DRN-4995872

The complaint

Mr S complains that Revolut Ltd hasn't reimbursed the money he lost to a scam.

What happened

Mr S has fallen victim to a cryptocurrency investment scam. He was introduced to a company I'll refer to as 'X' by a friend, who had seen some initial success in trading with X after coming across an advertisement on social media. He says he carried out an internet search to check X wasn't a scam and couldn't find anything to suggest the company was illegitimate, and he found good reviews about X on review platforms. So, he decided to invest.

He made the following two card payments to his own cryptocurrency exchange account, then converted the funds into cryptocurrency which was sent to X:

Date of payment	Amount of payment
14 February 2023	£5,000
6 March 2023	£4,000

When Mr S realised he'd been defrauded, he complained to Revolut that it had failed to protect him from the scam. Revolut said that:

- It doesn't owe a duty to prevent fraud and scams.
- It followed Mr S' instructions to execute the disputed transactions.
- It had no reason to suspect the disputed payments were being made as a result of fraud – it appeared that Mr S was purchasing cryptocurrency from a legitimate merchant.
- Transactions to a known cryptocurrency provider align with the established purpose of Mr S' account, and the disputed payments weren't out of line with the typical way in which a Revolut account is used.
- The money was lost to the scam from Mr S' cryptocurrency exchange account, not from his Revolut account. Revolut was simply used as an intermediary to receive funds from Mr S' external bank account and transfer it on to his external cryptocurrency exchange account.

What did our investigator say?

Our investigator thought Revolut and Mr S should share liability equally for the financial loss in this case. He found that Revolut ought to have been concerned about, and intervened with, the disputed payments and he said that if it had, the scam would most likely have come to light. But he also found that Mr S didn't act reasonably in the circumstances.

Mr S accepted our investigator's findings, but Revolut asked for an ombudsman's final

decision. The case has now been passed to me to decide.

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 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 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 – among other things – 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"* (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's ('FCA') Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks. In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in February 2023 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.

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 did in fact seek to take those steps, often by:

- Using algorithms to identify transactions presenting an increased risk of fraud.
- 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. For example, it is my understanding that in February 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

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 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, 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.
- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So, it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulator's 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 February 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).
- 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.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in February 2023, Revolut should in any event have taken these steps.

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 scam here, nor that he authorised the disputed payments to his own cryptocurrency exchange account (from where the exchanged cryptocurrency was transferred to the fraudster).

I'm aware that cryptocurrency exchanges like the one Mr S used generally stipulate that the

card used to purchase cryptocurrency at its exchange must be held in the name of the account holder. Revolut would likely have been aware of this fact too. So, it could reasonably have assumed that the disputed payments would be credited to a cryptocurrency wallet held in Mr S' name.

By February/March 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 customers' 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 disputed payments being made, 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 some circumstances, as a matter of what I consider to have been fair and reasonable good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And, as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Considering all of the above, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mr S' own name should have led Revolut to believe there wasn't a risk of fraud. So, I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr S may be at a heightened risk of fraud that merited its intervention.

The first disputed payment was relatively high-value, it was clearly going to a cryptocurrency provider, and it was significantly larger than any other payments that had debited Mr S' account in the previous six months. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr S was at heightened risk of financial harm from fraud. In line with good industry practice and

regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before the payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, I think it was a combination of the characteristics of this payment which ought to have prompted a warning.

I do not suggest that Revolut ought to apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above, I'm satisfied that by February 2023, Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Mr S and what kind of warning should Revolut have provided?

Revolut has said that it did not intervene with the first payment Mr S made to the scam (or the second payment) because it had no reason to be suspicious about it/them.

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to the first payment Mr S made will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time the payment was made.

Taking that into account, I think Revolut, knowing the payment was going to a cryptocurrency provider, ought to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scams, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – 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 common cryptocurrency investment 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; access to a fake trading platform; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr S by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

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

I think that most consumers would take note of, and be positively impacted by, the type of intervention I've described, and I haven't seen anything to suggest Mr S wouldn't have been. I can't see that Mr S was being coached by the scammer, or reassured about the legitimacy of what was happening. And the scam he fell victim to carried some of the typical features of cryptocurrency investment scams, so I think that a warning highlighting the key features of

common cryptocurrency investment scams would most likely have resonated with him.

In saying this, I acknowledge that Mr S' external bank account provider did provide some fraud warnings when he transferred the money he ultimately lost to the scam into his Revolut account – and these warnings were unsuccessful in halting the scam. But the external account provider had less information available to it about the ultimate destination of Mr S' funds, and the warnings it gave were generalised and not relevant to cryptocurrency investment scams. I don't consider that they were particularly impactful, and I'm not persuaded that Mr S moving past them is indicative of what would have happened if Revolut had given a warning specifically about cryptocurrency investment scams as I've described.

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

In reaching my decision about what is fair and reasonable, I have taken into account that the payments which ultimately funded the scam were paid into Mr S' Revolut account from another account in Mr S' name held with a different regulated financial business, and that the disputed payments went from Revolut to a cryptocurrency exchange account in Mr S' name. I have carefully considered Revolut's view that it merely acted as an intermediate link – being neither the origin of the funds lost nor the point of loss.

But as I've set out in some detail above, I think that Revolut should still have recognised that Mr S might have been at risk of financial harm from fraud when he made the first disputed payment, and in those circumstances it should have intervened proportionately. If it had, I'm satisfied that it would most likely have prevented the losses Mr S suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to another of Mr S' own accounts does not alter that fact and I think Revolut can fairly be held responsible for Mr S' losses in such circumstances. I don't think there is any point of law or principle that says a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

Overall, I am satisfied that it would be fair to hold Revolut responsible for Mr S' loss from the first disputed payment (subject to a deduction for Mr S' own contribution which I will consider below).

Should Mr S bear any responsibility for his loss?

I've thought about whether Mr S should bear some responsibility for his loss by way of contributory negligence, and, in the circumstances, I think he should share responsibility for his loss with Revolut equally – each being responsible for 50% of the loss. This is because I'm persuaded that Revolut ought to have done more to protect Mr S from financial harm, but he ought reasonably to have done more to protect himself from financial harm too.

I say this because there isn't a wealth of information available online about X, and Mr S doesn't appear to have been in communication with the scammer for long or been offered much convincing information about X's legitimacy before he decided to invest a fairly sizeable amount. Mr S doesn't appear to have taken any substantial steps to verify the legitimacy of the investment opportunity and/or X before he made the disputed payments as I think he ought reasonably to have done in order to protect himself from financial harm.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint in part and instruct Revolut Ltd to refund 50% of both disputed payments and pay interest at a rate of 8% simple per annum from the date of each payment to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 30 April 2025.

Kyley Hanson
Ombudsman