DRN-4738154

The complaint

Miss R complains that Revolut Ltd hasn't refunded her after she fell victim to a scam.

What happened

I issued a provisional decision for this complaint on 29 October 2024. In it I set out the background and my proposed findings. I've included a copy of the provisional decision at the end of this final decision, in *italics*. I won't then repeat all of what was said here.

Both parties have now had an opportunity to respond to the provisional decision. Miss R accepted the outcome. Revolut didn't respond. As the deadline for responses has now expired, I'm going on to issue my 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.

Having done so, I'm upholding the complaint in line with my provisional findings.

As Miss R accepted those findings, and Revolut didn't respond, there is no further evidence or argument for me to consider. I see no reason to depart from the findings and reasoning I've already explained.

Putting things right

On Miss R's acceptance of this final decision, Revolut should:

- refund the £5,838 Miss R lost to the scam; *and*
- pay interest on that sum at 8% simple per year, calculated from 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 Miss R to accept or reject my decision before 10 December 2024.

Provisional decision

I've considered the relevant information about this complaint.

Having done so, I'm reaching a different outcome to that recommended by our investigator.

I'll look at any more comments and evidence that I get by 12 November 2024. But unless the

information changes my mind, my final decision is likely to be along the following lines.

The complaint

Miss R complains that Revolut Ltd hasn't refunded her after she fell victim to a scam.

What happened

Miss R received a call from someone claiming to work for a well-known cryptocurrency platform. Miss R has explained how the number appeared on her phone and displayed the name of the platform. The person she then spoke to appeared very knowledgeable and helpful, and was aware she'd lost money to a cryptocurrency investment previously. The caller said she could help Miss R recover her funds.

Miss R didn't know at the time, but she'd been contacted by a scammer. But she was convinced at the time the caller was genuine, and so listened to what they had to say.

She was told that in order to recover her lost funds she'd have to reactivate a cryptocurrency wallet as it hadn't been used in a long time, and she needed to prove she had personal financial liquidity. To do so she'd need to add funds to her wallet.

Miss R followed the scammer's instructions, including the downloading of AnyDesk. She also set up an account with Revolut to facilitate the necessary payments.

But once Miss R paid money into the cryptocurrency wallet, using her Revolut card details, it was sent on and was lost to the scam. Once Miss R realised what had happened she reported it to Revolut.

Revolut looked at the circumstances but ultimately said it wouldn't reimburse Miss R's loss. And so Miss R brought her complaint to our service, where it was considered by one of our investigators.

She said the complaint ought to be upheld as Revolut had missed an opportunity to protect Miss R from the scam. She could see Revolut intervened in the first payment Miss R attempted to make, but that the questioning and warnings that followed were insufficient. Given that failing she said Revolut ought to bear some responsibility for Miss R's loss.

Our investigator went on to say that Miss R ought also to bear some responsibility, given her own actions and the circumstances behind the scam.

Miss R agreed with the investigator's findings, but Revolut did not. And so the complaint has been passed to me for review.

What I've provisionally 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 intend to uphold it. Unless I receive persuasive new evidence or arguments from either party by 12 November 2024, my final decision will be along the following lines.

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 Miss R 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 March 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 March 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.*

---

[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.

- *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 March 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*

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

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

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

It isn't in dispute that Miss R has fallen victim to a cruel scam here, nor that she authorised the payments she made by card to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

It isn't entirely clear whether Miss R then transferred the money out of her cryptocurrency wallet onto the scammers herself, or whether this was done by the scammer, aided in part by manipulating screens and taking some control of Miss R's device using AnyDesk. But the outcome of this complaint isn't altered by whichever scenario is true.

Whilst I have set out in detail in this decision the circumstances which led Miss R 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 Miss R might be the victim of a scam.

What is evident though, is that Revolut did identify that Miss R was at risk of financial harm through fraud. That is reflected in the fact that it stopped the first attempt to pay the cryptocurrency wallet, where a £3,000 payment was declined and Miss R was directed to the in-app chat.

What did Revolut do to warn Miss R?

Revolut discussed the attempted payment with Miss R, asking her a series of questions. This culminated in the following warning being given:

Thank you for your cooperation. Please be aware that scammers are using increasingly sophisticated techniques to gather personal information and convince customers to transfer funds in complex scams. If you have any concerns then do not proceed and let us know, we will be here to further assist you. Remember, if you continue to send your money to the account details you have been provided, we cannot guarantee that we will be able to recover your money and you risk losing it.

What kind of warning should Revolut have provided?

Revolut needed to give Miss R a much more direct and detailed warning than it did. The reason being that it had been presented with information by Miss R – over and above what it already knew about the payment and the risks associated with it – that ought to have given significant cause for concern, and irrespective of its existing perceived level of risk.

Revolut did ask some relevant questions. But I can't say that it was fairly and reasonably reassured by the answers given. Miss R wasn't hiding what she was doing; she was very forthcoming in answering the questions. She told Revolut the following, in response to several different questions relating to cryptocurrency scams (though Revolut hadn't given any context for the questions being asked):

- *Ok I have access to the crypto account which is in my name. I have bitcoin waiting to exchange back to sterling but because I have not used my wallet account I need to deposit funds again*

- *My bitcoin account manager gave me instructions on how to do it*

- *Oh I see As far as I am aware I am able to withdraw*

Revolut, in its position as an industry professional, ought to have been able to recognise the common hallmarks of a cryptocurrency scam here, even without knowing the specifics or that it was a recovery scam Miss R was caught up in.

Miss R had revealed that she was paying money in to reactivate an account she'd not used in a while. There's no such requirement to do so.

She's explained that she was being directed by a 'bitcoin account manager' for which there are no legitimate services, and the suggestion of someone performing such a roll is very common in cryptocurrency related scams.

She didn't know if she could actually withdraw and hadn't attempted to do so.

Revolut ought to have picked up on these details and considered Miss R's responses more thoroughly. That ought then to have led to further questions, dynamic in nature so that they were tailored to the specific circumstances. That ought to then have culminated in a strong warning against proceeding, with an explanation as to why it was likely Miss R was falling victim to a scam.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Miss R suffered?</u>

Miss R clearly trusted the scammer and the instructions she was being given. But I've not seen any evidence to suggest she was told to lie to Revolut if it questioned what was happening. Indeed, the evidence shows that Miss R was being completely honest with Revolut.

There's then nothing to indicate that she wouldn't have listened to what Revolut had to say about scams, or that she wouldn't have heeded a proper warning. And so I'm satisfied the scam could have and should have been avoided.

<u>Is it fair and reasonable for Revolut to be held responsible for Miss R's loss?</u>

In reaching my decision about what is fair and reasonable, I have taken into account that Miss R purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, at least to some degree, she remained in control of her money after he made the payments from her 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.

In reaching my decision, I have taken into account that the payments were 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 Miss R might have been at risk of financial harm from fraud when she attempted the payment of £3,000 payment, and in those circumstances, it should have made far more if its enquiries than it did. If it had taken those steps, I am satisfied it would have prevented the losses Miss R 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 Miss R'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 Miss R 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 Miss R could instead, or in addition, have sought to complain against those firms. But Miss R 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 Miss R's compensation in circumstances where: she 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 Miss R's loss.

Should Miss R bear any responsibility for his losses?

I've thought about whether Miss R should bear any responsibility for her loss. 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 the circumstances of this complaint including taking into account Miss R's own actions and the reasonableness of them.

I recognise that there were signs that ought to have caused Miss R concern. She was contacted out of the blue by someone she didn't know. They claimed to work for one cryptocurrency platform but also to be able to facilitate the return of funds with an unconnected one. And much of Miss R's contact with the scammer was through WhatsApp, which is perhaps an unlikely platform for legitimate correspondence.

However, it appears that the scammer did know details about Miss R's previous losses. That wouldn't be very surprising as, from the limited information I know about that investment, it seems quite likely that was in and of itself a scam, I appreciate that might come as shocking and surprising news to Miss R. But it does seem a likely explanation, and might be something Miss R wants to look into further.

What is common when such an investment scam has taken place, is for there to then be a follow-up scam, where the scammers claim to be able to help in the recovery of lost funds. Details of the victims of one scam might be retained and reused to set up the follow-up

scam.

Miss R has also explained how, when she received the call, the number showed as that of the cryptocurrency provider, with its name displayed on her phone. This is a common fraud tactic and is known as number spoofing. The purpose of it is to trick the victim into believing they are receiving a call from the genuine business that is being spoofed. It's an incredibly powerful tool, as many people will trust what their device is telling them in terms of an incoming communication, meaning they in turn trust what the caller is telling them.

With these factors in mind I don't believe it would be fair to say Miss R acted so unreasonably that her compensation from Revolut ought to be reduced.

Putting things right

Subject to any further evidence or arguments made that might alter my findings, and should Miss R ultimately accept, Revolut should:

- refund the £5,838 Miss R lost to the scam; and

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

My provisional decision

*I intend to uphold this complaint against Revolut Ltd***.**
Ben Murray
Ombudsman