DRN-5228058

The complaint

Mrs N complains that Revolut Ltd hasn't protected her from losing money to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, Mrs N has explained that in April 2023 she made 11 debit card payments totalling £12,828 from her Revolut account for cryptocurrency which she then lost to a job scam.

Mrs N subsequently realised she'd been scammed and got in touch with Revolut. Ultimately, Revolut didn't reimburse Mrs N's lost funds, and Mrs N referred her complaint about Revolut to us. As our Investigator couldn't resolve the matter informally, the case has been passed to me for a decision.

I sent Mrs N and Revolut my provisional decision on 6 December 2024. Now both parties have had fair opportunity to respond, I'm ready to explain 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.

Mrs N told us that she accepts my provisional decision. And Revolut didn't respond to my provisional decision. So, in the absence of evidence or arguments persuading me otherwise, I've reached the same conclusions as in my provisional decision, and for the same reasons. I've explained my reasons again below.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted

Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mrs N 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 April 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;

[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_/

- 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 April 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

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

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – 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

[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"

(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 April 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.

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

It isn't in dispute that Mrs N has fallen victim to a scam here, nor that she authorised the payments she made to the cryptocurrency wallets (from where the cryptocurrency was subsequently transferred to the scammers).

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

By April 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 this 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 customers' 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 April 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 account to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Mrs N made in April 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at 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, it is the specific risk associated with cryptocurrency in April 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 Mrs N's own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mrs N might be at a heightened risk of fraud that merited its intervention. And I think that whilst Revolut should have identified that the first four payments were going to a cryptocurrency provider, these first four payments were relatively low in value and not of the magnitude where I'd reasonably expect Revolut to yet be concerned or think it was yet proportionate to intervene in them. However, I'd reasonably expect Revolut, when Mrs N instructed her fifth payment – which was for almost £2,000 and would take her instructed payments for cryptocurrency to almost £3,500 in less than four hours – to have provided Mrs N with a tailored written warning that covered the scam risk identified. And then, given the nature of Mrs N's in-app chat with Revolut the next day on 8 April 2023, I'd expect Revolut, on receiving Mrs N's instructions to make the sixth payment, to have escalated this intervention (as I will explain further below).

What did Revolut do to warn Mrs N?

It's my understanding that Revolut has said that Mrs N had to authorise these card payments through the 3D Secure system but that, when this was done, it didn't intervene in the payments or warn Mrs N about the possibility she was falling victim to a scam.

What kind of warning should Revolut have provided?

I've already said above that I think Revolut should first have provided Mrs N with a tailored written warning that covered the scam risk identified when she instructed her fifth payment. I think, however, that when Mrs N instructed her sixth payment that a proportionate response to the escalation in risk presented by the surrounding context would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs N's account. I think it should have done this by, for example, directing Mrs N to its in-app chat to discuss the payment further. I say this because:

- Mrs N's first five payments were all made on 7 April 2023. And the in-app chat history presented by Revolut shows that the morning after, Mrs N got in touch with Revolut in the in-app chat to ask if Revolut could cancel her card because she'd accidentally shown a screenshot of her card and CVV number to someone and she wanted to make sure this card was now deleted/cancelled. Revolut asked Mrs N who she'd shown her card to, and Mrs N replied, *"It was a mentor trying to help me generate money through a programme"* and *"She suggested I download Revolut as a means to place money into and to also withdraw to"*. Revolut asked Mrs N if she had any unauthorised transactions and Mrs N said, *"Not yet but I am afraid I might once I get my salary"*.

- There wasn't any other activity on Mrs N's Revolut account that Revolut might reasonably have thought this concerned. And Revolut ought reasonably already, as I've said, to have been sufficiently concerned to have provided Mrs N with a tailored written warning.

- As I've said, our service has 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. This is what was happening here, and Revolut now knew this from what Mrs N said in the chat – that a mentor trying to help her make money had suggested she download the Revolut app. I think this ought to have been a very clear red flag to Revolut such that it ought to have escalated its intervention either at this point or when Mrs N instructed her next payment – which was the sixth payment later that day also for cryptocurrency.

If Revolut had provided a warning of the type described, would that have prevented the losses Mrs N suffered from the fifth or sixth payment onwards?

I'm not persuaded an appropriately tailored written warning that covered the scam risk identified would most likely have stopped Mrs N from proceeding with the payments. I say this because I think at the time, given the prevalence of cryptocurrency *investment* scams, in April 2023, at the date of these payments, the most effective way for Revolut to limit harm caused by cryptocurrency-related transactions was to give a warning related to cryptocurrency investment scams, tackling some of the key features of the scam, so as not to be so broad as to dilute things by covering off too many different scam risks. But I don't think this would have resonated with Mrs N, given that she wasn't falling victim to a cryptocurrency investment scam, but instead a fake job opportunity which required her to

complete tasks and to make cryptocurrency payments. I appreciate this isn't ideal for Mrs N, but I wouldn't expect Revolut to have done more than this yet, and I don't think this likely would have prevented Mrs N from still proceeding with her payments.

However, as I've said, I think Revolut's intervention ought to have been escalated to an in-app chat when Mrs N instructed her sixth payment.

I've thought really carefully about what I think would then have happened, and I think this is a close call. This is because I'm aware that the funds used for the scam originated from Mrs N's account with a third-party bank "S", and S *did* intervene and spoke to Mrs N before she sent money from her account with S to her Revolut account that would ultimately fund her last two payments from Revolut to her crypto wallet. During this intervention, Mrs N wasn't upfront with S. It's also apparent, having reviewed the messages exchanged between Mrs N and the scammers, that Mrs N was somewhat tricked by the scammers and quite under the spell at least at some points. However, whilst it is therefore a possibility that if Revolut had intervened in-app as I think it should have, that Mrs N wouldn't have been upfront with Revolut and/or Revolut's intervention ultimately wouldn't have prevented her from making the payments anyway, I think in this case it's more likely that it would have. I say this because the intervention from S occurred on 12 April 2023, at a materially different point of the scam – at which point it's clear from the evidence of messages exchanged that Mrs N was concerned but ultimately decided to go "all-in" in a final attempt to withdraw her "earnings" because she was somewhat desperate. However, at the point Revolut ought to have intervened in-app, on 8 April 2023, the scam was at a different stage: Revolut already had good information about the likely nature of the payments from what Mrs N had already told it in the chat; and I think it probably ought to have been able to quickly get the context and give Mrs N a really strong warning about the typical features of job scams. I think at this stage, this likely would have resonated with Mrs N, who clearly didn't trust the scammers at this point or else she wouldn't have been concerned about her card. So I think that had Revolut done what it should have done at this point, it's more likely than not that Mrs N would have stopped, considered things, perhaps discussed things with her husband, and ultimately not have proceeded with the sixth payment nor the subsequent ones.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs N transferred money from her account with S to her Revolut account before transferring it on again to crypto wallets.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs N might have been at risk of financial harm from fraud when she made the sixth 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 most likely have prevented the losses Mrs N suffered from the sixth payment onwards. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mrs N's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs N's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

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

I'm also not persuaded it would be fair to reduce Mrs N's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mrs N's loss from the sixth payment onwards which amounts to £9,371 (subject to a deduction for Mrs N's own contribution which I will consider below).

Should Mrs N bear any responsibility for her loss?

I've thought about whether Mrs N should bear any responsibility for the loss of the £9,371 I've said Revolut should have prevented. 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 the circumstances of this complaint.

In this case, I don't think it's unfair to say Mrs N really wasn't as careful as she should have been. It's clear from the messages she exchanged that Mrs N really ought to have realised before she made the sixth payment that things looked too good to be true and that something didn't seem right, but she proceeded anyway. I'm persuaded in the circumstances of this case that it's therefore fair that Mrs N shares responsibility for the loss with Revolut, such that Revolut should pay Mrs N 50% of the £9,371 loss, and so £4,685.50.

Recovery

For completeness, I'll address recovery. After these payments were made, because they were debit card payments, the only potential avenue to recover them would have been through the chargeback scheme. However, Mrs N didn't make the debit card payments to the scammers. Instead she made them to legitimate crypto exchanges, which would have provided the services intended. So Revolut could only have brought chargeback claims against the crypto exchanges (and not the scammers) but these wouldn't have succeeded given the circumstances. So I can't say Revolut therefore unreasonably hindered recovery of the funds.

Interest

I consider 8% simple interest per year fairly reflects the fact Mrs N has been deprived of this money. So Revolut should also pay Mrs N interest on the £4,685.50 from the date of loss to the date of settlement calculated at this rate.

My final decision

For the reasons explained, I uphold this complaint in part and I direct Revolut Ltd to pay Mrs N:

- £4,685.50; plus
- interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement (if Revolut deducts tax from this interest, it should send Mrs N the appropriate tax deduction certificate).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs N to accept or reject my decision before 19 January 2025.

Neil Bridge
Ombudsman