DRN-5012020

The complaint

Mr T is unhappy that Revolut Ltd ("Revolut") won't refund the money he lost to job scam.

What happened

In October 2023 Mr T came across remote job opportunity which involved completing tasks for commission. Mr T signed up to the job platform where he would complete his tasks and he could see his commission building up. Mr T was then assigned a set of 'combination' tasks he was told attracted higher commission but also caused his balance on the job platform to turn negative. Mr T then needed to clear the negative balance by way of a deposit in cryptocurrency in order to unlock further tasks and earn the commission.
As a result of the scam Mr T made the following payments to two genuine cryptocurrency providers M and S.

Payment #	Date	Type	Amount
1	10 October 2023	Card payment to M	£84.80
2	10 October 2023	Card payment to M	£76
3	11 October 2023	Card payment to M	£300
4	11 October 2023	Card payment to M	£750
5	11 October 2023	Card payment to M	£1,450
6	11 October 2023	Card payment to M	£3,389
7	18 October 2023	Card payment to S	£2,500
8	18 October 2023	Card payment to S	£2,500

The cryptocurrency was placed in wallets in Mr T's own name and from there he transferred the cryptocurrency to what he thought was the job platform but unbeknown to him at the time was actually going to the scammer. Mr T followed the instructions of the scammer until the deposit amounts became too high and then realised he'd been the victim of a scam.

Revolut declined to refund Mr T. It said they blocked his card on five payments which meant he had to log in in order to unblock his card. It said this ought to have caused Mr T to realise the payments he was making were likely to be a scam. They released the payments once Mr T confirmed he was authorising them. Revolut also argued that:

- The payments were authorised and such payment should proceed without undue delay.
- The payments weren't unusual or out of character.
- It blocked the card at the beginning of the scam, yet Mr T disregarded its intervention.
- There is a high degree of negligence in this case.
- The customer owned the beneficiary accounts.

Our investigator upheld the complaint in part. He felt by the sixth payment Revolut ought to have recognised that Mr T was at risk of financial harm from fraud. He considered Revolut

should have asked a series of questions about the payments Mr T was making in order to attempt to narrow down the specific scam risk and then provide a warning which covered off the key features of the scam risk it identified. However, he also felt it was fair for Mr T to share in the responsibility for his loss and therefore it was fair for Revolut to reduce the refund on the last three payments by 50%.

Mr T accepted the view, but Revolut did not accept the outcome. As the complaint has not been resolved informally, it's been passed to me for a 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.

When considering what is fair and reasonable, I'm also required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

Where I can't know for certain what has or would have happened, I need to weigh up the evidence available and make my decision on the balance of probabilities – in other words what I think is more likely than not to have happened in the circumstances.

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 T 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*".

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***

We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:

- *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 T and the Payment Services Regulations to carry out his instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should, in October 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And, I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But 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 October 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 do 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 October 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).

- 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[2], which a number of banks and trade associations were

[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] 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).

- Since 31 July 2023, under the FCA's Consumer Duty[3], 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). 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"[4].*

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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 October 2023 that Revolut should:

---

[3] 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.
[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)
[5] 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.

- 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 and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in October 2023, Revolut should in any event have taken these steps.

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

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

Whilst we now know the circumstances which led Mr T 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 T might be the victim of a scam.

I understand that cryptocurrency exchanges like M and S 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 the payments would be credited to a cryptocurrency wallet held in Mr T's name.

By October 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[6]. And by October 2023, further restrictions were in place[7]. 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 T made in October 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. 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 T'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 T might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider) but the initial payments were low in value and spread out. So I don't think Revolut should reasonably have suspected that they might be part of a scam.

On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of the first five payments, I don't think Revolut ought to have been sufficiently concerned about the first five payments that it would be fair and reasonable to expect it to have provided warnings to Mr T at this point.

---

[6] 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.

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

But by the sixth payment, given the sum involved and the pattern (increasing sums and frequency) that was emerging along with what Revolut knew about the destination of payment six, I think that the circumstances should have led Revolut to consider that Mr T was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before the sixth 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.

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 October 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 kind of warning should Revolut have provided?

Revolut hasn't submitted it provided any warnings in this case. Although it did decline a number of transactions (set out in the investigator's view) but other than asking Mr T if it was he who was authorising the transactions, it did not provide any scam warnings. So 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 October 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. I 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 that by October 2023, on identifying a heightened scam risk, a firm such as Revolut should 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 sixth 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 October 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mr T made the sixth 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 T was at risk from.

In this case, Mr T 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 T 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 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 T wouldn't have done so here.

I accept that there are a wide range of scams that could involve payments to cryptocurrency providers. I am also mindful that those scams will inevitably evolve over time (including in response to fraud prevention measures implemented by banks and EMI's), creating ongoing challenges for banks and EMI's.

In finding Revolut should have identified that the sixth payment presented a potential scam risk and that it ought to have taken steps to narrow down the nature of that risk, I do not suggest Revolut would, or should, have been able to identify every conceivable or possible type of scam that might impact its customers. I accept there may be scams which, due to their unusual nature, would not be easily identifiable through systems or processes designed to identify, as far as possible, the actual scam that might be taking place and then to provide tailored effective warnings relevant to that scam.

But I am not persuaded that 'job scams' would have been disproportionately difficult to identify through a series of automated questions (as demonstrated by Revolut's current warnings – which seek to do exactly that) or were not sufficiently prevalent at the time that it would be unreasonable for Revolut to have provided warnings about them, for example through an automated system.

I have thought about the prevalence of 'job scams' in October 2023 and I am satisfied that this was a sufficiently common scam. For example, I'm aware, from my own experience of considering complaints involving similar scams, that:

In March 2023, several months before Mr T's payments, another EMI offered "paying to earn money by working online" as a payment option as part of its system designed to (i) identify

the purpose of payments and (ii) provide tailored warnings to the common scam types associated with those payment reasons. Where the consumer selected this option, the EMI then provided a warning about job scams (like the one Mr T fell for) where the consumer is asked to pay money and then start earning by watching ads or writing reviews before then being asked to pay greater amounts over time. It encouraged the consumer to 'stop' as 'this is a scam'. Those warnings involved APP not card payments, but they support my view that job scams of this nature were sufficiently common and well known to feature in scam prevention systems in October 2023.

Versions of job scams have been around for some years (and in many countries). For example, one such example – about which the Financial Ombudsman Service received complaints at the time – featured in an article in the Sun in March 2022 https://www.thesun.co.uk/money/18068901/five-ways-crooks-cost-living/ and a very similar scam was described in a Which? article in June 2023 - https://www.which.co.uk/news/article/job-scams-fraudsters-are-posing-as-employers-and-recruiters-on-indeed-and-linkedin-a7NNv8L84n97. And data from Ofcom published in March 2023 found that of 43 million adults who have encountered scams or fraud online, 30% have come across content related to fake employment scams.

The Financial Ombudsman Service has issued numerous final decisions relating to this type of scam, including some against Revolut, many of which relate to events which pre-date October 2023.

Regarding the overall feasibility of providing a warning using the automated systems example I have referred to (and being mindful that other options are available to establish the purpose of a payment – including human intervention), I note:

- Revolut itself was able to introduce a similar process in October 2023 – around the time the payments were made.

- I am aware from other cases that in October 2023 it could have declined the payment to provide warnings through its chat function (whether or not in practice it did); and

- As I have explained above, the Consumer Duty (which came into force on 31 July 2023 after an extended implementation period), required Revolut to take steps to avoid foreseeable harm – for example by having adequate systems in place to detect and prevent scams from 31 July 2023.

As I've set out, I accept that under the relevant card scheme rules Revolut cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Revolut ought to have initially declined the £3,389 payment in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Mr T attempted the payment again, should Revolut have made the payment.

And as I've set out above it did have systems in place by October 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time.

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

I think that a warning of the type I've described would have identified that Mr T's circumstances matched an increasingly common type of scam.

I've read the instant message conversation between Mr T and the fraudsters. That conversation suggests that prior to the sixth payment he'd been asked to place deposits in quick succession and queried this with the scammer. I don't think it would have taken much persuasion (that a warning could have provided) to convince him that he was falling victim to a scam prior to making that payment.

I appreciate Revolut may question what steps have been taken to establish whether any other financial business involved in the payments Mr T made might have provided warnings that he should have taken notice of. But most of the payments here were funded by friends and although there were a few payments from Mr T's high street bank – looking at the sums, pattern and account history of that account make it, in my view, very unlikely that any warnings were provided by Mr T's bank that would have alerted him to the possibility he was being scammed.

Overall, I think that a warning provided by Revolut would have given the perspective Mr T needed, reinforcing his own developing concerns and he would more likely than not have concluded that the scheme was not genuine. In those circumstances I think, he's likely to have decided not to go ahead with the sixth payment, had such a warning been given.

Is it fair and reasonable for Revolut to be held responsible for Mr T's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr T 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 the payments were made to another financial business (a cryptocurrency exchange). The payments that funded the scam were made from other accounts at regulated financial businesses (though some of those accounts were not held in Mr T's name).

But as I've set out in some detail above, I think that Revolut still should have recognised that consumer might have been at risk of financial harm from fraud when he 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 have prevented the losses Mr T 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 Mr T's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr T's loss in such circumstances. I don't think

there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr T 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 Mr T could instead, or in addition, have sought to complain against those firms. But Mr T has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

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

Should Mr T bear any responsibility for his losses?

I've thought about whether Mr T should bear any responsibility for his loss connected to the payments. 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 of the circumstances of this complaint including taking into account Mr T's own actions and responsibility for the losses he has suffered.

Mr T accepted the investigator's conclusions to make a deduction for 50%, but broadly I agree for the same reasons:

I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking platform, which was used to access and manage Mr T's apparent earnings and tasks.

But the scam appears to have had some features that made its plausibility questionable - certainly by the time of the sixth payment. I think that on some level Mr T ought reasonably to have questioned whether the activity he was tasked with carrying out (which does not appear to be unduly time-consuming or difficult) was capable of generating the returns promised. And at the point at which he was required to make a further substantial payment. Indeed, the messages indicate he *did* question the repeated requirement for further deposits and whether this was a scam.

I recognise that the scam operates on a cruel mechanism – always making the victim believe that one final payment will allow them to get back what they've put in. But I think Mr T should have become increasingly aware of (and to some extent appears to have recognised) this risk before making the payments I am asking Revolut to refund.

So, given the above, I think he ought reasonably to have realised that there was a possibility that the scheme wasn't genuine (before going ahead with the sixth payment). In those circumstances, I think it fair that he should bear some responsibility for his losses.

For the avoidance of doubt, it is not my finding that Mr T knew that he was likely falling victim to a scam and went ahead anyway. Rather my finding is that he seems – to some extent – to have recognised that the platform could prevent him from withdrawing funds by continuously granting him combination tasks. I consider he could have realised from this and the other information available to him, that there was a possibility that the employment scheme wasn't genuine or that he might not recover his money. In those circumstances it would not be fair to require Revolut to compensate him for the full amount of his losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mr T in relation to the payments because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything to recover Mr T's money?

The payments were made by card to a cryptocurrency provider. Mr T sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds.

In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that M and S provided cryptocurrency to Mr T, which he subsequently sent to the fraudsters.

Putting things right

To put things right for Mr T Revolut Ltd should

- Reimburse 50% of Mr T's loss for payments 6, 7 and 8 (so 50% of £8,389)
- As Mr T has been deprived of the use of this money - pay interest on the above refund calculated at 8% simple per year * from the date the transactions were made to the date of settlement.

*****If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Mr T how much it's taken off. It should also provide a tax deduction certificate if Mr T asks for one, so the tax can be reclaimed from HM Revenue & Customs if appropriate.

My final decision

My final decision is that I uphold this complaint in part, and I require Revolut Ltd to put things right for Mr T as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 9 May 2025.

Kathryn Milne
Ombudsman