DRN-5026137

The complaint

Mr G is unhappy that Revolut Ltd ("Revolut") won't refund the money he lost to a third-party scam.

What happened

Mr G was looking to invest and saw an article about a celebrity who had made a lot of money from cryptocurrency. He followed the link in the article to express an interest. Mr G was contacted by a 'senior broker' working for an organisation, I will refer to as V.

He bought cryptocurrency (transaction shown in the table below) and placed it in wallets in his own name and moved his cryptocurrency to the scammer's wallet for what he believed to be further trading.

Date	Payee	Amount
16 May 2023	Card payment to R	£2,000
16 May 2023	Card payment to R	£1,900
16 May 2023	Card payment to V	£6,000
16 May 2023	Card payment to V	£5,100

After a week the broker said she had been hospitalised and a few days later the website went down. And shortly after the broker ceased all contact and Mr G was unable to withdraw his money.

Revolut declined to refund Mr G. It said these were 'self to self' transactions (as the card payments were for cryptocurrency which was placed in wallets in Mr G's name) and Revolut was just the intermediate link. It says it has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. Revolut referred to the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25. It said articles had been published, before Mr G invested, in which the celebrity discusses cryptocurrency scams and says that he had never endorsed any or knew anything about cryptocurrency.

Our investigator upheld the complaint in part. She thought Revolut ought to have been concerned by payment two, but she didn't think proportionate intervention would have made a difference. However, she considered further intervention on payment three would have made a difference to Mr G proceeding with the payment. So she recommended payments three and four be refunded but with a 50% reduction for Mr G's share in responsibility for what happened.

Revolut didn't agree and reiterated its previous points, adding that the allocation of responsibility is at odds with the approach the regulator deems appropriate and is irrational.

As the complaint could not be resolved informally, it's been passed to me for a 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.

When considering what is fair and reasonable, I'm also required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

Having done so, I have come to the same overall conclusion as the investigator; broadly for the same reasons and I am upholding this complaint in part.

Where I can't know for certain what has or would have happened, I need to weigh up the evidence available and make my decision on the balance of probabilities – in other words what I think is more likely than not to have happened in the circumstances.

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 G 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 May 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;
- 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 May 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).

[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_/

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 – 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.

---

[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"

- 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 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 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 May 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr G has fallen victim to a cruel scam here, nor that he authorised the card payments to purchase cryptocurrency which he then placed in his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst we now know the circumstances which led Mr G to make the payments using his 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 Mr G might be the victim of a scam.

But 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. And by May 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 Mr G 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.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, 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 May 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 the payments in this case were going to an account held in Mr G's own name should have led Revolut to believe there wasn't a risk of fraud.

So, I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr G might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments were going to a cryptocurrency provider, but the first payment was relatively low in value (although I appreciate it is a lot of money to Mr G), and I don't think Revolut should reasonably have suspected that it might be part of a scam. The payment was after all for a genuine purchase of cryptocurrency and to an account in Mr G's name. And not all cryptocurrency payments are scams. So Revolut needs to strike a balance between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

But the second payment was made just a few minutes later and - combined with the first payment - amounted to almost £4,000. The activity on the account (which had been dormant since October 2022) was looking unusual and payment two was clearly going to a cryptocurrency provider. The purchase of cryptocurrency was out of character for Mr G. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of this payment (and the pattern that preceded it), I think Revolut ought to have been sufficiently concerned about this payment that it would be fair and reasonable to expect it to have provided warnings to Mr G at this point.

Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr G 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 this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

I do not suggest that Revolut should 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 May 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 kind of warning should Revolut have provided on payment two and would that have prevented the loss Mr G incurred on payment two?

Revolut didn't provide any warnings in this case. So 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 primary 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 Mr G attempted to make the second 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.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented the loss on payment two in this case. And on the balance of probabilities, I don't think it would have.

I say this because when faced with written security questions from one of the cryptocurrency providers – Mr G turned to the scammer for advice (copying that text into the chat with the scammer). On balance, I think it likely he would have asked the 'broker' how to respond to any written warning from Revolut which would likely have resulted in him (albeit on the advice of the scammer) disregarding any warning provided by Revolut and proceeding with the payment.

What kind of warning should Revolut have provided on payment three and would that have prevented the losses Mr G incurred from that point?

For the third payment Revolut needed to go further. Payment three was for £6,000 and to a second cryptocurrency provider within a few hours. By now almost £10,000, over three payments within a few hours, had left the account to buy cryptocurrency.

Having thought carefully about the risk payment three presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mr G's account. I think it should have done this by, for example, directing Mr G to its in-app chat to discuss the payment further.

Had it done so, it would have had the opportunity to ask Mr G open and probing questions about the transaction. When Mr G made the payment from his high street bank account to his Revolut account, Mr G was given a cover story to say he was making the transfer because he was 'travelling'. This was a plausible explanation (especially for a Revolut account) in those circumstances and the high street bank could not see the ultimate destination was cryptocurrency. The bank's written warning was actually centred on safe account scams – again reasonable in the circumstances as Mr G was moving money to his own account with Revolut. So it's understandable why he moved passed the warning – as he wasn't falling victim to a safe account scam.

But Mr G's cover story wouldn't have worked with Revolut, given what Revolut would have known about the destination of the payment. I've thought about whether Mr G would likely have been provided with an alternative cover story if Revolt had intervened. It's certainly a possibility I've considered. But if Revolut had reached out to Mr G to ask probing and open questions as part of a human intervention, I think it would have been much harder for Mr G to maintain a cover story - given the ultimate destination of the payment. Mr G also commented within the chat messages with the scammer that he was nervous with reference to his conversation with the other bank. So, I don't think it would have taken too much before any cover story would have unfolded.

And if Revolut had highlighted 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, fake trading platforms, Mr G would have realised he was falling victim to a scam and stopped payment three and the payment that followed.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr G purchased cryptocurrency which credited an e-wallet held in his own name, 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.

But as I've set out in some detail above, I think that Revolut still should have recognised that consumer might have been at risk of financial harm from fraud when he made payment three, 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 consumer 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 consumer's own account does not alter that fact and I think Revolut can fairly be held responsible for consumer'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 consumer 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 consumer could instead, or in addition, have sought to complain against those firms. But consumer has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce consumer'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 consumer's loss from payment three (subject to a deduction for consumer's own contribution which I will consider below).

Should Mr G bear any responsibility for his losses?

I've thought about whether Mr G should bear any responsibility for his loss connected to the last two payments. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Mr G' own actions and responsibility for the losses he has suffered.

I recognise that there were relatively sophisticated aspects to this scam, not least, V appears to be a clone of a genuine business name and I understand Mr G had access to a trading platform. But Mr G was told not to let his bank know his payment was for cryptocurrency and instead say he was travelling. I think Mr G ought to have found this concerning given this was supposed to be a legitimate investment run by a legitimate business. Mr G says he searched around the celebrity endorsed within the article he'd seen - but I think if he had done so, he would have found some articles (I found some going back to 2019) suggesting this was a scam.

So, given the above, I think he ought reasonably to have realised that there was a possibility that the scheme wasn't genuine and question it further. In those circumstances, I think it fair that he should bear some responsibility for his losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mr G on payment three and four because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

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

The payments were made by card to cryptocurrency providers. Mr G sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that R and V provided cryptocurrency to Mr G, which he subsequently sent to the fraudsters.

Putting things right

In order to put things right for Mr G, Revolut must:

- Refund 50% of transactions three and four (so £5,550 in total)
- Add simple interest* on the above refund at the rate of 8% per annum from the date the payments were made to the date of settlement.

*****If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Mr G how much it's taken off. It should also provide a tax deduction certificate if Mr G asks for one, so the tax can be reclaimed from HM Revenue & Customs if appropriate.

My final decision

My final decision is that I uphold this complaint in part and Revolut Ltd must put things right for Mr G as set out above.

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

Kathryn Milne
Ombudsman