 'dummy accounts' and being told that other banks or staff may be complicit. Additionally, if Revolut had any doubt about the information Mr S was providing for the payment purpose, I think it would've been prudent to ask for evidence, such as invoices, for the payments Mr S was making, which, of course, he wouldn't have been able to provide.

Had Revolut covered impersonation scams in the way I've set out above, I think all these factors would have resonated with Mr S and made him realise he may have fallen victim to a scam.

As mentioned, while other banks had referenced safe account scams, none covered the specific type Mr S was falling victim to here and essentially, Mr S wasn't sending money to a safe account at this point for the message to have resonated to the same extent – he was sending funds to another of his own accounts.

Had Revolut used the greater wealth of information it had available to question Mr S on his account activity and provide a more specific warning to the scam he was falling victim to, I think it's more likely than not that Mr S would've been prevented from making payment two onwards towards the scam and that these losses could therefore have been prevented.

Should Mr S bear any responsibility for his losses?

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.

In doing so, I've considered all elements of this scam. I accept that, at times, some of the things Mr S was asked to do may have been less plausible than others - for example being told to leave his bank cards outside his home. However, there were also elements of this scam that I consider would have been believable – for example, Mr S has explained that the fraudster knew about a number of his accounts without him providing this information, it had information about bank clerks that served him in branch that I consider too specific to have guessed and would, to me, suggest that the fraudsters went to the extent of following Mr S. Mr S was told not to speak to even family about what was happening and, in any event, the scam unfortunately occurred at a time when a close family member of Mr S was away, leaving Mr S to deal with the situation alone and with a real fear that his money could be lost. Additionally as mentioned, I think Mr S' age is a notable factor here, and within a bracket we know to be targeted for this scam.

Having considered all circumstances holistically, and taking Mr S' personal circumstances into account, I don't think it would be fair and reasonable to hold Mr S partially responsible for his losses, given the elaborate level of the scam and sense of urgency we know to be applied in these circumstances.

Could Revolut have done anything else to recover Mr S' money?

I've thought about whether Revolut could have done more to recover the first payment made towards the scam that I'm not recommending Revolut reimburses. 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/services 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 that first payment.

Trouble and upset caused from the scam

Mr S has raised that he had difficulty communicating with Revolut during the claims process, which caused additional distress and frustration. Having reviewed Mr S' in-app chat with Revolut, I can see Mr S raised this scam with Revolut late in the evening of 11 September

2023. He explains he has lost almost £200,000 to a scam, is vulnerable and needs to speak to someone by phone to raise a claim. Mr S is initially told he can't speak to anyone by phone, despite him having explained that there are too many payments to cover over the app. Mr S was eventually advised he will receive a call the following day – however despite chasing this the following afternoon no call was received until the day after – so over 40 hours after first reporting he was a fraud victim. Following the call it appears Mr S also received messages via the in-app chat, despite having raised that he can't access it.

I can imagine that these additional barriers, at a time when Mr S had just lost a lifetime of savings, would've exacerbated the upset and worry he was already facing. I think a further £250 compensation from Revolut is a fair way to acknowledge the impact this would have had.

My provisional decision

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

- *Refund Mr S his losses to the scam from payment two onwards, totalling £193,850. A deduction of £26.55 can be applied for funds already recovered by Revolut Ltd.*
- *Pay £250 compensation*
- *Apply 8% simple interest from the date each payment was made, until the date of settlement.*

Mr S agreed with the decision but Revolut didn't. To summarise, it said that:

- The consideration of vulnerability has been heavily weighted in this case and seems to rest entirely on Mr S' age;
- This was a business account, not a personal one. Applying vulnerability considerations to authorized users of such accounts presents substantial operational and regulatory challenges and such expectations over business accounts seem unrealistic for payment service providers. Such shifts in our service's approach should be communicated transparently across the sector;
- Mr S was provided with warnings by Revolut and, on each occasion, selected 'goods and services' as the payment purpose – indicating a legitimate transaction;
- My provisional decision suggests that stronger intervention by Revolut would have been successful, despite other banks having intervened. Revolut disagrees that causation has been clearly established here.
- Our service should conduct further inquiries into the actions and interventions of other banking providers and this is crucial and seems to have been overlooked.

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.

On the points Revolut has raised regarding the weight I've placed on Mr S' age and whether he should, as a business customer, have been considered vulnerable, I'd like to first clarify that my decision doesn't turn on this point. Regardless of Mr S' age, I think that when Mr S made the payment of £24,500, this was so out of character, it warranted further intervention by Revolut in the form of a phone call or in-app chat. I also think that, regardless of Mr S'

age, during this conversation with him, Revolut ought to have been alert to the fact that there were indicators of a safe account scam from Mr S' account activity, and that in such scams, customers are often told to mislead their banks and may need to be probed on more than one occasion to uncover the truth.

However in addition to the above, I think that Mr S' characteristics are still of importance here. The *FCA's 'Guidance for firms on the fair treatment of vulnerable customers'* states that while the guidance only applies to *'firms' dealings with retail customers who are natural persons, firms should remember that the Principles, including the obligation to treat customers fairly, extend to all customers.'* It also confirmed that firms *'may find this Guidance helpful when considering how to comply with their obligations under the Principles for incorporated business. For example, when dealing with a representative of an incorporated business who has characteristics of vulnerability'.* Therefore as explained, while my decision doesn't in any event pivot on this point, I don't agree that my consideration of vulnerability is a shift in our service's approach, and instead supports guidance set out by the FCA on how such vulnerabilities should be considered. I think it's important to remember here that at the time the scam occurred, Mr S was the sole director of B and Revolut would therefore have held information about him as a customer to consider during any interactions that occurred. As a customer and individual behind the business, I don't think it's unreasonable to conclude that Mr S' characteristics should be taken into consideration, particularly when individuals of this age bracket are known to be more susceptible to safe account scams, as was the immediate danger here.

Moving on to causation concerns raised by Revolut, I accept that this is a finely balanced case, and – of course – we can never know with certainty how Mr S might have responded to further questioning by Revolut. In terms of other banks' involvement, all relevant parties have already provided evidence of their own interventions. As set out in my decision, some other banking providers did cover relevant warnings such as safe accounts. However, none made reference to the FCA, which I think was crucial here and not unreasonable to expect, given the prevalence of such scams.

Additionally, as mentioned in my provisional decision, all other banking providers were questioning Mr S based on the limited visibility they had over the scam – all could see a maximum of five payment transfers being made from Mr S' personal account, to a business account owned by him. Therefore, the identifiable risk was very different to that available to Revolut, where it could be identified that these inward transfers were being made across several accounts, and then out to a new payee in values entirely out of character for the account.

Revolut therefore had a stronger starting point to question Mr S on why he was taking such action and a greater reason to question his answers. Additionally, Mr S has explained the difference in his thought processes when moving money from his other accounts versus Revolut. From other accounts, he knew he still had control over the funds, and was merely moving it between accounts. However once with Revolut, he believed the accounts he was paying were 'pretend'. Therefore, had Revolut provided an in-depth explanation of how safe account scams work, as I think was appropriate here, I think this would've been sufficient to resonate with Mr S and make him doubt what he had been told by the fraudsters.

For these reasons, having considered the additional points raised by Revolut, my opinion on this complaint remains the same as set out in my provisional decision.

My final decision

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

- Refund Mr S his losses to the scam from payment two onwards, totalling £193,850. A deduction of £26.55 can be applied for funds already recovered by Revolut Ltd.

- Pay £250 compensation
- Apply 8% simple interest from the date each payment was made, until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask B to accept or reject my decision before 22 July 2025.

Kirsty Upton
Ombudsman