DRN-4887873

Complaint

Mr J is unhappy that Revolut Ltd didn't refund him after he fell victim to a scam.

Background

One evening in May 2023, Mr J received a phone call from a withheld number. The caller told him that they worked for the Financial Conduct Authority (FCA). They told Mr J that there had been fraudulent activity on one of his accounts. The security of his account with his bank (a separate bank that I'll refer to as H) was, therefore, compromised.

He was told it was essential that he move his funds to a *"safe"* account and that, if he followed the caller's instructions, his money would be protected. He was asked to set up a new account with Revolut. He transferred his funds from the account with H into that new account. The scammers then told him he needed to transfer the money on to an e-wallet maintained by a third-party cryptocurrency platform, that I'll refer to as C. The scammers told him this would *"throw [the fraudsters] off the scent."*

Mr J made two payments from his Revolut account – each for £19,900. Those funds were deposited into the e-wallet with C, converted into cryptocurrency and then transferred to a blockchain address controlled by the fraudsters. However, the first payment was paused. Mr J was directed to interact with a Revolut employee via its app. That interaction is relevant to the outcome of this complaint and so I've reproduced the key sections of it below. Mr J says that he responded to Revolut's questions based on the guidance of the fraudster.

Revolut said:

> *We have noticed an emerging fraud trend and so we want to check some further details with you before you transfer your money. If you have been called by any bank claiming that your account is not safe and you need to move your money to another account, stop […] This is a lie and is a tactic which scammers are using to scare you […] Is this something similar to the reason of your transfer?"*

Mr J responded:

> *"No, nothing relevant."*
>
> *"I am speaking to the FCA."*

Revolut then asked:

> *"Have you recently been contacted by anyone unexpectedly on the phone or by text , advising you of a concern and asking you to move money to another account?"*

Mr J responded:

> *"No, I have not been contacted."*
>
> *"I am happy to continue with the payment."*

There were some further questions which didn't give Revolut cause for concern. Finally, it warned Mr J about the risk of purchase scams. In the end, Mr J confirmed that he knew what he was doing and was happy to proceed. Revolut processed the payments.

When he later realised that he'd fallen victim to a scam, he informed Revolut. It didn't agree to refund him. It said that it had displayed relevant fraud warnings when Mr J was making the payments through the app. He'd chosen to go ahead anyway. Mr J wasn't happy with that response and so he referred his complaint to this service. It was looked at by an Investigator who upheld it in part. The Investigator thought the fact that Mr J said he was speaking to the FCA ought to have been a red flag for Revolut, even if his subsequent answers to its questions didn't give any grounds for concern.

However, she thought it was fair and reasonable for Mr J to bear some responsibility for his own losses by way of contributory negligence. Mr J disagreed with the Investigator's conclusions. He argued that he'd acted reasonably in the circumstances, and it therefore wasn't fair for Revolut to make a deduction from any compensation that was payable.

Revolut also disagreed. Its response was lengthy, but the key points were as follows:

- Mr J was on the phone to the fraudsters during his interaction with Revolut and they were directing the contents of his messages. Even if Revolut had probed further, it's unlikely that Mr J would've given open and honest answers to its questions.
- Mr J paid an account in his own name and so this isn't consistent with the DISP rules' definition of an authorised push payment (APP) scam.
- Mr J's decision to move the funds onwards from the e-wallet with C was a break in the chain of causation.
- It would be more appropriate for Mr J to direct his complaint to one of the other firms involved in the transfer of his funds.
- Mr J acted carelessly in falling for the scam.

As no agreement was reached between the parties, the complaint was 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 J 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 J 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 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 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.

---

[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 *"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 customers' 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).
- 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 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

[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"

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, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Revolut have recognised that Mr J was at risk of financial harm from fraud?

Mr J set up his Revolut account at the request of the fraudster. This put Revolut in a disadvantageous position in terms of spotting potential fraud. It was expected to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might have indicated a fraud risk. However, as this was a brand-new account, it had no data to serve as a basis of comparison. In this instance, it did treat the first payment Mr J made as being worthy of further scrutiny and I think it was right to do so.

Revolut was aware that Mr J was making payments to a well-known cryptocurrency platform. Most cryptocurrency exchanges (including this one) require that the customer's e-wallet and the account used to make deposits be in the same name. It could, therefore, have reasonably assumed that Mr J was making payments to his own account here.

By May 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[5]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wished to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

[5] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr J made in May 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think the fact that the payments in this case were going to an account held in Mr J's own name should have led Revolut to believe there wasn't a risk of fraud. In this instance, Revolut should've been concerned by the value of the payments, the payee and the fact that Mr J inadvertently revealed he was talking to the FCA about the payments.

What did Revolut do to warn Mr J?

Revolut identified that there may be a risk associated with the first payment and so directed Mr J to interact with one of its agents via the chat function in its app. I can see that it gave a reasonably clear (albeit lengthy) warning about the risks of safe account scams. In particular, the warning told Mr J that if a bank called him and told him his account wasn't safe, he shouldn't follow their instructions. In this instance, Mr J had been called by someone claiming to work for the FCA, rather than a bank. Nonetheless, I think it would've been reasonably clear to him that the warning would be applicable to him too.

Revolut asked him several questions and he gave misleading answers. Revolut was satisfied with those answers and so allowed the payments to be processed. According to Mr J, he answered Revolut's questions based on the direction given by the fraudster. There wasn't really any way that Revolut could've known Mr J was being directed in this way. That fact aside, it needed to take into consideration that, in safe account scams, fraudsters will direct victims to give misleading information to the PSP. They might say this is essential because, perhaps, the fictional fraudsters who pose a threat to the customer's account can monitor the interaction or staff at the firm are implicated in the scam.

However, it's significant here that, before those warnings were displayed and those questions put to him, Mr J wrote in the chat that *"I am speaking to the FCA".* There's really no plausible reason why he would've believed he was speaking to the FCA about these payments other than being involved in a scam of this type. In my view, Revolut should've picked up on the significance of this remark, set aside its standard questions and asked him to elaborate on the nature of his conversation with the FCA.

It's hard to know for sure what would've happened if it had done so, but I think the most likely result would be the fraudsters directing him to explain away the message or say that it was sent in error. But I don't think that would've been enough to put Revolut's mind at rest about the potential fraud risk. Essentially, I find that if Revolut had probed Mr J's responses to this follow-up questioning, it's unlikely that he'd have been able to give a plausible and coherent explanation as to why he'd said he was talking to the FCA.

In response to that, Revolut should have provided Mr J with a clear and unambiguous warning that any call he received from an employee of the FCA that required him to make payments in this way could only be a scam. I think, on the balance of probabilities, that's likely to have caused Mr J to stop. I can see no reason for him to have continued if he was warned in those terms.

I accept that the same substance of that warning was contained in the warnings that were delivered to him in the chat. However, it's a known feature of scams like this one that the fraudsters take steps to diminish the effectiveness of any measures taken by the firm to warn the customer, including by keeping the customer on the phone and talking to them throughout, something which we know happened here.

In essence, Revolut needed to recommunicate the same overall message (i.e., that there's no such thing as a 'safe account') more than once to ensure that it resonated with Mr J and to avoid complicating matters by discussing other types of scam, such as purchase scams. I'm satisfied that, if Revolut had probed Mr J's answers to its questions, the genuine circumstances surrounding these payments would've become apparent and it could've provided him with a clear warning. If it had done so, I think his loss would have been prevented.

Is it fair and reasonable for Revolut to be held responsible for Mr J's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut wasn't the point of Mr J's loss. He was paying his own account and needed to take further steps to transfer those funds into the control of the fraudster.

Revolut has pointed out that that means this doesn't constitute an APP scam as defined in the DISP rules. I'm not persuaded that's relevant to the outcome. The DISP rules contain a definition of an APP scam for the purpose of delineating this service's jurisdiction over a specific type of complaint. I don't think it has any bearing on whether Revolut acted fairly and reasonably in its dealings with Mr J.

As I've set out above, I think that Revolut still should have recognised that Mr J might have been at risk of financial harm from fraud when he attempted to make these payments and, in those circumstances, Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses he suffered. The fact that the money used to fund the scam wasn't lost at the point it was transferred to Mr J's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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 either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr J has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr J could instead, or in addition, have sought to complain against those firms. But he has not chosen to do that, and I cannot compel him to. In these circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr J's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); 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 have been) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr J's losses (subject to a deduction for Mr J's own contribution which I will consider below).

Should Mr J bear any responsibility for his 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 recognise that Mr J took the steps he did in the sincere belief that it was necessary to protect his money. Unfortunately, I'm not persuaded that belief was a reasonable one.

I've come to that conclusion because it doesn't seem as if the fraudsters needed to do very much to persuade him that they were legitimate. They didn't demonstrate that they had access to information about his accounts, for example. Nor did they attempt to make it look as if the call had genuinely come from the FCA and encourage Mr J to validate that, something which is frequently seen in scams of this type. As far as I can see, they didn't need to take any of these steps because Mr J took their claims at face value. Once he had accepted in his own mind that the call was a legitimate enquiry from the FCA, it's not unreasonable that he wasn't put off by any of the other unusual factors here. But I still think that the typical customer would've required the fraudsters to do more to persuade them that they were legitimate.

For that reason, I'm persuaded that it's fair and reasonable for Mr J to bear some responsibility for his own losses by way of contributory negligence and, weighing up the fault on both sides, that Revolut should be free to deduct 50% from the compensation it pays him.

Final decision

For the reasons I've set out above, I uphold this complaint. If Mr J accepts my decision, Revolut Ltd needs to pay him 50% of the money he lost to the scam. It also needs to add 8% simple interest per annum to those payments calculated to run from the date they left his account until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 4 October 2024.

James Kimmitt
Ombudsman