DRN-5237069

The complaint

Mr W complains that Revolut Ltd did not refund a series of payments he lost to a scam.

What happened

Mr W found an advert online for a company that could help him invest in cryptocurrency. I'll refer to them as 'V' for the purposes of this decision. Unfortunately, this turned out to be a scam.

Mr W says most of the communication was via phone calls. He says he was told to download screensharing software, and this was used to facilitate the opening of accounts with various cryptocurrency providers. Mr W also opened the Revolut account to facilitate payments to the cryptocurrency wallets before passing them onto the scam. Mr W was chased for more and more money until eventually he realised that he had been the victim of a scam. The card payments from the Revolut account went from December 2022 to November 2023.

Mr W raised a scam claim with Revolut some time after the scam ended. They said they would try to raise chargeback claims for the payments and did not agree to reimburse Mr W in the meantime. However, as the card payments went to genuine merchants to purchase cryptocurrency, they could not process the chargeback claims.

Mr W referred the complaint to our service and our investigator looked into it. They felt that the payment of £2,500 Mr W made on 23 January 2023 should have been seen as unusual and that a tailored cryptocurrency warning should have been provided. And they felt it was more likely this would have revealed the scam at the time. They also felt Mr W should accept some responsibility for the loss as he said he carried out no research into the investment company before parting with his money. The Investigator therefore recommend reimbursement of 50% of the funds lost from the £2,500 payment made on 23 January 2023, which totals £11,111.72, as well as 8% simple interest on this amount from the date of the transactions to the date of settlement.

Mr W accepted the findings, but Revolut did not. They highlighted the funds moved to another account within Mr W's control and did not think the Investigator had considered earlier interventions by other banks, amongst other points. As an informal agreement could not be reached, the complaint has been passed to me for a final decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In 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 W 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 January 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 January 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

[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.

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

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

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

It isn't in dispute that Mr W fell victim to a cruel scam, nor that he authorised the card payments to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

By January 2023, when the trigger point has been established from in the view, 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.

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 W made in January 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, 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.

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 Mr W'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 W might be at a heightened risk of fraud that merited its intervention. I can see this was a new account that Mr W opened in order to facilitate payments to the scam. So, I am conscious that there was no genuine account activity for Revolut to compare the scam payments to. Looking at the payments themselves, the first three were relatively low in value with the highest being only £500. A higher value payment of £2,900 followed, but the pattern of payments up to that point would not have been concerning to Revolut. And a fifth payment of £1,120 was made a few days later, again this was relatively spaced out.

However, on 23 January 2023, Mr W made a payment of £500 to a known cryptocurrency merchant, followed by another payment of £2,500 just five minutes later, That bought the total paid that day to £3,000 across multiple payments. On balance, I think this could have

been seen as unusual and should reasonably have been a sign that Mr W may be at risk of financial harm. 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.

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

Revolut has not provided any evidence to show a warning was provided for any of the payments relating to the scam. However, Mr W was required to authenticate most of the payments made by card via 3DS security.

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 that when Mr W attempted to make the payment of £2,500 on 23 January 2023, and Revolut knew (or strongly suspected) that the payment was going to a cryptocurrency provider, it ought to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every 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 W by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr W suffered from the payment of £2,500?

I've considered whether a tailored cryptocurrency investment scam warning at the payment of £2,500 would reasonably have uncovered the scam. In doing so I have considered the features of the scam Mr W fell victim to.

Mr W found the investment opportunity online, though he has not been able to confirm exactly where he found it. Mr W was assigned an advisor, was told to download screensharing software and was heavily guided to open multiple cryptocurrency wallets in a short space of time.

Considering all of this, I think it is likely a clear warning about the typical features of cryptocurrency investment scams would have revealed the scam to Mr W. And I think it would have prevented him from making further payments towards the scam.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr W 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 she made the payments from her 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 W might have been at risk of financial harm from fraud when he made the payment of £2,500, 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 Mr W suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr W's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr W's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr W has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and he could instead, or in addition, have sought to complain against those firms. But Mr W has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr W'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 Mr W's loss from payment 4 (subject to a deduction for Mr W's own contribution which I will consider below).

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved. While the third-party account provider has confirmed one transaction to Revolut was declined on 6 January 2023, it cannot confirm if a scam warning was provided.

Should Mr W bear any responsibility for his losses?

I've finally considered whether or not Mr W should reasonably bear some responsibility for the losses as a result of any negligence in his actions and if it is therefore reasonable for me to make a reduction in the award based on this. In doing so, I've considered whether Mr W has acted as a reasonable person would to protect himself against the loss he suffered. The test is objective but needs to take account of the relevant circumstances.

In doing so, I have considered that Mr W said he did not carry out any research at all about the investment company before beginning to invest. I can see there are now some

concerning posts about V, though it is unclear how early these were available online. Though I can see some would have been available during the time in which Mr W was investing.

Mr W was also guided to open multiple cryptocurrency wallets in a short period of time and gave control of his computer over to the scammer to help facilitate payments. And he has described being chased endlessly for money by the scammers. On balance, I think he could reasonably have had concerns over a legitimate investment company continuously chasing him for more funds in the way he has described.

With the above in mind, I think it is reasonable for Revolut to reduce the reimbursement by 50% to account for Mr W's contribution to the loss.

Putting things right

Revolut Ltd should reimburse Mr W 50% of the loss from the payment of £2,500 on 23 January 2023 onwards. This totals £11,111.72.

It should add 8% simple interest from the date of the transaction to the date of settlement. If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr W how much it's taken off. It should also give him a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

I uphold Mr W's complaint in part and direct Revolut Ltd to pay the redress set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 16 April 2025.

Rebecca Norris
Ombudsman