DRN-4483900

The complaint

Mr O complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr O was researching cryptocurrency online when he came across a company which I'll refer to as "L". L was endorsed by a well-known celebrity and Mr O spoke to someone I'll refer to as "the scammer" who told him he worked for L and that he could make money by investing in oil, gold, gas and cryptocurrency.

Mr O was given access to an online portal where he could monitor his investment and see his deposits in real-time. He was also advised to download remote access software and to open a Revolut account, which he did on 2 February 2023, stating the purpose of the account as 'spend or save daily'.

The scammer asked him to first purchase cryptocurrency through a cryptocurrency exchange company which I'll refer to as "B" and from there, the scammer used AnyDesk to load the cryptocurrency onto an online wallet. Mr O sent funds to the Revolut account from an account he held with Bank H, and on 7 February 2023 and 8 February 2023 he paid £6,500 and £4,000 to B using a debit card connected to his Revolut account. £61 was returned to Bank H from B on 7 February 2023.

Mr O was able to make small withdrawals from the platform before he made the larger payments, but when he decided he wanted to make a withdrawal, he was told he'd have to make a payment to release his funds. He was also told he'd have to pay capital gains tax on the returns, at which point he realised he'd been scammed.

He complained to Revolut, but it refused to refund any of the money he'd lost. It said claims were raised under Mastercard's chargeback scheme, but Mr O failed to produce the information it requested so the claims were cancelled.

Mr O wasn't satisfied and so he complained to this service with the assistance of a representative who said the scam was very complex and he had no reason to doubt the investment was genuine. They accepted he'd previously bought a very small amount of cryptocurrency but was unaware of the risks.

The representative argued that even though there was no account history to compare the payments with, large sums of money moving into the account and being paid out to a high-risk merchant on the same day, with the balance returning to £0 each time, ought to have raised concerns. They said Revolut should have questioned Mr O about the payments, and had it done so he'd have explained he'd been approached by someone offering an opportunity to invest in cryptocurrency and it would have detected the scam.

Revolut further commented that the transactions were 3DS authenticated and it has controls within its app to prevent remote access, so it wasn't possible for a third party to have initiated the payments.

It said the payments weren't concerning because Mr O was paying an account in his own name with a well-known cryptocurrency merchant, there was no historical spending to compare the payments with, and they didn't take place in quick succession. It further argued the fraudulent activity didn't take place primarily on the Revolut platform as Mr O sent the funds B and lost control of them further in the chain. And he didn't question the unrealistic returns or do appropriate due diligence.

Our investigator thought the complaint should be upheld. He thought Revolut ought to have been concerned when Mr O made the first payment because even though there was no spending history to compare the payments with, the transaction was a high-value payment to a well-known cryptocurrency merchant, which wasn't in line with the account opening purpose. He thought Revolut ought to have intervened and asked Mr O relevant questions and provided a tailored written warning covering the key features of cryptocurrency scams in a clear and understandable way.

Had it done so, there was no evidence Mr O had been coached to lie and so our investigator was satisfied it would have been apparent that he was falling victim to a scam. He concluded Revolut had missed an opportunity to prevent Mr O's loss and so it should refund the money he'd lost from the first payment onwards.

Our investigator further explained that he didn't think Mr O had contributed to his own loss because he was an inexperienced investor who believed he was dealing with a genuine investment company, and he'd been provided access to a professional looking trading platform when in fact he was the victim of a sophisticated scam. So, he didn't think the settlement should be reduced for contributory negligence.

Revolut has asked for the complaint to be reviewed by an Ombudsman arguing that the payments fell within Mr O's account purpose declaration, so there was no reason to suspect the activity was unusual.

It has argued that it is bound by contract, applicable regulations, and the common law to execute valid payment instructions, citing the Supreme Court's judgment in Philipp v Barclays Bank UK plc [2023] UKSC 25 where the Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, "no inquiries are needed to clarify or verify what the bank must do. The bank's duty is to execute the instruction, and any refusal or failure to do so will prima facie be a breach of duty by the bank."

It has further argued that there is no rational explanation as to why it should be held responsible in circumstances where Mr O was paying an account in his own name because it is merely an intermediate link, and there were other authorised banks and other financial institutions in the payment chain that have comparatively greater data on him than Revolut.

Revolut has also argued the settlement should be reduced by 50% for contributory negligence because it's easy to find information about L. It has referenced a review dated 7 February 2023 (the date of the first transaction) which states L "*is just another unregulated forex broker, which means the customers are not protected, and it is highly likely they will get away with your hard-earned money and there will be no regulating agency to hold them responsible":* It argues this shows Mr O failed to conduct due diligence and demonstrates the requisite degree of carelessness required to displace any liability it might otherwise have had and contributed to his own loss.

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've reached the same conclusion as our investigator. And for largely the same reasons.

Prevention

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 O 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;
- 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".*

[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_/

[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.

- 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.

- 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

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

particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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

By February 2023, firms like Revolut had been aware of the risk of multistage scams involving cryptocurrency (that is scams involving funds passing through more than one account controlled by the customer before being passed to a fraudster) 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 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. That's particularly true of payments to B. This left a smaller number of payment service providers, including Revolut, that allow customers to use their accounts to purchase cryptocurrency with few restrictions.

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 the vast 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.

So, taking into account all of the above, I am satisfied that, by the end of 2022, prior to the payments Mr O made in February and March 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

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

The payments didn't flag as suspicious on Revolut's systems. There was no spending history to compare the payments with and Mr O was paying a legitimate cryptocurrency exchange. But on 7 February 2023, he paid £6,500 from a newly opened account to a payee which was identifiably linked to cryptocurrency, having received a large credit into the account earlier that day, and the payment wasn't in line with the account opening purpose. So, I think Revolut ought to have recognised that Mr O was at risk of financial harm.

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 Mr O attempted to make the payment on 7 February 2023, knowing 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 Mr O 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 consumer 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 O's payments, such as finding the investment through an advertisement endorsed by a public figure, being assisted by a broker and being asked to download remote access software.

I've also reviewed the text conversation between Mr O and the fraudsters (though I note that Mr O appears to have spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations). I've found nothing within those conversations that suggests Mr O was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr O expressed mistrust of Revolut or financial firms in general.

Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning. I understand that Mr O did not agree to the fraudsters demands for him to pay capital gains tax on his returns and it was this request that led him to realise that he'd been scammed.

I've taken into account that Mr O had received some small withdrawals, but the weight of evidence that I've outlined persuades me that Mr O was not so taken in by the fraudsters that he wouldn't have listened to the advice of Revolut. I've also seen no evidence that Mr O wasn't provided with any cryptocurrency investment warnings by the firm from which the funds used for the scam appear to have originated (there were interactions at the time of the payments, but the warnings Mr O was given weren't relevant to the circumstances of the investment).

Therefore, on the balance of probabilities, had Revolut provided Mr O 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 broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad (as he did, of his own accord, following this payment). I'm satisfied that a timely warning to Mr O from Revolut would very likely have caused him to realise sooner that L was operating fraudulently – revealing the scam and preventing his further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr O 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.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr O might have been at risk of financial harm from fraud when he made the first 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 loss Mr O 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 Mr O's own account does not alter that fact and I think Revolut can fairly be held responsible for his loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr O has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr O could instead, or in addition, have sought to complain against those firms. But he chose not 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 O's compensation in circumstances where: he has only complained about one respondent from which his 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 O's loss from the first payment (subject to a deduction for Mr O's own contribution which I will consider below).

Should Mr O bear any responsibility for his loss?

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mr O to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

Mr O had very limited experience of investing in cryptocurrency, and I accept he didn't have a full understanding of the risks and wouldn't have known how to check the information he'd been given or that a celebrity endorsement and the use of remote access software are red flags for fraud. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he'd spoken to someone he believed was a representative from L and he'd trusted the broker and believed the trading platform was genuine and had been able to make a withdrawal early on.

Revolut has argued that Mr O failed to do reasonable due diligence and that a simple Google search would have brought up a negative review about L. But I've considered the review and while I accept it states L wasn't regulated by the FCA, it doesn't go as far as confirming the company was operating a scam, so I don't agree it would have been careless for Mr O to have gone ahead with the payments having seen the review without having warned about the scam risk by Revolut.

So, I don't think he can fairly be held responsible for his own loss.

Chargeback

Mr O's own testimony supports that he used cryptocurrency exchanges to facilitate the payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that B would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr O's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I'm satisfied Mr O 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, he is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr O didn't intend his money to go to scammers, he did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Compensation

I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I don't think Revolut needs to pay any compensation given that I don't think it acted unreasonably when it was made aware of the scam. And Mr O wasn't entitled to compensation for legal fees, as our service is free to access.

Recovery

The payments were made by card to a cryptocurrency provider. Mr O sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds.

My final decision

My final decision is that Revolut Ltd should:

- refund the money Mr O lost from the first payment onwards.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 18 November 2024.

Carolyn Bonnell
Ombudsman