DRN-5659426

The complaint

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

Ms B, who is the director of G, brings the complaint on G's behalf. For ease of reading, I'll refer to all submissions as being made by Ms B directly throughout this decision.

What happened

On 11 June 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.

Ms B has explained that in December 2023, she was contacted by an individual purporting to work for Revolut. Unfortunately, unbeknownst to Ms B at the time, this individual was in fact a fraudster. She was told that there were attempted cyber attacks on her Revolut accounts, as well as another account held with a separate banking provider. Ms B has explained that the fraudster appeared to know what accounts she held, and that the accounts contained funds. Ms B was told that she would receive a call shortly from her other banking provider to secure her funds.

Shortly after this call, she received another, from a fraudster purporting to work for her other banking provider. This fraudster told Ms B that as Revolut was safer to hold her funds, she should move money to her Revolut account. Ms B has explained that she was initially concerned about the calls, so checked the phone numbers online, but found them both to be genuine numbers for Revolut and her other bank, which allayed her concerns.

Ms B was told a new business account and personal account had been set up for her to keep her money safe and she made transfers from her Revolut business account to these new accounts. In total she made the following transfers as a result of the scam, those in bold being her payments to the fraudster:

Date/time	***Payee***	***Value***
16/12/2023 14:03	*-*	*All funds within the account ($4,586.69) exchanged to GBP.*
16/12/2023 15:04	*External account belonging to G*	*+£4,800*
16/12/2023 15:27	*Ms B's personal account with Revolut*	*+£6,400*
16/12/2023 15:51	*External account belonging to G*	*+£9,822.23*
16/12/2023 15:52	*External account belonging to G*	*+£9,700*
16/12/2023 16:05	***Scam account 1***	***£100***
16/12/2023 16:07	***Scam account 1***	***£24,900***
16/12/2023 16:10	***Scam account 2***	***£100***

16/12/2023 16:11	***Scam account 2***	***£9,100***

Ms B has said at one point she began to doubt what she was doing, but the fraudster told Ms B that to reassure her, they would send a text. Ms B then received a text message on an existing thread of messages between her and Revolut, confirming that Revolut was working with her other bank to secure her account. This again provided Ms B with reassurance about what she was doing.

However, when Ms B attempted to send further funds across from her other account provider, this bank blocked her online banking and requested to speak to Ms B. During the call, the fraudsters asked to listen in via another phone. Ms B began having doubts again and entered her 'new' banking details on another of her banking apps. At this point she identified the accounts she was sending funds to weren't held with any of her own banking providers. Before being provided with any scam warnings or questioning by her bank, Ms B realised herself she'd fallen victim to a scam.

Ms B contacted Revolut to raise a claim. Revolut considered Ms B's claim but didn't agree it was liable to reimburse her. It concluded that as payments were initiated and authorised by Ms B, it had provided warnings to her during the payment process that it considers were proportionate and appropriate, and that Ms B failed to conduct appropriate due diligence. It also attempted to recover Ms B's funds, but was unsuccessful.

Ms B remained unhappy and referred her complaint to our service. An investigator considered the complaint but didn't uphold it. She determined that even if Revolut had done more to protect Ms B during these payments, it wouldn't have been able to stop the scam from happening.

Ms B disagreed with the investigator's view, so 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 Ms B 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 Ms B 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 December 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 EMIs 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.*

---

[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_/

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 "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 December 2023 that Revolut should:

- *have been monitoring accounts and any payments made or received to counter*

---

[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)

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).*

Should Revolut have recognised that Ms B was at risk of financial harm from fraud?

It isn't in dispute that Ms B has fallen victim to a cruel scam here, and whilst I have set out in this decision the circumstances which led Ms B to make the payment transfers using her 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 Ms B might be the victim of a scam.

When Ms B made the first scam payment, this was low value and not out of character for the account – so I don't think Revolut ought to have identified at this point that Ms B was at risk of financial harm from fraud.

However, when Ms B made the second payment of £24,900 towards the scam, I think there were several indicators at this point that Ms B may have been at risk. Prior to any payments having been made, Ms B had exchanged all funds within her business account from USD to GBP. She had then made four payments into the account, all of notable sizes, from two different accounts. Ms B was then attempting to make a payment to an account where she had entered G's details as the account holder, but where Revolut was able to identify that this account name did not match the account details.

By transferring sizeable amounts into the account from different external accounts, followed by attempting a large payment out to a new payee (where the account details provided didn't match the account), I think that by the £24,900 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 Ms B?

When Ms B made the transfer from her personal account to her business account, Revolut provided 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 Ms B was making the payment for and Ms B selected

'transfer to my other account.' As a result, Revolut asked Ms B some further questions, via a questionnaire, which she responded to as follows:

Is anyone prompting or guiding you? Answer: No, I am not being guided.

If someone is telling you to ignore these warnings, they're a scammer

Only continue if you're sure that you are not being prompted into making a payment.

Why are you making this transfer? Answer: Transfer to my other account – foreign exchange or money transfer.

Have you been asked to install software?

Scammers might ask you to install software (eg. Anydesk) to view your screen and help you to set up your investment account. Answer: No, I was not asked to install any software.

Were you told your account isn't safe?

Fraudsters will lie, telling victims their account is no longer safe and that they need to move their funds to another account. Answer: No, I was not told my account isn't safe.

Is the transfer to an account you control?

Scammed customers can move funds to an account they don't control and lose their money. Answer: Yes, it's my existing account.

Ms B was then shown a 'story' based warning, each screen providing different information about scams. The screens stated:

'This could be an impersonation scam

STOP: Fraudsters pretend to be financial institutions and panic you to act fast!

Be wary of unexpected calls

Clever scammers can impersonate bank agents and phone numbers. If in doubt, hang up and contact the bank yourself.

Don't give anyone remote access

Scammers may ask you to install software to view your screen. Uninstall software that gives someone else control

Told your account isn't safe?

Financial institutions don't ask customers to urgently move funds. Do not transfer to an account you didn't open yourself

Never ignore these warnings

Scammers will tell you to ignore warnings. If you've been told to ignore these red flags we've raised, then stop, it's a scam.'

Ms B was then routed to Revolut's in-app chat facility. Ms B was asked why she was making the transaction in question and she confirmed she was transferring funds between her own accounts.

Revolut replied to say:

'Thank you for your confirmation. Scammers may impersonate Revolut, another bank or the police and pressure you to make a payment urgently, telling you to ignore our alerts. Never ignore these alerts, even if someone tells you to.

Please stop and let us know if you are concerned for your account safety.

It seems like this isn't a case where someone is instructing you what to do, which can be a red flag for scams.

Could you confirm that you aren't being guided to make this transaction in any way?'

Ms B replied 'I can confirm I'm not being guided'.

Revolut then stated:

'I can see that you mentioned that you're moving money to one of your other accounts. Fraudsters may contact you telling you your account is unsafe and you need to move money fast. If someone created this account for you and assisted you to create the account using remote access software then stop.

Could you please confirm that you have NOT received contact from anyone asking you to move your money?'

Ms B replied 'yes, I can confirm'.

As a result, Ms B was allowed to transfer the funds from her personal account to her business account.

When Ms B attempted to make the first payment of £100 to the fraudster, she was again asked to confirm she knew and trusted the payee.

For the second payment, Revolut again held the transaction and asked Ms B the payment purpose. This time Ms B selected 'payment for goods and services' and, as a result, was provided with an irrelevant warning to the scam she was falling victim to.

Lastly, before agreeing to make the transfer, Ms B was shown a screen that stated:

*'**This transaction could be a scam***

Before transferring money, please be aware that:

1. *fraudsters can fake phone numbers to impersonate an organization*
2. *Revolut Business will never call you without verifying via the in-app chat*
3. *Revolut Business will never tell you to move your money into a new 'safe' account*
4. *Asked to ignore this warning'*

Ms B selected to agree and make the transfer.

For payment three, Ms B was again asked to confirm she knew and trusted the payee. There were no scam warnings for payment four.

Clearly Revolut made several attempts here to assure itself that Ms B wasn't falling victim to a scam – and under the fraudster's instruction, Ms B wasn't honest in her responses. However, the majority of warnings it presented to her were in questionnaire, or passive review formats. When she made the payment of £24,900 to the fraudster, I don't think this form of questioning was proportionate in the circumstances, particularly given banks' awareness that customers can be told to conceal matters from them. 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.

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

When Ms B made the payment of £24,900 towards the scam, based on the payment value and the account activity prior to this payment, in order to assure itself that Ms B wasn't falling

victim to a scam, I think Revolut ought to have spoken to Ms B via in-app chat to understand the payment further.

I don't think it was sufficient for Revolut to asked Ms B 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.

Additionally, as I've referenced, I think the overall picture painted by Ms B's account activity was that the greatest fraud risk here related to safe accounts (based on large payments being made 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.

If Revolut had provided a warning of the type described, would that have prevented the losses Ms B suffered from payment two?

I accept here that it's entirely probable that had Ms B spoken to Revolut via in-app chat about the £24,900 payment, the fraudster would have guided her on what to say – and it's also likely that she would have initially followed this guidance based on her responses to previous questioning by Revolut.

However, I also have to bear in mind that when Ms B was asked by her other banking provider to call to unblock her account, she realised without any input from her bank that she was being scammed, largely because the fraudster wanted to listen into her call with them. She's also explained she identified other red flags during the process, but that the fraudster had been able to overcome these concerns.

Therefore I think this paints a picture that Ms B wasn't so 'under the spell' of the fraudster that she couldn't have been reasoned with, if there was sufficiently meaningful warnings provided. I've also had to bear in mind that while Revolut uses an in-app chat, rather than phone as it's primary communication method, I would still expect this tool to be used in a way to overcome the possibility that customers may be on the phone to fraudsters and being guided – and sufficiently challenge that to overcome the external pressure caused.

I've also factored in that when Ms B initially spoke to Revolut via in-app chat, she was moving her funds from one of her trusted accounts to another, so the identifiable risk here was lower. Whereas when she was making the scam payments, there was more cause for her to be concerned about what was happening. I've also considered that in any chat Ms B would've had with Revolut, before a conversation even started Revolut would have valuable information at hand to be able to question Ms B's actions – she was making a payment for 'goods and services' and yet the account details she'd entered was her own business' name – and the actual account name didn't match this. I think these facts would've been an ideal starting point to begin a conversation from – and providing some clarity here that this account was not in her business' name would've had a real impact – as would providing context on safe account scams and how they unfold in a more personable, interactive format.

I appreciate that this is a finely balanced case – Ms B did mislead Revolut during questioning and bypass relevant information provided in warnings – but she also uncovered the scam herself with just some space to reflect. Having considered the circumstances holistically, I think the evidence suggests it's most likely that this outcome could have been reached sooner with a more meaningful interaction from Revolut.

Should Ms B bear any responsibility for her 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.

While I've set out my reasoning for how and why Revolut should have done more to protect Ms B, I also accept there was information provided to Ms B from Revolut that was relevant to the scam in question that she bypassed, albeit under the influence of the fraudster. I think Ms B could also have acted with greater caution when proceeding through the warnings provided and further questioned what she was doing in light of some of the information she was shown.

Therefore, considering the complaint holistically, I think it would be fair and reasonable for Ms B to also be partially responsible for her losses and I think a fair split of liability is 50/50 between Ms B and Revolut, from payment two to the scam onwards.

Could Revolut have done anything else to recover Ms B's money?

Revolut has confirmed it attempted to recover Ms B's funds the same day she reported the scam, but was unsuccessful. I therefore think Revolut took reasonable steps to recover Ms B's funds.

My provisional decision

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

- *Refund 50% of Ms B's losses to the scam from payment two onwards, totalling £17,050;*
- *Apply 8% simple interest from the date the payments were made, until the date of settlement.*

Revolut confirmed it had nothing to add to my provisional decision and would await the final decision. Ms B accepted liability on both sides of the complaint, although raised whether liability should be more heavily weighted towards Revolut. She referenced an earlier payment she had received, where Revolut applied much more scrutiny before allowing the payment to be released.

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've considered Ms B's comments that liability should be placed more heavily on the side of Revolut. I understand Ms B's strength of feeling, and why she feels Revolut could have done more – and I agree with her on this point which is why I've determined that Revolut could have stopped the scam. However, I think there were also actions Ms B could also have taken to stop the scam – so having considered the matter holistically, I remain of the opinion that an equal share of liability is a fair outcome in the circumstances of this complaint.

My final decision

My final decision is that I uphold this complaint in part and that Revolut Ltd should:

- Refund 50% of Ms B's losses to the scam from payment two onwards, totalling £17,050;
- Apply 8% simple interest from the date the payments were made, until the date of

settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask G to accept or reject my decision before 29 July 2025.

Kirsty Upton
Ombudsman