DRN-5255912

The complaint

R is a limited company. It complains that Revolut Ltd ('Revolut') won't refund the money it lost as a result of a scam and about the service it received once the matter was reported.

It is being represented by one of its Directors who I'll refer to as 'Miss T'.

What happened

The background to this complaint is known to both parties, so I won't repeat all the details here. In summary:

- The scam began with another Director at R who received a phishing text and was then called by someone claiming to be from Revolut's fraud team. Miss T says she became involved when the contact was passed on to her as the named person on R's business account which had allegedly been compromised.

- A fake 'authentication code' was first sent to her mobile apparently to show the identity of the 'advisor' she'd be speaking to. She was then called by a scammer claiming to be from Revolut's fraud team working with the Financial Conduct Authority. And was led to believe they'd be helping her to keep R's money safe.

- Several calls were held with the scammer over about seven hours on 10 November 2023. But the contact relating to the payments lost from this particular account happened over roughly the first two hours from about 13:15. The initial calls came from a number on Revolut's website and the fake 'authentication code' appeared in the same thread as genuine messages from Revolut (a tactic known as 'spoofing'). Messages with legitimate OTP codes to process the payments were also sent to Miss T's mobile.

- Miss T says all this made the scam convincing. And that the transactions from R's account were all carried out by the scammer using remote access software she'd been instructed to download to her laptop and mobile. She says that she was, at times, asked by the scammer to be away from her laptop as it needed to be away from her mobile to avoid a *"data exchange".* And that when she saw the first two payments (as listed below) had left the account, without her knowledge, she shouted at the scammer. But was persuaded it was all part of the plan to keep R's money safe.

Below are the transactions I've considered in this complaint. To note, the transactions (in *italics*) were returned to R's account on 10 and 15 November 2023. And the scam calls and more scam payments continued until about 19:30 from other accounts beyond those listed here. A separate complaint is being considered about that under a different reference.

	Date	Time	Type	Payee name	Amount
1	10-Nov-23	13:43	Transfer	R (scam a/c)	£30,000
2	10-Nov-23	13:44	Transfer	R (scam a/c)	£11,400
3	10-Nov-23	14:09	Transfer	R (scam a/c)	£5
/	*10-Nov-23*	*14:57*	*Credit*	*R*	*£30,000*

4	10-Nov-23	15:06	Transfer	SR Ltd (scam a/c)	£29,300
/	*15-Nov-23*	*15:14*	*Credit*	*R*	*£11,400*

The scam was reported to Revolut on 10 November 2023. A formal complaint was raised and then referred to our Service. Our Investigator considered it and upheld it. She thought that although the payments in dispute should be treated as 'authorised', Revolut ought to have identified R was at risk of financial harm and intervened on payment 1 – and that, if it had, the scam would have likely been unravelled. She also concluded R should share equal liability for the losses, such that the refund Revolut needs to pay can be reduced by 50%.

As the matter couldn't be resolved informally it's been passed to me to decide.

Provisional decision

I issued my provisional decision to both parties on 20 December 2024. The background to the complaint was set out as above and I said I intended to uphold this complaint. I provided the following reasons:

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

Authorisation

The first two payments (1 and 2 above) were, according to Revolut, returned to the account by the receiving firm. As such, they don't represent a loss to R. I've therefore considered whether the next two payments (3 and 4) should be treated as authorised, in line with the relevant regulations – the Payment Services Regulations 2017 (PSRs).

This is important as R would generally be liable for authorised payments and Revolut for unauthorised ones. And, as set out in the PSRs, a payment would broadly be deemed as authorised if the account holder consented to it being made or gave their consent for someone else to make it.

In this case, Miss T gave the scammer access to her mobile and laptop. And she'd have had to log into R's account for the scammer to access, albeit under false pretences. I note Miss T says all the transfers were made by the scammer. But I've seen that genuine text messages with OTP codes were also sent to a mobile in her possession. It's clear from these that the transfers had been initiated to leave R's account and had to be 'authenticated' in-app before being processed. I understand this step wouldn't have been possible through remote access at the time as Revolut didn't allow remote access in-app and limited the functions that could be performed on its website (such as restricting the ability to add new payees).

Even if I were to accept Miss T's comments that the scammer took all the steps required to make the transfers, I still wouldn't be persuaded they should be treated as unauthorised. As above, remote access was given for the scammer to act and it was clear the OTP codes Miss T received were needed to confirm the transfers. The premise of the scam, according to Miss T's testimony (and particularly by payments 3 and 4), was that money had to leave the account to keep it 'safe'. I can't overlook, for example, in the scam report to Revolut she said: "I was on the phone with 2 people…who asked me to move money around a few times" and "he gave me a speech that they were moving money as it was already set to leave the account by the hackers so they had to save it". In the Police report "they [the scammer] claimed they were moving money…they needed to keep it safe elsewhere".

I accept Miss T was tricked into believing the money had to leave as part of an elaborate scam involving 'spoofing' techniques. I don't imagine she'd have gone along with any of it if she thought she wasn't speaking to Revolut. But when it comes to authorisation, the PSRs don't distinguish between payments made with full knowledge and those made under deception. As I'm satisfied she understood money would be leaving R's account (under the false reasons given) and the transactions couldn't have been made without the OTP codes being provided in-app, under the PSRs the transactions would be deemed authorised.

Prevention

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 (the 2017 regulations) and the terms and conditions of the customer's account. And, as the Supreme Court 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 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 wasn't the same as being under a legal duty to do so.*

In this case, the terms of Revolut's contract with R 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 R and the PSRs to carry out its 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'm satisfied, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time that, by November 2023, it should 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).

---

[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).

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'm mindful that in practice all banks and EMIs 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'm also mindful that:

- *EMIs (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 ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken in the course of the relationship). I don't suggest 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 (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).*

---

[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"

- *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].*

To summarise, 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 that in November 2023 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).*

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

There's no dispute R was scammed. And, whilst I've set out the circumstances that led to the payments being lost to a fraudster, I realise Revolut had much less information available to it on which to discern if any payments presented an increased risk that R might be the victim of a scam. I also note Revolut's comments that this was a business account, it expected frequent transfers of various amounts, and the disputed payments didn't therefore stand out.

But I've considered the above against the fact that the account was not newly opened and Revolut had material account history on which to assess the level of risk presented by the disputed payments; payment 1 itself was for a considerable amount; it was significantly higher than any payment that (according to the statements provided) had been made from R's account in previous months; and it was also to a new payee.

Taking these factors into account, I think payment 1 carried an elevated risk of financial harm from fraud and I'd have expected Revolut to have provided a warning that was proportionate to the risk it presented. I'll add here that subsequent payments arguably also presented a risk – payment 2 was made in quick succession after the first, to a new payee,

---

[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)

leaving a small balance on an account that had typically held much more. And payment 4 (representing most of the loss), again almost emptied the account just over an hour later.

What kind of warning should Revolut have provided?

Revolut says its systems flagged payments to newly added beneficiaries and it provided the following in-app warning for payment 1 (£30,000) and payment 4 (£29,300).

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

It also says these payments were placed on hold and were only processed after 'goods and services' had been selected as the 'payment purpose'; a warning had been shown that was relevant to that payment purpose; and Miss T was given the option to read its scam guidance or speak to one of its advisors if suspicious.

As mentioned earlier, Miss T says the transactions from R's account were carried out by the scammer using remote access. She also says she didn't see any of the warnings Revolut says were given. Given what I understand about Revolut's security measures, I'm not fully convinced that the warnings were dismissed by the scammer without Miss T seeing and I don't discount them entirely. I note they contain some information relevant to what was happening. That said, I don't think the steps Revolut took to prevent fraud went far enough here. I don't think the warnings it gave were a proportionate response to the risk presented by payment 1. And I think these were too generic to have the necessary impact unless Miss T already had doubts about who she was speaking to (and I don't think she did at that point).

In my view, thinking about the risk presented by payment 1 (and, given what I said above, arguably payments 2 and 4 also), a proportionate response would have been for Revolut to have contacted Miss T directly (for example, through its in-app chat) to discuss things and attempt to establish the circumstances of the payment before allowing it to debit the account.

If Revolut had attempted to establish the circumstances on payment 1, would the scam have come to light and R's loss been prevented?

I'm satisfied that if Miss T had told the 'genuine' Revolut she was being assisted to keep R's money safe from 'hackers', then it would have immediately recognised the hallmarks of a scam. I'd have expected it to provide a very clear warning about what the situation looked like. And, given that Miss T had no desire to lose R's money, it's likely she would not have gone ahead with allowing more payments and R's losses would have been prevented.

I appreciate the success of such an intervention would have been partly dependent on what Miss T would have revealed in answer to Revolut's questioning. I've thought about this carefully, including Revolut's comments that an intervention may have been intercepted and the scammer's 'spell' was such that Miss T would have likely continued anyway.

But, as part of an intervention, I'd have expected Revolut to have satisfied itself it was communicating with its customer. And from what Miss T has said, it seems to me much of her trust in the scammer was a result of her receiving a fake 'authentication' code (in the same thread as genuine messages from Revolut) and calls from a spoofed number. I've seen little to make me think Miss T was prepared to deliberately deceive Revolut itself or was given much of a cover story (particularly at payment 1) other than that R's account was at risk and a Revolut 'advisor' was acting to secure it. So, I think she'd have likely answered honestly to contact from Revolut. And when thinking about the type of questions I'd have expected it to have asked (for example, what is the payment for? how do you know the

payee and the recipient details?) I think it's more likely than not that this interaction would have led to Miss T realising something was wrong. I'm also not convinced she'd have responded in a way that would have likely satisfied Revolut there was no risk either.

In other words, I think Revolut missed an opportunity here to unravel the scam. I'm not persuaded payments would have continued out of the account after a human intervention and a clear warning around what the situation looked like at that point. If Revolut had taken proportionate steps to probe and establish the situation around payment 1 and explained, as a minimum and in direct contact, that it'd never ask its customers to move money and phone numbers can be spoofed, I think it's likely Miss T would have realised something was wrong; the scam would have been unravelled; and R's losses would have been prevented.

Should R bear any responsibility for the losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what I consider to be fair and reasonable in the circumstances.

I've thought about what Revolut has said on the warnings it provided and that, if Miss T had properly checked the number she was called from, she'd have seen Revolut doesn't make outgoing calls from that number. I note an online search brings up results simply showing the number belongs to Revolut while one links to a spoofing blog by Revolut. I also accept that, in hindsight, there were some red flags that ought to have caused concern (some of which Miss T herself had identified) – such as the first payments being made without her knowing; the request to be away from her laptop; and funds being sent externally and to a different named third-party. At the same time though, I think it's important to keep in mind that:

- *Miss T was in an induced state of stress and panic when the payments were made. I don't underestimate the stress that can be caused by these types of calls and the panic they're meant to generate in the people who receive them.*

- *The tactics used by scammers are common, but nonetheless captivating to anyone unfamiliar with them. I can appreciate why the calls and fake 'authentication code' from spoofed phone numbers made Miss T think she was genuinely dealing with Revolut.*

- *Miss T says the transactions were carried out by the scammer and that the first two were made when she was out of the room. I can see the first three payments were sent with 'R' as the named payee and the reference 'cashback'. This was consistent with what the scammer was telling Miss T would happen. I can also see that before payment 4 was made, R's account was 'credited' with the first transfer of £30,000. This was an event Miss T says the scammer then used to further convince her that the intention was always to return the money to R and that this was all part of the plan to defeat the 'hackers'.*

- *Miss T spent about two hours on the phone to the fraudster by the time the last payment came about. I don't think this gave her the chance to reflect on what she was being told. And even if Miss T did engage with the warnings Revolut says were shown (something she disputes), I don't think the warnings provided sufficient context for me to conclude it was unreasonable for Miss T to have moved passed them in those circumstances.*

Overall, Miss T clearly didn't want to lose R's money. She was put under a state of panic and believed what she was being told by a fraudster using sophisticated techniques. I don't find her belief to have been unreasonable. And I don't find she acted carelessly or ignored clear warning signs in a moment of stress and panic such that it would be fair to reduce an award.

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

A business is generally expected to attempt recovery of funds once the scam has been reported. In this case, Revolut hasn't provided evidence of its attempts at recovery. However I've received information to indicate the disputed payments were utilised within minutes of them crediting the recipient account. It's therefore unlikely there was any prospect of it successfully recovering R's money by the time the scam was reported.

Distress and inconvenience

There's again no dispute that R's money was lost to a scammer and I'm sorry about the impact the whole experience has had on Miss T. But as the Investigator explained, R is the customer and, as a limited company, R itself can't suffer 'distress'. So, I can't award for the stress Miss T (and other individuals) suffered as a result of Revolut's actions or inactions.

I can make an award if I think R was inconvenienced. But I consider that much of the inconvenience, including the time spent in dealing with what happened, was a result of the scammer's actions in what was a sophisticated scam. And while I recognise Miss T was unhappy with Revolut's investigation into the claim and its outcome, I don't think, having looked at how it was handled, the service provided was so poor to warrant an award.

Once the scam was reported, Revolut took steps to gather the information it needed to assess the claim and replied within six days with its reasons for not offering a refund. It explained it was treating the payments as authorised and if Miss T didn't hear back within 21 days, recovery had failed. A complaint was raised days later and a response was provided, giving Miss T rights to our Service if she remained unhappy. This was in line with what I'd expect to happen.

Putting things right

I think Revolut Ltd ought to have intervened on payment 1. If it had done so, it's likely none of the payments would have been made. And I don't think there should be a deduction for contributory negligence here. As such, bearing in mind that both payment 1 and payment 2 do not represent a loss to R, I'm minded to direct Revolut Ltd to:

- *Pay R, the total loss resulting from payments 3 and 4; and*

- *pay 8% simple interest per year on that amount from the date of the payments to the date of settlement.*

Responses to provisional decision

I invited further comments and evidence from both parties. I explained that the deadline to provide any further comments or evidence for me to consider was 10 January 2025 and that, unless the information changes my mind, my final decision would likely be along the lines set out in my provisional decision.

Miss T responded (on behalf of R) to say she doesn't wish to submit any more information for me to consider. Revolut hasn't responded by the deadline given.

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 as neither party has provided any new information for me to consider, I

see no reason to depart from the findings I reached in my provisional decision, as set out above. In the circumstances, and for the reasons given, I uphold this complaint.

Putting things right

To put things right, I direct Revolut Ltd to:

- Pay R, the total loss resulting from payments 3 and 4; and

- pay 8% simple interest per year on that amount from the date of the payments to the date of settlement.

If Revolut Ltd considers it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell R how much it's taken off. It should also give R a tax deduction certificate if requested, so that tax can be reclaimed if appropriate.

My final decision

For the reasons given, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask R to accept or reject my decision before 10 February 2025.

Thomas Cardia
Ombudsman