DRN-5082108

The complaint

Mrs S complains that Revolut Ltd hasn't reimbursed her after she fell victim to a scam.

What happened

The background to this complaint is well-known to both parties and so I'll only summarise key events here.

In February 2023 Mrs S found what appeared to be a celebrity endorsed advert for cryptocurrency investment. Interested in the opportunity she followed the advert and ultimately sent £220 (using a credit card held outside of Revolut) as an initial investment, using the payment instructions she received.

What Mrs S didn't realise at the time was that the advert was fake. It had been created by a scammer.

Mrs S was then contacted by the scammer directly and they claimed to be her account manager. They talked on WhatsApp and over phone calls.

Mrs S has explained she only intended to invest the £220 from the outset. Her plan was to watch the returns grow before withdrawing further down the line.

The scammer went on to explain that if Mrs S wanted to withdraw anything she'd need to open a cryptocurrency wallet so her returns could be paid into it. She was encouraged to open such a wallet, along with a Revolut account which was also to be used to facilitate payments. Mrs S downloaded a screen sharing app so the scammer could help with the opening of these accounts.

Once those accounts were open Mrs S was told to make a payment of £15 from Revolut to the wallet to verify it. She then received what was a fake email – purporting to be from the wallet provider – which explained proof of liquidity was required in the form of a £5,000 deposit.

Mrs S didn't have that money and so the scammer suggested applying for a loan. Mrs S has explained it was the scammer that completed an application in her name. She felt uncomfortable but the scammer had already gone through the process, making use of the screen sharing software again.

Mrs S says the scammer then went on to make a £5,000 card payment to the cryptocurrency wallet. The scam was revealed shortly after. Mrs S says she couldn't see the credit funds in her wallet and received a further request for payment. She then couldn't withdraw anything at all and that's when she knew something was wrong and she reported what had happened to Revolut.

Revolut considered what had happened and said it wouldn't reimburse any of Mrs S' loss. It said it had made the payments in accordance with her instructions and there had been no reason for it not to do so. Mrs S was unhappy with its response and so brought her

complaint to our service.

One of our investigators considered the complaint and recommended it be upheld. She felt the £5,000 represented an identifiable scam risk that Revolut ought to have recognised. She said it ought to have identified Mrs S was at risk of financial harm through fraud and so to have given a tailored warning about cryptocurrency investment scams. She was satisfied that, had it done so, the scam would have been revealed and Mrs S' loss avoided. So she recommended Revolut be partly responsible for that loss.

Our investigator also felt Mrs S could have done more to protect herself. She acknowledged Mrs S had put faith in an apparent celebrity endorsement, but considered the scam hadn't been very sophisticated. She also noted there was a live FCA warning about the firm behind the supposed investment and that the requirement to pay £5,000 to verify an account seemed unrealistic. With that in mind our investigator recommended Mrs S bear equal responsibility for her loss of the £5,000 as her actions hadn't been reasonable throughout.

Mrs S confirmed receipt of the decision but didn't indicate whether she accepted the findings or not.

Revolut didn't accept the findings and said, in summary:

- The payments had been properly authorised;
- There wasn't enough of an identifiable scam risk for it to step in;
- The payment went to an account in Mrs S' name and control, and so it shouldn't be responsible for the loss;
- The loss occurred outside of Revolut, and there were payments in from other FCA regulated firms, and so the actions of those firms ought to be taken into account too.

As agreement hasn't been reached the complaint has been passed to me.

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'm upholding it along the same lines as our investigator, and for broadly the same reasons. I'll explain more.

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 Mrs 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 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;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;

[1] 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_/

- 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)[2].
- 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[3], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- 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 –

[2] 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.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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, 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 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); 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.

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 Mrs S was at risk of financial harm from fraud?

From what Mrs S has said, there is an indication that she may not have completed all of the transactions connected to the scam herself. Though I am satisfied they ought to be treated as authorised as she did know they were taking place. I consider it's more likely than not she knew about both the loan application and the payments to the crypto wallet. Key evidence in that regard is:

- Within the messages between Mrs S and the scammer she says, "Loan is agreed, in account in 2 days" followed by (the next day), "Hi sorry I was on a call. Yes loan is in my account". This shows me that Mrs S knew about the loan application when it was made, knew it would take some time to credit her account, and informed the scammer of when this happened.

- Revolut's app will not allow screen sharing apps to view devices on the payment processing screens. That means it wouldn't have been possible for the scammer to complete the payment process. But, even if I'm wrong on this point, Mrs S has confirmed she knew the payment was being made.

These points don't change the fact that Mrs S was the victim of a cruel scam. But it's important I make a finding on these issues.

Whilst I have set out in detail in this decision the circumstances which led Mrs S to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mrs S might be the victim of a scam.

I'm aware that cryptocurrency exchanges like the one used here generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the first payment would be credited to a cryptocurrency wallet held in Mrs S' name.

By February 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. And by February 2023, when these payments took place, further restrictions were in place. 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 Mrs S made in February 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.

To be clear, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees.

As I've set out in some detail above, it is the specific risk associated with cryptocurrency in February 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those 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.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Mrs S' own name should have led Revolut to believe there wasn't a risk of fraud.

The second payment made – the £5,000 transaction – carried a significant risk. The value involved was high, and ought to have concerned Revolut. It didn't match the account opening purpose, being a crypto payment where the account purpose was stated as 'transfers'. And it'd been funded only a short time before by an incoming payment, with the outgoing one draining the account completely. This is on top of what I've described above, that being the high inherent risk with cryptocurrency payments.

Whilst Revolut didn't have an account history to work from, the above factors ought to have been enough to cause a degree of concern.

What did Revolut do to warn Mrs S?

There's been no suggestion of warnings being provided to Mrs S at the time she made payment.

What kind of warning should Revolut have provided?

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 this one 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 this payment was made.

Taking that into account, I think Revolut ought, when Mrs S attempted to make the £5,000 payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, 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 scam, 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; 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 Mrs 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 Mrs S suffered from the £5,000 payment?

I'm satisfied Mrs S would have seen the warnings when the payment was being made, regardless of what's been said about the screen sharing software being used.

I've also considered that Mrs S was clearly in regular contact with the scammer and was being told what to do at each stage of the scam.

However, I've seen no evidence to suggest she was being coached through warnings and told to ignore them. And given the characteristics of the scam she was caught up in were so closely aligned to what the warning ought to have said, I'm persuaded it would have resonated with her and had an impact.

She was already nervous about proceeding with the loan. And so a suitable warning would have given her further reason to question what she was doing and to have stopped. Her loss would then have been avoided.

It's also the case that Mrs S received no warning when she paid the loan funds from her other current account into her Revolut one. So there are no interventions or warnings from other FCA regulated firms for me to consider.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, notwithstanding what's been said about the scammers use of screen sharing software, 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 £5,000 payment was made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made the £5,000

payment, and in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mrs 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 Mrs S's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs 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 Mrs 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 Mrs S could instead, or in addition, have sought to complain against those firms. But Mrs S has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs S'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 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 Mrs S' loss of the £5,000 payment (subject to a deduction for Mrs S's own contribution which I will consider below).

Should Mrs S bear any responsibility for their losses?

Our investigator found that Mrs S ought to bear some responsibility for her loss too. Mrs S didn't object to those findings and made no counter-argument. It's also not a point that Revolut disagrees with, so there's no remaining dispute on this point and therefore little for me to make a finding on.

All I'll say is that I am in agreement that Mrs S ought to bear some responsibility. I find there were signs all was not as it seemed and characteristics of the scam that ought to have been questioned. And Mrs S had opportunities to uncover the scam herself, had she sought to ensure everything was legitimate.

It's then fair and reasonable for both parties to share responsibility for the £5,000 loss.

Was there any other opportunity to recover Mrs S' money?

Because this was a card payment to a cryptocurrency wallet, and we know the funds were moved on to the scammer, there was no prospect of recovering this money. It couldn't be returned from the account that received it as it was already gone. And a chargeback would never have succeeded, given the service which was paid for was delivered, in that Mrs S' wallet was credited with the funds which were then used.

Putting things right

On Mrs S' acceptance Revolut must:

- Reimburse 50% of the £5,000 loss; *and*

- Pay interest on that sum at 8% simple per year, calculated form the date of loss to the date of settlement.

My final decision

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 24 April 2025.

Ben Murray
Ombudsman