DRN-4701466

The complaint

Mr N is unhappy that Revolut Ltd won't reimburse money he lost to a scam.

What happened

On 29 February 2024 I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Mr N was looking for job opportunities online. He thought he'd found a role which involved promoting products. He corresponded with his proposed employers over a popular instant messaging service and was provided with access to an online platform – "W".

The fraudster explained that "our role is to help merchant improve their product reviews and portfolio packaging products by creating consumer data on the W third-party platform so they can sell more products". Mr N appears to have been given an hour of 'training' and initially promised $80-200 commission per day, as well as a bonus of $500 for meeting his target for five consecutive days. It was also claimed that the 'base salary' was $5,800.

Over the course of the following few days, it was explained to Mr N that he would actually need to deposit money onto the platform in USDT (a U.S. Dollar linked 'stablecoin') as part of his role. Mr N questioned this and was told "we need the cost to enhance the product because the company needs real data to help merchant enhance their products, but rest assured the USDT we use is just an advance payment that will not be consumed and we can recoup our money including profit after completing the product".

As early as 9 August 2023, Mr N seems to have recognised the issue with this arrangement, saying "but [I] still don't understand how I make money from this because I deposited 27 yesterday and also if I deposit 100, I am at a loss". He was reassured that he'd receive his profits and be able to withdraw after completing '80 boosts'.

As is common with this type of scam, Mr N was given "packages of products" which had to be completed in full before any withdrawal could be made. But before Mr N could 'complete' a package, he'd be given a new one (apparently by chance), such that he'd never be able to complete his packages and withdraw his money. Each package he was given would reduce the balance of his account and require him to 'recharge' (i.e. pay more money) to bring him back to a positive balance (and in theory to be able to withdraw his money). These packages became increasingly expensive and Mr N was told he'd need to deposit increasingly large sums or risk losing all of the commission he'd earnt and any money he'd deposited.

By 12 August 2023, Mr N appears to have essentially run out of money and was encouraged to borrow from his friends and family. He questioned this and suggested that the scheme was sounding 'scammy' and that the whole process was 'fraudulent' as he was unable to withdraw his initial deposits. At this point he reported the matter as a scam to the banks he'd made payments from up to this point. However, Mr N was persuaded by the fraudsters to

continue making deposits or risk losing the money he'd already deposited. After borrowing money from friends and family and opening a Revolut account, he began making payments towards the scheme from his Revolut account. After 22 August 2023 Mr N said that he had no more money to give and, once again accepting he'd been the victim of a scam, he reported the matter to Revolut.

Mr N made four payments using his Revolut debit card to a genuine cryptocurrency provider – "B" between 18 and 22 August 2023. From B he sent cryptocurrency to e-wallet addresses provided to him by W. All of the payments prior to 18 August 2023 took place from his accounts at other financial businesses. The payments from his Revolut account are set out below:

Date	*Amounts*	*Type of payment*	*Recipient*
18 August 2023	*£2,111.89*	*Debit card*	*B*
20 August 2023	*£3,314.82*	*Debit card*	*B*
22 August 2023	*£807.08*	*Debit card*	*B*
22 August 2023	*£238.50*	*Debit card*	*B*

Mr N reported the matter to Revolut, but it said that it wasn't responsible for his loss. In summary it argued:

- *Mr N reported the transactions as being fraudulent, but it couldn't raise a chargeback on that basis because they had all been authorised by Mr N and were for the benefit of genuine merchants, which had provided legitimate services to Mr N.*
- *The fraudulent activity did not take place on the Revolut platform, but rather the cryptocurrency platform. Revolut was only an intermediate link between Mr N's bank account and the cryptocurrency platform.*
- *The transactions were spread out over four days and it had no previous account activity to compare the transactions against.*
- *It was required to process payments without undue delay and the starting position in law is that liability rests with the payer, even if they've been duped into making the payments.*

Mr N referred the matter to our service, but one of our Investigators didn't uphold the complaint. He thought that Revolut should have found the £3,314.82 payment Mr N made ("the 20 August Payment") to be concerning, such that it ought to have provided a written warning to him. But the Investigator thought that such a warning should cover off the most common cryptocurrency scam risk – that of cryptocurrency investment scams. As Mr N wasn't falling victim to this type of scam, the Investigator didn't think such a warning would have resonated with Mr N and, therefore, he would have made the payment regardless.

Mr N disagreed. He said that it was wrong to assume that he would have continued with the payments if he had been warned.

As no agreement could be reached, the case was passed to me for a final decision.

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.

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

For the reasons I shall set out below, I am minded to conclude that when Mr N made the 20 August Payment Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely cryptocurrency related scam Mr N was at risk from. But, had it done this, I'm not persuaded that Mr N would have stopped making that payment and I don't think his losses from that point onwards would have been prevented. I'll explain why.

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.*
- *The express terms of the current account contract may modify or alter that position. For example, 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 duty to do so.*

In this case, the terms of Revolut's contract with Mr N at the time did expressly allow it to refuse or delay a payment for a number of reasons, but those reasons did not explicitly include circumstances where Revolut believes its customer is at risk of financial harm from fraud.

So Revolut was required by the implied terms of its contract with Mr N and the Payment Services Regulations to carry out Mr N's instructions promptly, and (as Philipp reiterated) it was not under a contractual duty or obligation to concern itself with the wisdom of Mr N's payment decisions.

But the requirement to carry out an instruction promptly does not mean immediately[1]. And whilst Revolut was not required or obliged under its contract with Mr N to concern itself with the wisdom of Mr N's payment decisions – for example by making fraud related enquiries – the contractual requirement to make payments promptly did not prevent it from doing so either.

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 regulatory expectations and requirements (including the Financial Conduct Authority's "Consumer Duty") and what I consider to have been good industry practice at the time, Revolut should in August 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.

In reaching that view, 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.*

For example, it is my understanding that in August 2023, Revolut operated a process whereby if it identified a scam risk associated with a card payment through its automated systems, it might initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat). If Revolut was satisfied with the response to those questions and/or it provided a relevant warning, it would then allow the consumer to make the payment.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- *FCA regulated firms are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2).*
- *Over the years, the FSA, and its successor the FCA, 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).*
- *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*

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

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.

- *Since 31 July 2023, under the FCA's Consumer Duty[4], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G), and one example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was "consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[5]*

- *Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[6]. 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 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 August 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;*
- *have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams;*
- *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*

[4] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6) As from 31 July 2023 the Consumer Duty applies to all open products and services.
[5] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)
[6] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

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 disputed payments he made to his cryptocurrency wallet (where his funds were subsequently transferred to the scammer).

Whilst I have set out in detail in this provisional 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 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.

I'm aware that cryptocurrency exchanges like B generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments in question for the purchase of cryptocurrency would be credited to a cryptocurrency wallet held in Mr N's name.

However, by August 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.

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[7]. And by August 2023, when these payments took place, further restrictions were in place[8]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions.

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

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr 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

---

[7] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

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

to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And, as I've set out, the introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Revolut to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.

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 likelihood that most of 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 been concerned that Mr N was likely at heightened risk of fraud.

I think Revolut should have identified that the payment on 18 August 2023 was going to a cryptocurrency provider (it was being paid to a fairly well-known cryptocurrency exchange). That payment was also larger than any payments that had taken place previously on his account. But I'm mindful that the account had only been open a few days and there had been very limited activity. Taking into account that Revolut needs to strike a balance between protecting against fraud and not unduly hindering legitimate transactions, as well as the value of this payment, I don't think Revolut ought to have been so concerned about this payment that it ought to have provided warnings to Mr N at this point.

However, the 20 August Payment was larger in value and it came just two days after the previous payment. Taking that into account, as well as what Revolut knew about the destination of the payment, I think it should have considered that Mr N could be at heightened risk of financial harm from fraud and, in line with good industry practice, warned its customer before the 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 (and those which came before it) that, in combination with the fact the payment went to a cryptocurrency provider, ought to have prompted a warning.

<u>What kind of warning should Revolut have provided?</u>

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 primary duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying

the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by August 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. As I explained earlier in this decision, I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment. I also understand in relation to Faster Payments it already had systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider a firm should by August 2023, on identifying a heightened scam risk, have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that the 20 August Payment was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I am satisfied that, by August 2023, fairly and reasonably, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mr N made the 20 August Payment, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely cryptocurrency related scam Mr N was at risk from.

In this case, Mr N was falling victim to a 'job scam' – he believed he was making payments in order to receive an income.

As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Mr N gave. I'd expect any such warning to have covered off key features of such a scam, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw any money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Mr N wouldn't have done so here.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Mr N suffered from the 20 August Payment and those that followed?</u>

Mr N insists that a warning about this kind of scam would have prevented his losses. Revolut didn't provide any warnings and, as far as I'm aware, Mr N did not receive any warnings specific to 'job scams' from any other firm either.

However, I'm not persuaded that, had Revolut given a warning of the type I've described, this would have made a difference to Mr N's decision to go ahead with the 20 August Payment.

As I've set out, prior to making the payments from his Revolut account, Mr N reported that he'd fallen victim to a scam to two other banks (from which he'd made payments towards the scheme). I haven't seen any of the correspondence between Mr N and one of those banks – but I understand he had a telephone conversation with it and it refunded a transaction.

I have seen his report to the other bank. Mr N said initially he was 'unaware this was a scam' and had made the payments to the scam 'assuming this is all genuine' but 'this was not the case' and he cannot go on making deposits 'in good conscience'. While that bank doesn't appear to have responded to Mr N's claim in any detail until after he made the 20 August Payment, it's clear that Mr N recognised that he'd fallen victim to a scam.

I understand what tempted Mr N back to the scheme was the reality that he'd lose the money he'd already paid if he didn't continue to make more payments. But, I have to conclude that Mr N made those payments with, at the very least, a very strong suspicion that he had been the victim of a scam.

So, I have to consider what the impact of the kind of warning that I've described would have been in circumstances where Mr N had already recognised, not just that he was falling victim to a scam, but how that scam operated – that it would continually require him to deposit more money. In those circumstances, I think a warning would have done little more than highlight the risks he was already aware of (and had already decided to accept).

While it's possible that a further warning might have tipped Mr N back towards disbelief in the scam, I don't think that's more likely than not. So, I don't think I can fairly conclude that Revolut's failure to provide such a warning has caused his loss from the 20 August Payment (or those which followed it).

Could Revolut have done anything to recover Mr N's money?

As the payments were made by card and sent to a cryptocurrency account held in Mr N's name, Revolut would not have been able to recover the funds. I don't consider that a chargeback would have had any prospect of success given there's no dispute that B provided cryptocurrency to Mr N, which he subsequently sent to the fraudsters.

My provisional decision

For the reasons I've explained, my provisional decision is that I do not uphold this complaint.

Revolut said it agreed with the overall outcome and didn't think it was necessary to provide any additional comments or evidence.

Mr N didn't agree with my provisional decision. In summary he said:

- He only became aware of the fraudulent nature of the scheme after he made the initial payments. He was manipulated and pressured into borrowing money to keep making payments.

- He continued to make payments after he'd reported the matter as a scam because he was threatened with losing the money he'd already paid.

- It was difficult for him to identify that the scheme was definitely fraudulent due to the sophistication of the scam.

- Revolut should have provided a warning to him of the type I've described, particularly

as the payments he made were going to a cryptocurrency provider. He thinks that such a warning might have prompted him to reconsider his decision to make the payments.

- The loss of the money has had a significant impact on his mental health and this should be taken into account.

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.

I know that this scam has had a significant impact on Mr N and I'm sorry that he's been the victim of a cruel scam. However, I've explained that while I think Revolut should have provided a warning of the type I've described, I need to consider whether its failure to do so, on the balance of probabilities, caused some of Mr N's loss.

I don't doubt how convincing the scheme was to Mr N and I understand that the threat of losing the money he'd already paid to the fraudsters was what encouraged him to continue making payments even after he'd reported the matter as a scam to two banks. But, as I've set out, it appears it was exactly that (understandable) desire to recover his earlier payments that was a powerful motivation in him continuing to make payments, despite his very clear doubts about the legitimacy of the scheme. In those circumstances, and having taken into account Mr N's further submissions on this point, I continue not to be persuaded that Mr N would have been receptive to a warning of the type I've described. That means I'm not going to depart from the conclusion reached in my provisional decision and I've decided not to uphold this complaint.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 25 April 2024.

Rich Drury
Ombudsman