DRN-4848125

The complaint

Mr N complains about Revolut Ltd.

He says that Revolut didn't do enough to protect him when he became the victim of a scam and would like it to refund him the money he has lost as a result.

What happened

Mr N received a message from an individual claiming to work for a recruitment agent, supposedly offering task-based remote work. Mr N was interested in the opportunity and agreed to take up the role. Unfortunately, the opportunity was actually a scam.

Mr N was required to purchase tasks and would then earn a commission. The tasks would be purchased via cryptocurrency, which Mr N bought by moving funds from his account with L (another bank) to Revolut and then purchased crypto from his account with Revolut, which was transferred to the scammer.

Mr N made the following payments.

Payment	Date	Payment type	Payee	Amount
1	2 July 2023	Faster payment	NT	£1,700
2	3 July 2023	Faster payment	NT	£1,002
3	4 July 2023	Faster payment	NT	£4,555
4	4 July 2023	Faster payment	NT	£3,640
5	5 July 2023	Faster payment	NT	£5,000
6	5 July 2023	Faster payment	NT	£2,235
7	5 July 2023	Faster payment	NT	£2,550
8	7 July 2023	Faster payment	NT	£2,256
			Total	**£22,938**

Mr N made a complaint to Revolut, but it didn't uphold his complaint. Mr N then brought his complaint to this Service.

Our Investigator looked into things and thought that Mr N's complaint should be upheld in part – and that Mr N should also bear some responsibility for the loss due to contributory negligence.

Neither Mr N or Revolut agreed with this, so the complaint was passed to me for a final decision.

I have previously written to Mr N and Revolut and explained that I also thought Mr N's complaint should be upheld in part – but that Revolut should have intervened earlier than it did.

As the time I provided for further comment has now passed, I will make my final decision on the matter.

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 deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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 N modified the starting position described in *Philipp,* by 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*".

So Revolut was required by the implied terms of its contract with Mr N and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

---

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in July 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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 do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, 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)[3].
- 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[4], which a number of banks and trade associations were

[2] 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_/

[3] 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.

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

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.

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 July 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 Mr N was at risk of financial harm from fraud?

It isn't in dispute that Mr N has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in this decision the circumstances which led Mr N to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr N might be the victim of a scam.

---

[5]See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.

[6] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022

By July 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

However, by the end of 2022 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[5]. And by July 2023, when these payments took place, further restrictions were in place[6]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

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

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr N made in August 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in July 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mr N'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 N might be at a heightened risk of fraud that merited its intervention.

With this in mind, I think that Revolut ought to have been concerned about the payments Mr N was making from payment 3 – it was clearly going to a crypto exchange, and the payments Mr N was making had increased quickly in only a day – so I think that it should have intervened with a written warning at this time to alert Mr N that there may be a problem. But I am also aware that Mr N had fallen victim to a job scam – which was not the most common type of scam at this time – so I wouldn't have expected the warning it should have provided to have included this type of scam.

However, by payment 4, Mr N had now paid out over £10,000 in only 24 hours to a crypto exchange – which I think should have given Revolut serious concerns about what was happening – and it should have taken further steps to warn Mr N before this payment went ahead.

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

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by July 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Mr N?

Revolut has told this Service that it showed Mr N a new payee warning when the payee was set up on 2 July 2023 – and that when he selected the payment purpose of 'cryptocurrency' for payments 1 and 2, he was shown a warning at this time – but while these warnings didn't apply to the type of scam Mr N fell victim to, I don't feel that these warnings would have been effective in bringing to life the key features of a crypto investment scam in either. It didn't provide any further warnings to Mr N for any of the following payments.

What kind of warning should Revolut have provided?

While I accept that Revolut has attempted some steps to prevent harm from fraud, the warnings it provided were too generic and not applicable to this particular scam to have had the necessary impact required here.

Having thought carefully about the risk payment 4 presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mr N's account. I think it should have done this by, for example, directing Mr N to its in-app chat to discuss the payment further, and having established the facts, provided Mr N with a warning about what he was doing.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr N suffered from payment 4?

Had Revolut got in touch as I would have expected, I think it would have asked him about what the purpose of the payments was, and why Mr N was making them.

I haven't seen anything to suggest Mr N would have hidden this from Revolut – he had already told it he was purchasing crypto – so I think that he would have also told it that the payment was part of a job, and that he had been sent an unsolicited message about the opportunity. Once Revolut was privy to this information – I think that this would have appeared very unusual to it, and immediately recognised this very likely to be a scam – it is not normal to pay for employment, and even more unusual to be asked to pay via crypto.

It would have been able to provide a very clear warning and, given that Mr N had no desire to lose his money and nothing to gain from going ahead with the payments, it's very likely that he would have stopped, not followed the fraudster's instructions and the loss would have been prevented.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut is essentially the 'middleman' in the transaction journey leading to the ultimate loss – the funds were originally transferred from L to Revolut, and Mr N purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that payment 4 was made to another financial business (a cryptocurrency exchange based in another country) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out above, I think that Revolut still should have recognised that Mr N might have been at risk of financial harm from fraud when he made payment 4, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mr N 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 N's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr 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.

Ultimately, I must consider the complaint that has been 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 N's loss from payment 4 (subject to a deduction for Mr N's own contribution which I will consider below).

Should Mr N bear any responsibility for his losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

While I do think that Revolut should have done more to prevent Mr N's loss from this point, Mr N also wasn't as careful with his money as he should have been. He received an unsolicited message from an individual offering employment which he didn't need to apply for, and received no employment contract, or documentation prior to starting the supposed job – and was asked to part with money in order to fund his own job – which should have seemed highly unusual to him. The salary and returns promised were also too good to be true – and should have raised questions about the legitimacy of the opportunity presented to him.

And while I know that Mr N did carry out some checks before parting with his money, I don't think that the steps he took were thorough enough or went far enough to verify what he had been told, before parting with a significant amount of his money.

On this basis, I think that it is fair that responsibility for the loss from payment 4 should be shared between Revolut and Mr N – on a 50% basis each. Revolut was ultimately the more knowledgeable party – and had more experience of these types of scams than Mr N – and it missed an opportunity to provide him with a meaningful warning about what he was doing, so I don't think that a higher deduction would be appropriate in these circumstances.

Putting things right

Revolut Ltd should refund Mr N 50% of the payments from and including payment 4.

I calculate this to be £7,840.50.

On top of this Revolut Ltd should also pay Mr N 8% simple interest from the date the payments were made until settlement (less any lawfully deductible tax).

My final decision

I uphold this complaint in part. Revolut should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 10 October 2024.

Claire Pugh
Ombudsman