

## **The complaint**

Mrs A complains that Revolut Ltd hasn't refunded her after she fell victim to a scam.

## **What happened**

The background to this complaint is well-known to all parties, and so I'll only provide a brief summary of events here.

Mrs A received a text which appeared to be from her bank – which I'll call L. The message appeared in a string of previous texts received from L and appeared to come from the same number. To Mrs A it looked genuine. But it had been sent by a scammer using a technique called number spoofing.

The text message said that a payment was being processed and that it required further authorisation. Mrs A knew she hadn't made the payment and so was immediately concerned her account was under threat. She called the number given within the text message. This in turn prompted a call from an unknown number, presenting on the phone screen as 'No Caller ID'.

Mrs A answered and the person claimed to work for L, where they were in fact a scammer. They said they were getting in touch to help protect Mrs A's account. After going through some security questions, the scammer said that Mrs A should move all of her money in order to keep it safe. She was convinced to transfer it from L to Revolut and was told a new account would be set up for her. Mrs A was then told to transfer the money to that new account, which is when it was lost to the scammers. The money was sent across three transactions, all within six minutes: £100, £250, and £23,000.

Mrs A realised she'd been scammed the next day, after the panic had subsided somewhat and she checked her online banking. She reported what had happened to Revolut and asked it to help get her money back.

Revolut looked at what had happened and tried to recover the funds from the account they'd been sent to. But it could only recover less than £10. It then said it wouldn't refund the loss as Mrs A had authorised the payments and it had given warnings about scams. It also felt Mrs A hadn't done enough to ensure the people she was in contact with were legitimate.

## **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.

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 Mrs A modified the starting position described in *Philipp*, by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with Mrs A 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<sup>1</sup>. 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 May 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;<sup>2</sup>

---

<sup>1</sup> 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).

<sup>2</sup> 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/>

- 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)<sup>3</sup>.
- 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<sup>4</sup>, 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).

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 May 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is

---

<sup>3</sup> 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.

<sup>4</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

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).

*Should Revolut have recognised that Mrs A was at risk of financial harm from fraud?*

The first two payments made by Mrs A were low in value and unremarkable. And so it would not be fair and reasonable to say that Revolut ought to have recognised a risk of financial harm from fraud.

Payment three, however, was much larger. It was of such a high value that I'd expect it to have been seen as a risk in many circumstances. Here, specifically, it was the third payment in quick succession – just six minutes – to a newly created payee, with the payment values having increased quickly. This matches the common features of a safe account scam, which is what Mrs A was caught up in.

It's also true that the payment represented significantly unusual account activity. The account had been open for a long time and was used regularly. But that usage involved low value card payments and little else. I can't see there were any faster payments out of the account in the previous twelve months and there are no transactions even remotely close in value to the third payment made toward the scam. So the account activity marked a significant shift away from the norm, and Revolut ought to have linked that to an identifiable scam risk.

Revolut also knew that the name given by Mrs A on the payment instruction didn't match that on the receiving account. This ought to have been factored into the risk profile and given Revolut further cause for concern.

Revolut were also concerned about the sudden credit of £23,800 into the account. I believe it was right to be and it sent Mrs A an email asking about the source of funds. It ought to have also used this information, given it had detected unusual account activity, to assess the risk that a scam was taking place. This is another common feature of a safe account scam – where unusually large sums are transferred into an account – that Revolut ought to have acted on.

*What did Revolut do to warn Mrs A?*

Mrs A was shown two warnings when she first set up the payee used for the scam. The first was presented because Revolut could tell the account name stated on the payment instruction didn't match the recipient account. This is known as a confirmation of payee warning. It said:

***Account name doesn't match***

*The recipient's bank told us the name you entered is not the name on the account. Please double check the details and only continue if you're sure the recipient is trustworthy.*

Mrs A was able to proceed by clicking 'keep what I entered'.

She then set up the first payment and was resented with the following warning.

***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.*

Mrs A clicked to proceed, rather than cancel the payment. No warnings were presented for the second payment.

When it came to the third payment, Revolut recognised an increased risk and so presented the following messages across two different screens:

***Victims lose millions every year. In 2020, in the UK alone victims lost £479m to bank transfer scams. It's important that you take care and do your research before making a payment as once funds have been received by a fraudster, they're difficult to get back.***

***Fraudsters are professionals. They'll try to trick you into sending them money by pretending to be someone you trust. They can make their calls, emails and advertisements seem legitimate.***

Mrs A was then required to select a payment purpose from a list. She selected 'Something else'. I'll note here that 'transfer to a 'safe account' was an option.

Mrs A was then presented with three more warning screens in succession:

***Stop! This transaction has been flagged as suspicious. Take a few minutes to consider the situation before parting with your money.***

***Don't ignore warnings. Scammers pressure and persuade you to ignore our warnings. If you are being told to ignore warnings such as this, then it's a scam.***

***We won't call you to move money Revolut, banks and financial service providers will never ask you to move money to a different "safe" account.***

Mrs A then had to digitally sign what Revolut calls a 'risk agreement. It states:

*Revolut has warned me that this payment is suspicious and I understand the risk of losing my money.*

Mrs A signed the in-app form and clicked to send the money.

*What kind of warning should Revolut have provided?*

Given the identifiable scam risk, I'm satisfied a proportionate response would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs A's account. I think it should have done this by, for example, directing Mrs A to its in-app chat to discuss the payment further.

That chat ought to have involved detailed and tailored questions, based around Revolut's professional knowledge of how common scams tend to work.

I don't find the warnings presented by Revolut represented a proportionate response to the identifiable scam risk.

*If Revolut had provided a warning of the type described, would that have prevented the losses Mrs A suffered from the third payment?*

I'm satisfied a human intervention, with a full and detailed scams discussion, would have made a difference here.

Mrs A could and should have been asked specifically what she was doing and why. There's been no indication or evidence to suggest that the scammer's had told Mrs A to lie to Revolut or that it couldn't be trusted for some reason. And so it follows that she would have told what she believed to be the truth.

That being the case, Revolut ought then to have been able to identify the common scam features that were present in these specific circumstances. That in turn ought to have led to a very strong, clear, and stark warning against proceeding. Arguably, Revolut ought not have let the payment go through at all, as it would never have been able to be satisfied that the money was going to an account in Mrs A's control.

I have taken account of the warnings Mrs A did receive in making the above findings. I've already said how they weren't sufficient in the circumstances, but I do also acknowledge that Revolut did take some steps to warn against scams. And some of the warnings do touch on some of the common features of a safe account scam.

Those facts do not lead me, however, to conclude that Mrs A would always have proceeded anyway, even if there had been a suitable intervention in the payments. The written warnings do not encourage or require significant engagement from a customer. And typically, in safe account scams, as was the case with Mrs A, the customer is in a highly emotional and panicked state. Mrs A has described how terrified she was that she was going to lose her money and how this led her to quickly move through the screens. Had Revolut suspended the payment and required an in-app chat, Mrs A would have been forced to engage fully and I'm satisfied the scam would more likely than not have been revealed, with any further loss prevented.

That being the case, I find it's fair and reasonable for Revolut to bear responsibility for Mrs A's loss of money from payment three.

#### *Should Mrs A 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.

I don't find it would be fair to reduce the reimbursement due to Mrs A on the basis of her own actions.

Key to this is the consideration of how the scam was set up. Mrs A received a text from L that appeared entirely genuine. It looked like the kind of text that might be received to confirm a payment being made. And, importantly, it fitted into the string of existing texts Mrs A had received from L. It's then entirely understandable why Mrs A was convinced the text was legitimate. Number spoofing is an incredibly powerful tool used by fraudsters.

It then follows that Mrs A subsequently trusted the interactions that followed. They were all linked to that first text. Whilst different numbers, including the 'No Caller ID' call, were then used the trust had already been solidly established.

On top of that trust was then layered panic and fear. Mrs A was understandably scared about losing money. In such circumstances it is both common and understandable for a person to not think as clearly as they otherwise might. This doesn't constitute negligence on their part.

I've also thought about Mrs A's broader circumstances at the time. She'd spent considerable time in hospital with her husband who was in intensive care following open heart surgery. She was understandably mentally and physically drained. In addition, she was concerned about getting home to fulfil other duties and responsibilities, meaning her mind was understandably preoccupied. All of these points contributed to her most probably being more susceptible to a scam of this nature at that moment in time.

I've considered the warnings that Mrs A was given during the scam, including the confirmation of payee warnings. But I don't find these mean that Mrs A's actions were unreasonable. I've already explained why the warnings given weren't sufficient. And given the trust established by the scammer, and the panic created, it's understandable why Mrs A continued with the payments and her actions were reasonable in the circumstances.

#### *Recovery of funds*

It appears Revolut did act quickly to try and recover Mrs A's money, but only £9.95 was left. That isn't surprising in the circumstances as typically funds are removed from the recipient account very quickly, often within minutes. Given Mrs A didn't report the scam until the

following day, it seems unlikely there was ever much prospect of the bulk of her money being recovered.

### **Putting things right**

On Mrs A's acceptance, Revolut should:

- Reimburse Mrs A £23,000 of her loss;
- Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

### **My final decision**

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 8 November 2024.

Ben Murray  
**Ombudsman**