DRN-4945282

The complaint

Mr S complains that Revolut Ltd ("Revolut") hasn't protected him from losing money to an authorised push payment ("APP") investment scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything in detail here. But in summary, I understand it to be as follows.

Mr S had been looking to invest to top up his income. He has explained that, while he was browsing a video sharing service, an advert popped up offering an investment opportunity through a company I'll call 'Company N'. It involved making instant returns using online trading options. Mr S recalled the advert included investing in cryptocurrency, forex and gold. Mr S filled out an online application leaving his contact details and was then contacted by a representative of Company N.

Mr S was assigned an account manager who contacted him. Mr S on the instruction of the account manager set up a 'trading platform' with Company N, opened an account with Revolut and also opened an account with a cryptocurrency exchange provider – "K".

Mr S reviewed Company N via the website he was provided with by the account manager. He says it showed good reviews and showed the company had been running for a number of years. He was also asked to provide documentation including identification and proof of address as part of setting up the account with Company N. Mr S has said with the website and the process he felt reassured it was legitimate.

Mr S initially deposited £200 (through an account he held with another financial firm) and has said that after two to three weeks his initial investment appeared to be making good returns and had made around $300 in profit.

All of this led Mr S to believe that he was dealing with a genuine company and that this was a legitimate investment opportunity, but unknown to him at the time he was dealing with fraudsters.

Mr S proceeded to invest more and, as part of the scam, he made the following payments totalling €23,072.00, from his Revolut account. Mr S funded his Revolut account with transfers from his primary bank account held at another firm. The payments he then made from his Revolut account were to an account in his name with cryptocurrency exchange provider K, with him then exchanging the funds into cryptocurrency and sending them on to accounts controlled by the fraudsters.

Payment	Date	Time	Amount	To
1	21/06/2023	18:21	€5,762.00	Cryptocurrency account in Mr S' name
2	22/06/2023	14:19	€5,748.00	Cryptocurrency account in Mr S' name
3	29/06/2023	14:30	€11,562.00	Cryptocurrency account in Mr S' name

Mr S realised he'd been scammed when he attempted to withdraw funds from the investment, when it was sitting at around £60,000. He attempted to withdraw three times and then contact stopped.

Mr S raised the matter with Revolut, but it didn't agree to reimburse Mr S his loss.

Unhappy with Revolut's response Mr S brought his complaint to this service. One of our Investigator's looked into things and thought the complaint should be upheld in part.

In summary, it was our Investigators view that Revolut should have recognised that Mr S could have been at a heightened risk of financial harm when he made the first payment and that it should have intervened. It was our Investigators view that had an intervention taken place the scam could have been prevented and Mr S wouldn't have lost his money from this point.

But our Investigator also thought Mr S should bear some responsibility for his loss. In summary our Investigator thought the rate of return for the investment was too good to be true and that Mr S only really relied on the website / information that he had been provided with and didn't carry out any independent checks. The Investigator also thought Mr S should have been wary as to why he was being asked to lie to Revolut if challenged on the purpose of the payment as this wasn't something a legitimate investment firm would do.

Overall, our Investigator thought Revolut should refund Mr S 50% of his outstanding loss and that it should pay 8% simple interest on this amount from the date of the loss.

Through his representatives, Mr S responded and agreed with our Investigator's opinion.

Revolut responded disagreeing. In summary, it advised:

- Cryptocurrencies are extremely volatile investments that cannot be taken as 'guaranteed profit'. Such highly speculative and highly-volatile investments carry with them a greater responsibility of research before investing. The absence of such actions suggests a disregard for prudent financial decision-making. It is not reasonable for someone, who lacks investment experience, to commit to an investment without conducting proper research (as it was admitted in the investigators view).

- Revolut is, in essence, being asked to refund a customer of another financial firm that fell victim to a scam. At the outset of the scam, the customer did not have a Revolut account and was coached to create the account to facilitate the scam.

- The payments in question are in reality self-to-self payments. The fraudulent activity did not occur on the customer's Revolut account, as the payments being made were to perform legitimate cryptocurrency purchases to accounts held in the customer's own name.

- It is relevant to bear in mind that the type of account which the customer used is not a current account and Revolut is not a bank but an Electronic Money Institute (EMI). Typically, this type of account is opened and used to facilitate payments of a specific purpose and often not used as a main account (which Revolut say is the case here – with the customer not a regular Revolut customer).

As agreement couldn't be reached, the complaint has been passed to me for a 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.

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 Mr S 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 S 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 June 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.

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".*

---

[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.

- 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).

- 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 June 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); and

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

- 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 S was at risk of financial harm from fraud?

It isn't in dispute that Mr S has fallen victim to a cruel scam here, nor that he authorised the payments to the cryptocurrency account in his own name (from where he exchanged the fiat currency into cryptocurrency and subsequently transferred this to the scammer).

By June 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. 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 wish 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.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr S made in June 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.

I'm also mindful of the fact that this was a new account. Mr S only opened the account on the advice of the fraudster. That put Revolut in a more difficult position in respect of spotting payments that might have had an associated fraud risk because there was no historical data concerning his typical account usage that could've served as a basis of comparison.

Nonetheless, I agree with the Investigator's conclusions that it ought to have had concerns at the point Mr S made the payment of €5,762.00 on 21 June 2023 (Payment 1). I find that the value of the payment alongside the fact that it was being made to a third-party cryptocurrency exchange was significant enough to necessitate Revolut taking some steps to warn Mr S.

I also consider there were other factors that ought to have been apparent that its customer may be at risk of financial harm. Mr S, prior to Payment 1, had attempted five card payments to another cryptocurrency exchange provider which were all declined by Revolut with it advising its automated system declined the transactions. And Mr S had also been required to select a payment purpose for Payment 1 – with Mr S choosing 'safe account'. So, I think the activity here, of five declined card payments, then a faster payment to an identifiable cryptocurrency exchange while selecting a payment purpose as 'safe account' warranted Revolut taking some additional steps to satisfy itself that Mr S wasn't at risk of financial harm when he was making this payment.

I have also considered that the account opening purpose was consistent with the transaction Mr S was making. However, for reasons already explained, by the time this payment was made Revolut ought to have recognised that cryptocurrency transactions carried an elevated risk of the likelihood of the transaction being related to a fraud or scam. Therefore, I think it fair and reasonable to have expected Revolut to have had some concerns.

What did Revolut do to warn Mr S?

From the evidence that has been shared with me, Revolut initially provided Mr S with a new beneficiary warning under the 'review transfer' when he set up and made Payment 1. This asked if Mr S knew and trusted the payee and advised fraudsters can impersonate others and that Revolut would never ask a customer to make a payment. I understand that this warning is provided / generated whenever a new payee was being created. But this warning doesn't relate to the circumstances Mr S found himself in and I don't think it was a proportionate response to the risk Payment 1 presented.

Revolut has advised that it also provided a further warning in relation to Payment 1 (and also Payment 2), with Mr S having to select a payment purpose – with Mr S selecting 'safe account' each time.

While I appreciate that Mr S wasn't falling victim to a safe account and could have chosen a more suitable payment purpose, I am mindful that Revolut were aware that the payment(s) were in fact going to a cryptocurrency exchange. I am also mindful that a payment reason being chosen as 'safe account' can only apply if a customer is falling victim to a safe account scam or the consumer has potentially chosen an incorrect payment purpose. Either way, I think Revolut needed to satisfy itself that Mr S wasn't at risk here and explore why he chose the payment purpose he did, given the payments were also going to a cryptocurrency exchange provider. And it could have done this by directing him to its in-app chat or through having a conversation with him.

What kind of warning should Revolut have provided?

As mentioned above, I think Revolut, when Mr S attempted to make Payment 1 knowing that the payment was going to a cryptocurrency exchange, and that a payment purpose of 'safe account' had been selected, ought to have directed Mr S to its in-app chat or had a conversation with him about the payment he was making.

Mr S had been coached in part by the scammer, but only in a limited way. It seems if Mr S was asked, he was to say the payment was going to a friend.

It seems to me, had Revolut asked some open ended and probing questions then Mr S's potential reason for the payment would seem at odds with what it knew about the payment and the earlier activity, and that there was a heightened chance that he was at risk of financial harm. In short, I think it is reasonable to say that Revolut would be on notice that Mr S was making a payment to a cryptocurrency exchange provider – whereby the account was likely in Mr S's name, he had selected 'safe-account' as the payment purpose but might have initially alluded to the payment being for a friend, and there had also been five declined card payments prior. So I think Revolut, with the knowledge of what it knew about the payment and what had happened prior, would have been able to probe more. And it is more likely than not that the genuine reason / purpose for Mr S making the payment would have been uncovered.

Revolut then would have been in the position whereby it could have provided a warning that was specifically about the risk of cryptocurrency investment scams. And I think that such a warning should have addressed the key risks and features of the most common cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of such scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I think a warning covering the key features of cryptocurrency investment scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented, would have been a proportionate and reasonable way for Revolut to have acted in June 2023 to minimise the risk of financial harm to Mr S.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr S suffered from the first payment?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr S's payments, such as finding the investment through an advertisement on social media / video sharing service, being assisted by a broker / account manager, being asked to download remote access software, and having paid a small initial deposit which had quickly increased in value.

There's no evidence to suggest Mr S was asked, or agreed to, disregard any warning provided by Revolut. In addition, Mr S did not receive any specific warnings from his other banking provider (from which the money originated) when he transferred money to Revolut – so there's no evidence he ignored a specific and tailored warning.

On the balance of probabilities, if Revolut had provided Mr S with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into the supposed investment firm, which wasn't regulated to do what it was seemingly carrying out, before proceeding, as well as making further enquiries into cryptocurrency investment scams. I'm satisfied that a timely warning to Mr S from Revolut would very likely have caused him to do so, revealing the scam and preventing his subsequent losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr S sent funds to his own cryptocurrency account to enable the purchase of cryptocurrency, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out above, I think that Revolut still should have recognised that Mr S might have been at risk of financial harm from fraud when he made Payment 1, and in those circumstances Revolut should have made further enquiries with Mr S about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mr S suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr S's own cryptocurrency exchange account does not alter that fact and I think Revolut can fairly be held responsible for Mr S'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 either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr S 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 he could instead, or in addition, have sought to complain against those firms. But Mr S has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr S's compensation in circumstances where: he has only complained about one respondent from which he is entitled to recover his 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 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 S's loss from Payment 1 (subject to a deduction for Mr S's own contribution which I will consider below).

Should Mr S bear any responsibility for his losses?

There is a general principle that consumers must take responsibility for their decisions, and I am mindful of the law relating to contributory negligence and the impact a finding of contributory negligence may have to reduce the damages recoverable by a claimant in court proceedings.

I have duly considered whether Mr S should bear some responsibility by way of contributory negligence, and I'm satisfied he should in the circumstances of this case. I am mindful that Mr S has already accepted he should bear some responsibility in his case – so I will keep my comment here brief.

Overall, I consider there to have been enough warning signs that Mr S was being scammed, which he does not appear to have reasonably acknowledged or acted upon.

While Mr S came across the advert through a video sharing service, he doesn't seem to have done any other independent checks of his own. The contact here was seemingly through a cloud-based mobile and desktop messaging app – which to my mind doesn't seem in line with how a legitimate investment firm would communicate. And Mr S doesn't seem to have been provided, or hasn't provided this service, with any formal contract that he entered into – setting out the terms of any investment arrangement between the two parties.

Mr S had seemingly been told that he could receive substantial profits and within a short space of time. I think the promises made and so soon after investing ought to have stood out to Mr S as simply being too good to be true. I can't see that Mr S questioned how such high levels of returns could be realised.

I also don't think a legitimate investment firm would recommend to its customers that they don't disclose the true purpose for the payment if asked by their bank or payment service provider – which was the case here with Mr S being told to say the payment is for a friend.

As a result, I'm satisfied Mr S should've had reasonable cause for concern that things might not be as they seem. But it doesn't appear that he made adequate enquiries into the legitimacy of things or what he was being told. I might understand how in isolation any one of these things may not have prevented Mr S from proceeding. But when taken collectively I think there were sufficient red flags here that reasonably ought to have led Mr S to have acted far more cautiously than he did.

So, I think Mr S did have a role to play in what happened and I think that the amount Revolut should pay to him in compensation should fairly and reasonably be reduced to reflect that role. I think that a fair deduction is 50%.

Could Revolut have done anything else to recover Mr S's money?

For completeness, I'll address recovery. The Faster Payments were sent to Mr S's own account at K, converted into cryptocurrency and then sent to the fraudster. Though Revolut attempted to recover those payments, in these circumstances, it's difficult to see how any recovery would have been possible.

Putting things right

For the reasons explained, I uphold this complaint, in part, and now ask Revolut Ltd to:

- refund Mr S 50% of his loss (so €11,536 – that being 50% of the sum of Payments 1, 2 and 3)

- pay interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement (if Revolut Ltd deducts tax from this interest, it should provide Mr S with the appropriate tax deduction certificate).

My final decision

For the reasons given above, my final decision is that I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 4 April 2025.

Matthew Horner
Ombudsman