

Complaint

Mr T is unhappy that Revolut Ltd didn't refund him after he told it he'd fallen victim to a scam.

Background

In April 2022, Mr T fell victim to a scam. He received a call from someone who claimed to be an employee of a bank I'll refer to as 'P'. Mr T had an account with P, and so did his wife. The caller claimed they worked in P's fraud team. They went through a series of transactions that had apparently been attempted on Mr T's card and asked whether he was responsible for them. He said that he wasn't. The caller told him that this meant his account had been targeted by someone attempting to steal his money. Unfortunately, this call hadn't been made by a genuine employee of the bank, but a fraudster. It's significant, however, that the number that had called Mr T was genuinely one connected to P.

I understand the fraudster told him they could cancel those attempted transactions, but that he needed to move his money somewhere safe. He says the scammer knew that he had a Revolut account – he was told to put his money there while he waited for a new, safe account with the bank to be created. The fraudster also told him that the security of Mrs T's funds was similarly compromised, but that she could keep her money safe by putting into the Revolut account too. Importantly, the caller also persuaded Mr T that the person attempting to steal money from their accounts could be an employee of the bank.

Mr and Mrs T made two payments to the Revolut account. On both occasions, P queried the payments. They'd been prepared for this. They told the caller from P that they were transferring the funds to pay for a holiday. Mr T says that he was suspicious about these calls, because the quality of the line was poor and the callers sounded like they were calling from an overseas call-centre. Having been told that his money might be under threat from someone inside the bank, it made him consider the possibility that the person calling him might be connected to that attempt to defraud him.

The same day Mr T decided to contact P directly to ensure that this arrangement was above board. He explained the situation – i.e., that an employee of P had contacted him and told him to transfer his money to a Revolut account while waiting for his new P account to be set up. He mentioned that the call had come from a recognised number that was connected to P. Unfortunately, the person he was speaking to told him that, if the call had come from an authentic contact number for P, it was most likely that the enquiry had been a genuine one.

The following day the fraudsters contacted Mr T again. They told him that a new account had been set up. They provided him with an account number and sort code and told him to transfer the balance of £20,000 into the new account as soon as possible. Mr T did so.

Once Mr and Mrs T realised they'd fallen victim to a scam, they notified P. It agreed to refund a little over 50% of the money they'd lost. Revolut, however, didn't agree to pay a partial refund to Mr T. It said it had displayed warnings when Mr T was making the payment. Mr T wasn't happy with the response from Revolut and so he referred his complaint to this service. It was looked at by an Investigator who upheld it. She concluded that Revolut ought to have regarded the £20,000 payment as out of keeping with the typical way the account

had been used and taken some steps to warn Mr T about the risk of fraud. If it had provided him with a tailored warning about this type of scam, she was persuaded that it would've prevented him from going ahead with the payments.

Revolut didn't agree with the Investigator's view. It said:

- Mr T authorised the transaction and it processed it, as it is required to do under the relevant regulations.
- If P told Mr T that the scammer's call was likely genuine then P should be liable, not Revolut.
- In being taken in by the scam, Mr T was negligent. It noted that he was the director of a limited company and, in its view, it's unlikely that a customer of such "*calibre*" would fall for a scam like this one, except if he had acted recklessly.

Since Revolut disagreed with the Investigator's view, the case has been passed to me to consider and come to a final decision.

Findings

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 customer'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 T 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 T and the Payment Services Regulations to carry out his instructions promptly, except in the circumstances set

out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

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

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in April 2022 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

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

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

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

- Electronic Money Institutions like Revolut are required to conduct their business with *“due skill, care and diligence”* (FCA Principle for Businesses 2), *“integrity”* (FCA Principle for Businesses 1) and a firm *“must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”* (FCA Principle for Businesses 3)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

¹ The Payment Services Regulation 2017 Reg. 86 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/

³ Since 31 July 2023 under the FCA’s new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

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, the BSI Code⁴, 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).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

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 April 2022 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- 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); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Revolut have recognised that Mr T was at risk of financial harm from fraud and were the steps it took to warn him sufficient?

I recognise that, in cases like this one, Revolut is in a more difficult position in respect of identifying fraud risk as compared with, for example, a high street bank. This wasn't Mr T's main account for day-to-day spending and so it didn't have data on his spending patterns and behaviour to use as a basis of comparison when determining whether any individual transaction appeared to have an associated fraud risk.

⁴ BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

However, after a lengthy period of inactivity (several years), a payment of £20,000 would obviously appear unusual and out of character. In view of that, I'm persuaded that Revolut ought to have identified that payment as carrying a heightened risk of financial harm from fraud and it ought fairly and reasonably to have taken additional steps before allowing it to debit Mr T's account.

As I've already set out, Revolut did intervene by way of written warnings. That suggests it recognised some risk of financial harm from fraud. The payment request led to it providing him with a written warning. It said:

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'

The transaction was subsequently declined, and Mr T was presented with a further warning which said Revolut's systems had identified the transaction as being "highly suspicious." It went on:

"If you decide to make the payment again anyway, you can, and we won't decline it as we have warned you this transaction is highly suspicious and to not make the payment. If the person you pay turns out to be a fraudster, you may lose all your money and never get it back. You can learn more about how to continue with this payment and protect yourself from this link"

I've considered this carefully, but I'm not persuaded that these written warnings were sufficient in the circumstances. At a high level, the first warning did attempt to warn against impersonation scams. However, Mr T didn't need to interact with it and it was written in quite general terms. It didn't cover off the key features of an impersonation scam, the common techniques fraudsters use to trick their victims (e.g., number spoofing) nor the types of institutions commonly impersonated. This lack of context and detail served to diminish its potential impact.

The second warning was generic. It explained that Revolut had identified the payment as highly suspicious. It didn't explain why. It included a link to find out more about scams. Making use of that information would've required Mr T to go off looking for information relevant to his circumstances in a scenario where he sincerely believed he was following the instructions of P.

Overall, I don't think Revolut's interventions were a proportionate response to the risk the payment presented. I accept it did take some steps to prevent harm from fraud, but the warnings were too generic to have had the necessary impact – unless Mr T had any doubt about the legitimacy of the payment request, which I'm satisfied he didn't.

Since the payment Mr T was making was so unusual and out of character, Revolut ought fairly and reasonably to have made enquiries about the payment he was seeking to make. It's not up to me to set out exactly how Revolut should've done this, but I think it ought to have been via a human intervention such as through its in-app chat function.

Would the scam have come to light and Mr T's loss been prevented?

I've thought very carefully about whether the type of intervention I've described would've prevented Mr and Mrs T's loss. In doing so I've considered the interactions Mr and Mrs T had with the fraudster and P. If Revolut had attempted to establish the circumstances surrounding the payment, I think it's more likely than not that Mr T would've disclosed the legitimate reason for the payment.

I say that, even though I acknowledge that he didn't do so when P called him. The way the scam had been set up meant that Mr T was suspicious of the fraud calls from P. In addition, he says he remembers those calls being made on a poor quality phoneline with static interference and that the callers appeared to be calling from an overseas call centre. He'd been told that the attempted frauds could be coming from anywhere, so he was sceptical as to whether he was really talking to P when they called him.

Despite that, the fraudster had consistently told Mr T that his money would be safe with Revolut. I've seen no evidence to suggest Mr T was told that Revolut could be party to the fraud and so I think he'd have considered it safe to disclose what he believed was the purpose of the payment in an in-app chat with a Revolut employee. I don't think he'd have had any doubt that he was sharing the facts with a genuine Revolut employee, just as he had when he proactively called P to check what he'd been asked to do was legitimate.

If this had taken place, Revolut ought to have promptly recognised the scam risk. It could then have explained to Mr T the commonly occurring features of scams of this type, including the use of number spoofing. He'd only been convinced that he was talking to a genuine employee of P because, during a call with one of its employees, they'd failed to recognise the possibility of fraudsters spoofing official bank telephone numbers. I think it's likely he'd have recognised the reality of the situation, particularly since he began by exercising some caution.

Is it fair and reasonable for Revolut to be held responsible for Mr and Mrs T's loss?

As I've set out above, I think Revolut should've recognised the fraud risk here, made further enquiries and, in so doing, prevented the payment from taking place. The fact that the funds didn't originate in his Revolut account doesn't change that. I think Revolut can fairly be held responsible for Mr T's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against the firm that is the origin of the funds.

I've also considered that Mr and Mrs T have only referred a complaint to us against Revolut. I accept that it wasn't the only firm involved here. However, they've accepted an offer in full and final settlement of their complaint against P, so it's not open to this service to consider that complaint.

Ultimately, the only outstanding complaint regarding these events concerns Revolut. Mr and Mrs T have referred that complaint to us and, in those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr and Mrs T's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr and Mrs T's outstanding loss.

Should Mr and Mrs T bear any responsibility for their 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.

Having done so, I'm not persuaded that they should bear partial responsibility for their losses. Mr T has shown that he did receive calls from spoofed numbers. Considered alongside the fact that an employee of P told him that those calls probably did come from a legitimate employee of the bank, I don't think it was unreasonable for Mr T to have believed he was genuinely talking to his bank and following their instructions to protect himself from fraud.

Revolut has argued that, since Mr T is a company director, he must have acted recklessly in falling for the scam. I don't accept that argument. It's worth noting that there are over 5 million active companies listed on the Companies House register and each of those companies is legally required to have at least one director. Given the prevalence of impersonation scams, the implication that a company director must be too savvy to fall victim to them isn't at all persuasive.

Impersonation scams like this one are among the more sophisticated. They rely on social engineering and the application of psychological pressure to frighten victims into compliance. It's for that reason that there's no obvious correlation between a person's risk of falling victim to such a scam and their professional status. Fundamentally, anyone can fall victim to a scam. Mr T did exercise some caution here. He contacted P to check that he was doing the right thing. The mistaken response to his query would've reassured him and I don't think that was unreasonable. Overall, I'm not persuaded that he acted recklessly or negligently here.

Other issues

I've also considered whether Revolut needs to pay any additional compensation to Mr T on the grounds that the way it handled things caused him distress and/or inconvenience.

There's no doubt that Mr T experienced an enormous amount of distress in falling victim to this scam. The bulk of that wasn't caused by Revolut, but by the fraudsters. Nonetheless, I think the way Revolut responded to him did make things worse.

I've looked at the transcripts of the chat between Mr T and a Revolut employee in which he reported what had happened. His distress at having lost such a large sum was apparent. Despite that, Revolut's agents repeatedly told him to "*have a great day.*" I think this was an unfeeling way of responding to a customer who had fallen victim to a crime and served only to rub salt in the wounds.

The Investigator recommended Revolut pay Mr T an additional payment of £150 in recognition of the distress caused by the way it handled things and I think that's a fair sum in the circumstances.

Final decision

For the reasons I've set out above, I uphold this complaint.

If Mr T accepts my final decision, Revolut Ltd needs to:

- Refund the payment he made in connection with the scam, less the funds that were recovered and the settlement he received from P.
- Add 8% simple interest per annum to that sum calculated to run from the date the payment left his account until the date any settlement is paid.
- Pay him £150 in recognition of the distress it caused him.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 27 January 2025.

James Kimmitt
Ombudsman