DRN-5097253

The complaint

A company, which I'll refer to as W, complains that Revolut Ltd ("Revolut") won't refund payments that debited its account as part of a scam. Mr P, who is the director of W, has brought this complaint on W's behalf.

What happened

On 31 March 2023, Mr P received a call from someone claiming to be from Revolut. He said they knew his full name, company name, some of his Revolut account information and his contact number. He was told the account was in danger and that he needed to take immediate action. The individual said they could either block the card or create a new company account with Revolut, the latter of which Mr P went ahead with as he felt it was the safest option. He was provided with a new account and sort code and was instructed to send funds into the new account, which he did with his company name as the beneficiary name. He was also told to share a one-time passcode ("OTP") with this individual.

Mr P said the individual told him they would make his other bank aware and after receiving a call from someone claiming to be from his other bank, he came to realise he'd been scammed by a fraudster as he realised that call wasn't genuine. He also checked the payments he'd sent on his account and discovered the recipient's name differed, and he saw a payment had been made through Apple Pay – which was set up with the use of the OTP – that he said was carried out by the fraudster.

Mr P reported the scam on the same day to Revolut concerning the following payments:

Payment number	Date (2023)	Payment details	Amount	Reported as
1	31 March	Faster payment to third party account	£101	Authorised
2	31 March	Apple Pay payment to Apple Store	£1,698	Unauthorised
3	31 March	Faster payment to third party account	£13,550	Authorised
4	31 March	Faster payment to third party account	£8,200	Authorised
5	31 March	Faster payment to third party account	£622.65	Authorised

Revolut declined to refund W. It said as Mr P authorised these payments, it wasn't liable to refund the loss. It was able to recover £18.18 from the beneficiary account.

Unhappy with the decision Revolut reached, Mr P's professional representative referred this complaint to our service on W's behalf. It said these payments were out of character for W and that more should have been done by Revolut to have prevented the company's loss. Mr P said the individual held a lot of information about him, which persuaded him they were calling from Revolut. He said he shared the OTP not seeing that it related to setting up Apple Pay, and at no stage was he aware that the fraudster would be moving money but instead, an account was set up for him to move money into.

Mr P also explained that he recalled feeling very panicked about what he was told and that when he saw that the Apple Store payment had debited his account, this supported what the fraudster had told him. And when he made the faster payments, he didn't see any warning

that said he wasn't paying an account in his name. He also told the fraudster that a second payment to Apple Store was attempted that they encouraged him to reject.

One of our investigators looked into the complaint and upheld it. They didn't consider Revolut liable for the £101 payment Mr P authorised, saying it wasn't out of character compared to previous account activity, but considered Revolut liable for the remaining loss. They said the Apple Store payment was unauthorised and as Mr P (as the authorised signatory on the account) didn't fail in his obligations with gross negligence, Revolut was liable to refund the payment. They further concluded that Revolut ought to have intervened when Mr P authorised the £13,550 payment and that on balance an intervention would've unravelled the scam, so it ought to refund the remaining payments in full.

Mr P agreed with the investigator's outcome, but Revolut didn't agree. Initially it provided a number of points in relation to our service's position to authorised push payment scams. But in its most recent response to our service it said whilst it wasn't disputed that the fraudster completed the steps for the Apple Store payment, as Mr P said he shared the OTP to transfer funds, it considered he had authorised that payment. Concerning the authorised payments, it said it provided a warning that the beneficiary name Mr P input didn't match the account he was paying and that he proceeded despite a clear warning.

As Revolut didn't agree, the matter was passed to me to decide and on 27 September 2024 I issued my provisional decision to both parties where I upheld this complaint. A further copy of my provisional decision was sent to Revolut on 8 October 2024. Mr P's representative, on his behalf, agreed with my provisional decision, adding no further comments. Revolut didn't respond by the deadline given. As the time given has now passed, it's now appropriate for me to progress matters and issue my final decision.

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, I uphold this complaint. I'll explain why.

Was the Apple Store payment authorised by Mr P?

The starting position in line with the Payment Services Regulations 2017, the relevant legislation here, is that Revolut is liable for unauthorised payments. Specifically Regulation 67 sets out that for a payment to be authorised, Mr P must give his consent to the execution of the payment. In practical terms, it means he consents to a payment either by completing the agreed steps or allowing someone else to.

Revolut accepts Mr P didn't complete the payment steps, rather it argues that he gave consent to the fraudster to complete the payment steps on his behalf. Revolut says Mr P shared a OTP to transfer funds into a new account. Mr P has explained to our service that he wasn't of the understanding the fraudster was moving money for him, rather that was something he was doing himself by completing the payment steps through their instruction. And through his representative, he said the OTP was shared as a security measure to protect his account.

There have been different explanations provided about why the OTP was shared and what it was being used for. So I've considered what I think is more likely here.

Given what Mr P has explained, I do consider it more likely that his understanding throughout the process was that he was moving money into a safe account himself, not the

fraudster. He said he didn't understand at the time the OTP was relating to Apple Pay, which appears to be because of the panic he felt to act. And that in sharing the OTP, he wasn't giving the fraudster authority to set-up Apple Pay and authorise payments on his behalf, rather he was taking steps to keep his account secure. Mr P has been open when discussing how the scam unfolded and with all the evidence I have, I'm not persuaded the Apple Store payment was authorised by Mr P.

Did Mr P fail in his obligations with gross negligence?

The Payment Services Regulations set out Revolut can hold Mr P liable for unauthorised payments in certain circumstances. Of most relevance here is if he failed with gross negligence in his obligation to take all reasonable steps to keep safe personalised security credentials and to use the payment instrument in accordance with the account terms and conditions.

When I'm considering if Mr P has failed in his obligations with gross negligence, I need to consider that the test isn't simply whether someone was careless. For someone to fail with gross negligence they would need to have seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person.

Mr P thought he was speaking to Revolut. They knew his personal information, such as his name, company name, his Revolut account information and his contact number. I think most people would have also thought the call was genuine. Revolut has pointed out that both the OTP he was sent, and when he set up the beneficiary for the first payment, had warnings presented that should have concerned him. But in the context of the scam, believing his money was at risk, I don't think not reading the content of the warnings means that his actions were grossly negligent.

Taking everything into account, I'm not persuaded Revolut has shown Mr P has failed in his obligations with gross negligence. So in line with the Payment Services Regulations, it needs to put things right by refunding the unauthorised payment. Along with a refund, it should also pay interest to compensate W for the time it's been without its money.

The authorised payments

It's agreed Mr P authorised the four faster payments made to a third-party account – but he did so due to being tricked by a fraudster.

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 ("Barclays"), 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 Mr P 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 P 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 March 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;[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 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)[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 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[4], 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 March 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 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 Mr P was at risk of financial harm, and would an intervention have made a difference?

---

[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.

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

It doesn't appear Revolut intervened on any payments that left Mr P's account. I consider it was fair that Revolut didn't intervene on the £101 payment. I don't believe it was significantly out of character compared to recent genuine activity in the months prior to the scam that means it missed an opportunity to have prevented the payment. Revolut said when the first payment was initiated, he was presented with a 'do you know and trust this payee' warning, which I consider was proportionate in the circumstances.

But by the time Mr P made the payment for £13,550, I consider Revolut ought to have been concerned. Having considered W's statements 12 months prior to the scam – a time I consider reflects relevant recent activity – this payment was out of character, and a significant increase in outgoings compared to prior activity. W's account often operated on lower outgoing payments, although I recognise it's a business account so more likely to transact larger amounts. And although there was a previous larger payment for £5,000, which appears to go into Mr P's personal account, I still consider £13,550 was a significant increase. I also bear in mind that Revolut would have been aware at the time that the beneficiary name Mr P had input, which was a new payee set up earlier that day, didn't match the beneficiary's account name, so might have otherwise indicated suspicious activity.

Had Revolut asked about the payment purpose, I consider Mr P would have disclosed he was paying money into a safe account. With that information, and had he wanted to proceed, it would have then warranted Revolut to have discussed the payment in more detail with him. I've seen nothing to suggest Mr P would have been dishonest. With appropriate warnings around safe account scams, I'm satisfied that it would have stopped him from proceeding further, and so the scam would have unravelled.

I therefore consider it fair to hold Revolut liable for W's loss for the authorised payments from this point. I've then considered whether Mr P should share some liability for his losses.

Should Mr P bear any responsibility for his losses concerning the authorised payments?

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.

Revolut has argued that it provided clear warnings in the OTP it sent and at the time the new beneficiary was set up for the first payment, where the details didn't match, that should have given Mr P cause for concern. I've already explained why I've concluded that I think it's likely most reasonable people would likely have been satisfied they were dealing with their genuine provider, given what the fraudster knew about Mr P at the time. Mr P was being socially engineered into thinking his account was at risk, leading him to a false sense of panic and given he was told to reject a payment, I can see why he wasn't reasonably concerned or suspicious. Given the time pressure he was being put under, I don't think it was negligent of him not to acknowledge the reference to Apple Pay at the time or recognise the significance of the beneficiary name issue at the time given it only set out that it didn't match. It didn't specify the name on the account and at that point, he believed Revolut had set it up.

And though Mr P said he didn't check the number he was called on until after he realised he'd been scammed, I don't think he was negligent in not carrying out further checks. I think the fraudster did enough at the start to persuade Mr P he was speaking to someone at Revolut.

Taking the above into account, I don't consider that it would be fair to make a deduction in the circumstances. So Revolut should also refund the three payments it ought to have

prevented. Along with a refund of these payments, it should also pay interest to compensate W for the time it's been without its money.

Recovery

Revolut was able to recover £18.18 that remained in the beneficiary account after it was notified of the scam, and it provided evidence showing that when Mr P reported the scam, all but £18.18 had been moved on by the fraudster. Unfortunately in scams like these, it's common for fraudsters to move money on as quickly as possible which is what happened here. I consider Revolut fairly recovered what it could.

My final decision

For the reasons I've explained, I uphold W's complaint. Revolut Ltd must:

- Refund payments 2 to 5 (as set out in the table earlier), less any amount recovered or refunded.
- Pay 8% simple interest per year on this amount from the date of loss to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask W to accept or reject my decision before 19 November 2024.

Timothy Doe
Ombudsman