DRN-4967784

The complaint

Mr M complains that Revolut Ltd won't refund money he lost when he fell victim to an employment scam.

Mr M is being represented by a claims management company in this complaint.

What happened

In August 2023, Mr M was contacted on a popular instant messaging service by an individual purporting to be from a recruitment company. He was offered a job opportunity with an online optimisation platform "E", which required him to boost ratings and rankings of applications on various app stores.

Mr M showed interest and he was subsequently contacted by another individual who claimed to his supervisor. They explained that Mr M could earn wages through commission and a basic salary. Payments for both would be paid in cryptocurrency (USDT). Mr M understood that the commission could range between 50 and 200 USDT each day, whereas the salary depended on the "level" and could be up to 3,000 USDT per month.

After opening an account with E, Mr M could see the 'tasks' he had been assigned on the platform. It was explained to him that his job would involve completing them to earn commission. Mr M's supervisor also told him that he would sometimes be granted 'combination tasks', which required a group of tasks to be completed before any withdrawal could take place. Each combination task had a value, given in USDT. Each time a combination task was assigned, the value of the task in USDT would be deducted from Mr M's account balance with E, leaving him with a negative balance. He was told the balance needed to be made positive by depositing USDT in his account before any withdrawals could be made.

In order to make deposits into his account with E, Mr M was instructed to convert his money into USDT. He transferred funds into his existing Revolut account before making payments to a cryptocurrency exchange for conversion into cryptocurrency. Once converted, the cryptocurrency was sent to wallet addresses provided by his supervisor. Mr M believed he was making deposits into his account with E, given its account balance went up by the same amount. But before he could make withdrawals, he was given another combination task of a greater value, meaning he would have to complete those tasks (and therefore make another deposit).

Eventually, Mr M was told he needed to pay tax to complete his withdrawal. He questioned this and was informed it was a government regulation. But Mr M didn't have any money left to deposit. He was also unhappy that he was being asked to pay tax on money which he'd already paid tax on when he received his salary from his main employer. Mr M's supervisor told suggested taking out a loan, but he explained he wasn't eligible as he was in the UK on a student visa.

The following transactions, all card payments, are relevant to this complaint –

Payment number	Date and Time	Amount
	7 August, 14:06	£87.00 **(declined)**
	7 August, 14:08	£87.00 **(declined)**
Payment 1	7 August, 14:10	£87.00
	8 August, 12:06	£36.95 **(declined)**
Payment 2	8 August, 12:09	£36.95
Payment 3	8 August, 12:28	£15.03
Payment 4	9 August, 22:48	£90.00
Payment 5	10 August, 00:07	£400.00
Payment 6	10 August, 11:57	£90.00
Payment 7	10 August, 12:13	£650.00
Payment 8	10 August, 12:42	£1,300.00
Payment 9	10 August, 13:14	£3,500.00
Payment 10	10 August, 15:08	£15.02
	10 August, 21:25	£4,150.00 **(declined)**
Payment 11	10 August, 23:30	£4,150.00
	Total loss	**£10,334**

On 11 August, over 12 hours after making the final payment, Mr M reported the matter to Revolut. At the time, he said he wanted to report fraudulent activity on his account as he didn't recognise any of the above transactions. Mr M went on say that an app had been installed on his phone which he'd only noticed then. He also shared a screenshot of text messages containing One Time Passcodes (OTPs) sent to him by the same firm. Revolut looked into the matter and said the transactions weren't fraudulent as they had been approved in the Revolut app via 3DS.

A few days later, Mr M complained to Revolut via his representative. He explained he had been the victim of a job scam. But Revolut declined to refund any of the disputed payments, saying Mr M had authorised them and there were no chargeback rights.

Unhappy with this, Mr M referred his complaint to our service. One of our investigators looked into it and ultimately concluded that by the time Mr M authorised Payment 9, Revolut ought to have recognised that it carried a higher risk of being associated with fraud. Given the increased spending on cryptocurrency and multiple transactions on that day, the investigator considered that an appropriate response to the scam risk should have taken the form of a human intervention. They were persuaded that had Revolut asked further questions, it was more likely than not that the scam would have been uncovered.

The investigator considered that Mr M had been dishonest with Revolut when he later reported the matter. But they didn't think his actions at the time he contacted Revolut meant that Mr M would have also been dishonest had it intervened at the suggested trigger point.

In recommending a refund of the losses suffered from Payment 9 onwards, the investigator concluded that Mr M should share responsibility for what happened and so they made a deduction of 50% for contributory negligence.

Mr M accepted the investigator's outcome, but Revolut didn't. In summary, it says:

- All the disputed payments were sent from Mr M's own external accounts that he owned and controlled, meaning that the fraudulent transactions didn't originate from his Revolut account, and he eventually lost control of the funds further in the chain once Revolut's services had concluded. Revolut merely serviced as an intermediary in the fraudulent transfers. The scam didn't occur on Revolut's platform.

- Revolut isn't entitled to obtain information from other financial institutions such as the sending bank. But the Financial Ombudsman Service is empowered to compel disclosures from either relevant banks or from the customer themselves under the provisions of DISP 3.5.11 and DISP 3.5.12. Additionally, the Financial Ombudsman Service has the power under DISP 3.5.2 to inform a customer that it could be appropriate to make a complaint against another financial institution.

- Revolut shouldn't be responsible for Mr M's loss simply because the third party sits outside the Financial Ombudsman Service's jurisdiction either because the firm isn't authorised, or the product isn't regulated.

- There's no rational explanation as to why the Financial Ombudsman Service considers Revolut should be responsible for all, most or 50% of the customer's loss in such scenarios where the relevant transaction is self-to-self.

- Mr M gave misleading and contradictory information when reporting the scam to Revolut and the Financial Ombudsman Service, to an extend that he initially denied any knowledge of the payments. This implies a significant willingness to deceive and goes beyond negligence and recklessness and also strengthens Revolut's belief that Mr M would have lied had it intervened more.

As an agreement couldn't be reached, the complaint has been passed to me to decide.

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'm 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 M 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 M and the Payment Services Regulations to carry out their 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'm 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 August 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 doesn't mean that customers will always be protected from bad outcomes, Revolut was required 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've 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'm 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'm 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 August 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'm mindful that in practice all banks and EMIs 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 August 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'm 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

[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_/

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 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.

---

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

[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.

- 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 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 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.

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

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

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

I'm aware that cryptocurrency exchanges 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 all of the disputed payments would be credited to a cryptocurrency wallet held in Mr M's name.

By August 2023, when these transactions started, 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 August 2023, when these payments took place, 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'm satisfied that by the end of 2022, prior to the payments Mr M 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.

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 M'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 M might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all the payments were going to a cryptocurrency provider (the merchant is a cryptocurrency provider). The first eight payments were relatively low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

That said, I can see that three payments were declined in that period. According to Revolut's records, the first one of these – £87 on 7 August at 14:06 – was declined due to incorrect

---

[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.

expiry details being entered on the merchant's website. And it declined the other two payments – £87 on 7 August at 14:08 and £36.95 on 8 August at 12:06 – due to suspicious activity. Revolut froze Mr M's card on both occasions and sent him an in-app message asking him to confirm that it was indeed him making the transaction. Considering the individual amounts involved, I consider checking that the payment was genuinely made by Mr M was a proportionate response to the risk involved.

A few days later, by the time Mr M made Payment 9, I consider that a pattern of increased spending on cryptocurrency had emerged. The payment in question was significantly larger than any other payment that had debited Mr M's account, and it was the fifth cryptocurrency related payment in a 12-hour period. I think that the circumstances should have led Revolut to consider that Mr M was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Mr M?

Revolut says it declined the transactions it considered suspicious and froze Mr M's card. It says it informed Mr M it detected a suspicious transaction and required him to confirm he did in fact make the transaction.

While I don't discount Revolut's actions in relation to the earlier transactions which it declined, I don't think the steps it took then were proportionate to the risk presented by the transactions on 10 August. Even at the time of the earlier transactions, there was no information provided to Mr M about why Revolut considered them suspicious. It's difficult to see how Revolut's actions at the time would later resonate with Mr M or the specific circumstances of the transactions in question. I consider that Revolut needed to do more.

What kind of warning should Revolut have provided?

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 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 Payment 9 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'm 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 M made Payment 9, Revolut should – for example by asking a series of 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 M was at risk from.

In this case, Mr M 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 M 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. Revolut has argued that given Mr M lied about not recognising or making the transactions when he reported them, it's unlikely he would have been honest had it made further enquiries at the suggested intervention point. I can see from Mr M's chat history with Revolut that he wasn't honest about what had happened when he reported the transactions. While I understand the point Revolut is trying to make here, I don't agree with its inference. I accept that Mr M provided misleading information when he first contacted Revolut about the payments – he said he didn't make the payments when it has been established that he did. However, it doesn't follow that he would have mislead Revolut had it taken additional steps when I think it should have.

I say this because at the time of making the payment, Mr M thought he was making a legitimate payment for the purpose of completing a job task and had no reason not to provide accurate information. But in reporting the loss, he was fully aware he'd lost money and it would seem that there's been a lapse of judgement in how he presented his case to Revolut. I can't say for certain why Mr M did this, but it would likely be linked to the hope that he would recover funds that he lost through being the victim of a scam.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr M suffered from Payment 9 onwards?

I think that a warning of the type I've described would have identified that Mr M's circumstances matched an increasingly common type of scam.

I've read the chat messages between Mr M and the scammer, and around the relevant time he appears to have been concerned about repeatedly being assigned combination tasks. I think that a warning provided by Revolut would have given the perspective Mr M 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 that payment, and subsequent payments, had such a warning been given.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mr M 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 scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr M might have been at risk of financial harm from fraud when he made Payment 9, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I'm satisfied it would have prevented the losses Mr M 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 M's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr M'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 M 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 M could instead, or in addition, have sought to complain against those firms. But Mr M has not chosen to do that and ultimately, I can't 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 M'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'm satisfied that it would be fair to hold Revolut responsible for Mr M's loss from Payment 9 (subject to a deduction for Mr M's own contribution which I will consider below).

Should Mr M bear any responsibility for his losses?

I've thought about whether Mr M should bear any responsibility for his loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

I recognise that there were relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent earnings and tasks. Reading the chat correspondence with the scammer, I note that Mr M also seems to have been part of an

instant messaging group with other people who claimed to be making money. I can imagine this would have given some validation to the scheme.

But, at its heart, the scam appears to have been fairly implausible. While I haven't seen and heard everything that Mr M saw, the scammer's explanation for how the scheme worked is quite baffling and I think Mr M ought reasonably to have questioned whether the activity he was tasked with carrying out (which doesn't appear to be particularly time-consuming or difficult) could really be capable of generating the returns promised. He also appears to have had concerns about the scheme by the point I consider Revolut should have taken further steps.

So, given the overall implausibility of the scam and Mr M's own apparent recognition of the risk of being continuously granted combination tasks, I think he ought to have realised that the scheme wasn't genuine before going ahead with Payment 9. In the circumstances, I consider he should bear some responsibility for his losses.

I've concluded, on balance, that it would be fair to reduce Revolut's liability 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 M's money?

These were card payments to a cryptocurrency provider. Mr M sent that cryptocurrency to the scammer. So, Revolut wouldn't 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 the exchange provided cryptocurrency to Mr M, which he subsequently sent to the scammer.

So, I don't think Revolut should have done anything more to try and recover Mr M's money.

Putting things right

Revolut Ltd needs to refund Mr M Payments 9-11, making a 50% deduction for contributory negligence. It can also deduct any amount Mr M has recovered directly from the scammer.

Revolut Ltd also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of refund.

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require Revolut Ltd to put things right for Mr M as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 9 October 2024.

Gagandeep Singh
Ombudsman