DRN-5149444

Complaint

T, a limited company, complains that Revolut Ltd didn't refund its losses after it fell victim to a scam. This complaint has been brought by T's directors, Mr and Mrs H. For the sake of readability, I've generally referred to Mr and Mrs H in the text of the decision.

Background

T has an account with Revolut which is controlled by Mr and Mrs H. On 28 September 2023, Mrs H received a phone call from someone purporting to be from Revolut. The caller ID displayed a genuine Revolut number, and the caller told her that someone was attempting a fraudulent transaction on that account. Unfortunately, this wasn't a genuine call from Revolut, but a fraudster.

Mrs H tells us that she couldn't access the Revolut app on her phone as she was locked out. The scammer directed her to log into the account using her laptop, which she did.
From what she's said, she was then taken through a fabricated version of the Revolut chat service. She says it was indistinguishable from a genuine interaction with the firm and that, combined with the fact that the caller had demonstrated that his number matched an official Revolut number, persuaded her she was dealing with a genuine employee.

She said she was shown what appeared to be T's genuine account screen on her laptop. The scammer told her a payment of £18,700 had been attempted, and showed a red message that said *"cancel payment."* The scammer then appeared to cancel this transaction. Instead, a payment for that value was debited from the account. Around this time, Mr H also spoke with the scammer. He says he mentioned that he would login to his Revolut account using the mobile app, but the scammer insisted on using the laptop. When Mr H didn't agree to do so, the scammer ended the call.

Revolut said that a warning message was displayed at the time the payment was made, which Mrs H would have had to acknowledge to proceed. As the payment was being made to a new beneficiary, its system prompted Mrs H to confirm whether she knew and trusted the payee. Revolut said the payment was processed only after Mrs H acknowledged these prompts and confirmed the payment. It says she did this using her mobile device.

Mr and Mrs H complained that Revolut had failed to prevent the fraud from taking place. It looked into things, but it didn't agree to reimburse them. Mr and Mrs H weren't happy with that response and so they referred their case to this service. It was looked at by an Investigator who upheld it. Revolut disagreed with the Investigator's opinion, and so the complaint 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 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 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 T and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in September 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in

[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).

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.

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).

Overall, taking into account relevant law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in September 2023 that Revolut should:

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

[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"

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).

Was the payment authorised?

It's not entirely clear how this scam was carried out. Based on what Mrs H has told us, it seems likely that remote access software was involved, even though she doesn't recall downloading anything. The fact that the scammer ended the call when Mr H said he was going to use the app on his phone, rather than the laptop, suggests the scam likely relied on remote access to the laptop. This implies that continuing the interaction via the phone could have disrupted the scammer's ability to control what Mr and Mrs H could see.

I've taken on board what Revolut have said about the fact that it wouldn't have been possible for someone with remote access to Mrs H's laptop to make a payment from the account. It would've required that the payment be confirmed in the mobile app. Mrs H says that her Revolut account on her phone was locked and so she didn't do this. It's also noteworthy that, although Revolut has said that the payment was confirmed using a mobile device, the audit log it has shared with us only shows two devices interacting with the account and that both were using the Windows operating system.

In any event, the mechanics of how the scam was conducted aren't so important here. If I were to find that the payment was genuinely unauthorised in accordance with the PSRs, Revolut would be expected to refund the payment. However, even if I conclude that the payment was authorised, I still have to take into account all of things that I'd expect of Revolut in respect of spotting and preventing fraudulent transactions that I've described above.

I'm satisfied that Revolut should've been concerned about the risk of fraud in respect of this payment. In terms of its value, it was significantly out of keeping with the typical payments made from the account. I recognise that the threshold above which Revolut ought to be concerned might reasonably be higher for a business account. I've also taken into account that, when T's account was opened, Mr and Mrs H told Revolut they expected turnover of around £1 million. Nonetheless, the best information at its disposal to help it identify fraud risk was the existing payments that had been made from the account in the months since it opened. The fraudulent payment was in significant contrast to those. In addition to that, it was being made to a new payee and depleted the balance on the account almost entirely.

I don't think Revolut should've processed this payment without first taking some steps to protect T from the risk of financial harm due to fraud. I can see its systems provided a general warning, asking whether Mr and Mrs H trusted the payee. I don't think that warning was adequate in the circumstances. I think a proportionate response here would've been to temporarily pause the payment and contact Mr or Mrs H directly to establish the wider circumstances. From what I've seen, Mr H's phone wasn't under the control of the scammer and so it wouldn't have been possible for them to intercept any fraud prevention efforts on Revolut's part.

If Revolut had intervened—by placing a hold on the payment and contacting Mr and Mrs H to query the purpose of the transaction—I think it's likely the scam would have been uncovered and the payment stopped.

Should Mr and Mrs H bear any responsibility for T's 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've thought carefully about whether Mr and Mrs H should bear some responsibility for what happened. Having done so, I don't think it would be fair to make a deduction in this case.

The scammer persuaded Mrs H that they were a genuine employee of Revolut by spoofing one of its official telephone numbers. She also says that they knew information about the company's accounts that she wouldn't expect to be available to anyone other than an employee of the firm. The actions she subsequently took have to be seen in that context – she reasonably believed that she was interacting with a Revolut employee.

Given the uncertainty concerning the mechanics of this scam, I can't know for certain what she saw at this time. But even if she did see the warning screens that Revolut has described, it doesn't necessarily follow that she acted carelessly. For example, one warning screen told her that *"Revolut will never ask you to make a payment"* – but the premise of this scam was that her actions were *preventing* a payment from being made. It would therefore be understandable why that text wouldn't immediately resonate with her.

The Investigator argued that one of the screens that she might have seen would've showed the value of the payment, but without a minus sign to indicate that funds were being debited from the account. She's said that Mrs H might've misunderstood what was happening. Revolut argued that the screen clearly shows that a payment is being debited. However, it's common in scams such as this one for fraudsters to pressure their victims into taking actions quickly and to overload them with information to reduce their ability to think critically assess the information that's being presented to them. That seems to be what happened here. In addition to that, it's important to consider that she was reasonably acting under the assumption that the call was from Revolut. The spoofed caller ID, the scammer's apparent familiarity with her account, and the convincing interface all contributed to the impression that she was dealing with a genuine Revolut representative. In view of that, I don't think it would be fair and reasonable for a deduction to be made in these circumstances.

Final decision

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

If T accepts my final decision, Revolut Ltd needs to refund the fraudulent payment. It should also add 8% simple interest per annum to that sum calculated to run from the date it debited T's account until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 30 May 2025.

James Kimmitt
Ombudsman