DRN-4760872

The complaint

Mr P complains that Revolut Ltd won't refund money he lost to a scam.

What happened

Mr P fell victim to a fake job scam. He was contacted via a mobile messaging service by someone offering him a job. They said they'd got his details from a recruitment firm, and offered him a position which involved rating hotels online. He was told he would be paid for completing tasks, but needed to use his own money to buy cryptocurrency so he could unlock these tasks. He was told he'd receive his money back plus commission. Mr P opened accounts with Revolut and with a cryptocurrency provider to facilitate his payments to the job platform. Unfortunately, and unknown to Mr P, the job was not legitimate, he was being scammed.

As the scam progressed, Mr P was asked to pay increasingly large amounts to unlock the tasks, but aside from some small withdrawals from the job platform to his cryptocurrency wallet (which appear to have been reinvested), Mr P was unable to retrieve either the money he had paid in or any profits. Ultimately, he made the following card payments from Revolut to his cryptocurrency account over the course of four days:

	Date	Time	Amount
Payment 1	11/05/2023	12:39	£50
Payment 2	12/05/2023	12:21	£57.22
Payment 3	12/05/2023	17:10	£52
Payment 4	12/05/2023	17:57	£96
Payment 5	13/05/2023	10:23	£205.40
Payment 6	13/05/2023	11:05	£110.40
Payment 7	13/05/2023	11:47	£98.90
Payment 8	14/05/2023	12:05	£327.60
Payment 9	14/05/2023	12:35	£477.30
Payment 10	14/05/2023	12:53	£1,238.80
Payment 11	14/05/2023	13:34	£1,298.60
Payment 12	15/05/2023	11:37	£3,925.60
Payment 13	15/05/2023	18:35	£3,000
Payment 14	15/05/2023	18:52	£3,500
Payment 15	15/05/2023	19:50	£688.20

Mr P realised he had been scammed when the scammer continued to ask for more large deposits before he would be allowed to withdraw his profits. He told Revolut what had happened, but it didn't consider it had any responsibility for his loss. It said it had no responsibility to prevent scams, that the loss had not occurred from Mr P's Revolut account, and that Mr P had been grossly negligent by ignoring warning signs about what he was doing.

Our Investigator upheld the complaint in part. Ultimately, they felt that Revolut should have realised that not all was as it seemed when it questioned Mr P about payment 12, as the answers Mr P gave were inconsistent. The investigator thought that, had that happened, the scam would likely have been stopped. So, the investigator said that Revolut should refund the money Mr P had lost from this payment onwards, less a deduction of 50% in recognition of Mr P's own contributory negligence.

Revolut disagreed, amongst other, more general, arguments, it also does not think Mr P would have been honest about what he was doing if it had questioned him further about what he was making the payments for. So, it does not believe it could have uncovered the scam.

As no agreement could be reached, the matter has been escalated to me to determine.

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 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 P modified the starting position described in *Philipp,* by – among other things – expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*" (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should

have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in May 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- 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 May 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

[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_/

control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

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

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

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

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (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

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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 May 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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 May 2023, Revolut should in any event have taken these steps.

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

Mr P's Revolut account was opened shortly before this scam took place, apparently for the purposes of the payments associated with this scam. So, Revolut had a limited account history against which to compare the payments Mr P was making. And the initial payments Mr P made were small, so even though they were evidently payments to purchase cryptocurrency, I don't think these payments would have been an immediate cause for concern. However, by the time of the eleventh payment to the scam, I consider that a pattern was emerging which should have flagged to Revolut that something untoward could be going on.

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 payments Mr B was making would be to a cryptocurrency wallet held in Mr B's name.

But by January 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. 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.

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

And considering that, by the time of the eleventh payment Mr P made to the scam, a pattern had emerged of increasing payments within a short period of time, and given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr P 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 Mr P before this payment went ahead.

What kind of warning should Revolut have provided?

Revolut has confirmed that it did not provide Mr P with any warnings regarding the payments he made.

I consider that, by the time of Payment 11, Revolut should have taken steps to provide Mr P with a written warning based on the characteristics of the payment he was making. And given that it was identifiably to cryptocurrency I think this warning should have provided details relevant to common cryptocurrency scams. However, at that time, such a warning would most likely have been focused on the most common types of scams – investment scams – rather than the job scam that Mr P was victim of, and I don't think that it would have been clear to Revolut at the time of Payment 11 that it was a job scam specifically that Mr P was falling victim to. So, I can't see that the kind of warning Revolut would have reasonably provided at that time would have rung any alarm bells for Mr P. This is supported by the fact that Revolut did provide general cryptocurrency investment warnings when it discussed later payments with Mr P in its in-app chat, but those warnings did not stop Mr P from proceeding with his payments to the scam.

However, I consider that by the time of Payment 12, given the significant leap in value of this payment, the pattern of payments had become concerning enough that Revolut should have taken further steps to intervene. In the circumstances, I think a reasonable intervention would have been for Revolut to contact Mr P directly to find out more about the circumstances of the payments and to ensure he was not at risk of financial harm. And evidently Revolut did do this, it contacted Mr P in the in-app chat to ask him various questions about what he was making payments for. The question then is whether that intervention went far enough, and whether Revolut should have identified that Mr P was at risk given what he told it.

I've thought carefully about this, and I acknowledge that some of the answers Mr P gave when Revolut questioned him about Payment 12 did not reflect the whole story of what was actually happening. But I nonetheless think there was enough going on that Revolut should

have had specific concerns that Mr P was falling victim to an employment related scam, and so provided him with a warning relevant to those circumstances. I say this because Mr P specifically told Revolut that he was making payments to buy cryptocurrency for 'work purposes', and given that there are very few, if any, legitimate reasons why someone would be buying cryptocurrency for work, I think Revolut missed the opportunity to ask some more detailed questions about what Mr P was making these payments for. There was also a clear urgency in Mr P's responses, but again Revolut does not appear to have questioned why Mr P needed this payment to be made so quickly. Nor did Revolut question any of the inconsistencies in what Mr P had told it – for example, he'd said he opened the account for travel but was using it to buy cryptocurrency.

Revolut says that Mr P's responses when questioned show a willingness to be dishonest about what he was making payments for. It therefore considers that Mr P would likely have continued to be dishonest if questioned, but I don't agree. While there were some inconsistencies, it's also clear that Mr P was honest about the purpose of the payment, he said it was for work purposes and that was accurate, as far as he was aware.

Nothing I've seen or been told by Mr P indicates that he was given a cover story or otherwise told to be dishonest with Revolut. So, if he had been directly questioned about what 'work' related purpose he was making the payments for, I think it's likely he would have continued to be honest and it would have quite quickly come to light that he was making payments to buy cryptocurrency associated with a job. Revolut would have been aware that this was unlikely to be a legitimate job opportunity and could have provided Mr P with a detailed warning relating to that particular type of scam at this stage, and I've seen nothing to suggest that Mr P wouldn't have taken heed of such a warning and stopped making any further payments to the scam.

Is it fair and reasonable for Revolut to be held responsible for consumer's loss?
In reaching my decision about what is fair and reasonable, I have taken into account that Revolut was not the start or end point of this scam. Mr P moved his money from other accounts, to Revolut, and then on to his cryptocurrency account before ultimately passing it on to the scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr P might have been at risk of financial harm from fraud when he made Payment 12, and should have questioned him in more detail about that payment. If it had taken those steps, I am satisfied it would have prevented the losses Mr P suffered from that point on. The fact that the money used to fund the scam didn't originate at Revolut, and wasn't lost at the point it was transferred to Mr P's cryptocurrency account does not alter that fact and I think Revolut can fairly be held responsible for Mr P'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 P 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 – although I've seen no evidence that any other firms did intervene in the payments that went to Mr P's Revolut account – and Mr P could instead, or in addition, have sought to complain against those firms. But Mr P 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 P'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 Mr P's loss from Payment 12 onwards (subject to a deduction for consumer's own contribution which I will consider below).

Should Mr P bear any responsibility for his losses?

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

And, having thought carefully about this, I do think Mr P could have done more to protect himself from this scam. There were aspects of the scam that were convincing – the scammers appear to have copied details of a legitimate business – but I nonetheless think he ought reasonably to have had concerns about the legitimacy of the job offered, once he became aware of the requirement to send funds before he could earn any more profits. I think this should have given Mr P pause for thought and so led to him looking more deeply into this job he was apparently being offered. And I can see that Mr P did appear to have some concerns about what he was being asked to do, but the scammer was able to convince him to move past those concerns quite easily, without Mr P taking any steps to independently verify what he was being told to do.

Because of this, I think it would be fair and reasonable to make a 50% reduction in the award based on contributary negligence in the circumstances of this complaint.

I've also thought about whether Revolut could have done anything to recover the payments Mr P made to the scam. But given that the payments were made by card to a cryptocurrency provider, and Mr P sent that cryptocurrency to the fraudsters, 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 the cryptocurrency exchange provided cryptocurrency to Mr P.

I also note that Mr P did receive some returns form the scam in its early stages, but those returns were received before the point at which I consider Revolut should have been able to stop the scam, so they do not affect the redress I consider is due to Mr P.

Putting things right

To resolve this complaint Revolut should:

- Refund to Mr P 50% of his loss from Payment 12 onwards (inclusive).
- Pay 8% simple interest per annum on this refund from the date of each payment to the date of settlement.

My final decision

I uphold this complaint in part. Revolut Ltd should now put things right in the way I've set out

above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 13 February 2025.

Sophie Mitchell
Ombudsman