DRN-5025650

The complaint

Mr W is unhappy that Revolut Ltd (Revolut) won't refund the money he lost after he fell victim to an Authorised Push Payment ("APP") scam.

What happened

The background to this complaint is well-known to both parties, so I won't repeat it in detail here, but in summary, I understand it to be as follows.

In April 2023, Mr W fell victim to a task-based job scam. The fraudsters persuaded Mr W to pay his own money in order to proceed with work. He was instructed to send money to a cryptocurrency exchange - once his money had been converted into cryptocurrency, it was then sent to accounts controlled by the fraudsters.

To facilitate the payments, Mr W moved money into his Revolut account, from an account he held with another financial firm. The following transactions were then made (and received) from his Revolut account;

	Date	Time	Amount	Method of Payment	To / From
1	18 April 2023	19:18	£100.00	Debit Card Payment	To Cryptocurrency Exchange
2	20 April 2023	10:35	£70.00	Debit Card Payment	To Cryptocurrency Exchange
3	21 April 2023	11:05	£71.00	Debit Card Payment	To Cryptocurrency Exchange
4	21 April 2023	11:07	£15.00	Debit Card Payment	To Cryptocurrency Exchange
5	21 April 2023	12:32	£105.00	Debit Card Payment	To Cryptocurrency Exchange
6	21 April 2023	12:38	£15.00	Debit Card Payment	To Cryptocurrency Exchange
7	21 April 2023	14:21	£336.75	CREDIT	From Cryptocurrency Exchange
8	22 April 2023	11:33	£235.00	Debit Card Payment	To Cryptocurrency Exchange
9	22 April 2023	12:56	£640.00	Debit Card Payment	To Cryptocurrency Exchange
10	22 April 2023	13:23	£750.00	Debit Card Payment	To Cryptocurrency Exchange
11	22 April 2023	13:33	£15.00	Debit Card Payment	To Cryptocurrency Exchange
12	22 April 2023	14:01	£500.00	Debit Card Payment	To Cryptocurrency Exchange
13	22 April 2023	14:03	£500.00	Debit Card Payment	To Cryptocurrency Exchange
14	22 April 2023	21:30	£550.00	Debit Card Payment	To Cryptocurrency Exchange
15	22 April 2023	21:31	£550.00	Debit Card Payment	To Cryptocurrency Exchange
16	24 April 2023	11:30	£3,000.00	Debit Card Payment	To Cryptocurrency Exchange
17	24 April 2023	11:32	£3,000.00	Debit Card Payment	To Cryptocurrency Exchange
18	24 April 2023	11:33	£490.00	Debit Card Payment	To Cryptocurrency Exchange
19	24 April 2023	11:44	£95.00	Debit Card Payment	To Cryptocurrency Exchange
20	24 April 2023	19:24	£1,500.00	Debit Card Payment	To Cryptocurrency Exchange
21	24 April 2023	19:50	£1,200.00	Debit Card Payment	To Cryptocurrency Exchange
22	25 April 2023	18:56	£950.00	Debit Card Payment	To Cryptocurrency Exchange
23	25 April 2023	18:57	£950.00	Debit Card Payment	To Cryptocurrency Exchange
24	25 April 2023	18:58	£950.00	Debit Card Payment	To Cryptocurrency Exchange
25	25 April 2023	19:00	£950.00	Debit Card Payment	To Cryptocurrency Exchange
26	25 April 2023	19:01	£950.00	Debit Card Payment	To Cryptocurrency Exchange
27	25 April 2023	19:02	£300.00	Debit Card Payment	To Cryptocurrency Exchange
28	26 April 2023	16:29	£950.00	Debit Card Payment	To Cryptocurrency Exchange
29	26 April 2023	16:31	£950.00	Debit Card Payment	To Cryptocurrency Exchange
30	26 April 2023	16:32	£950.00	Debit Card Payment	To Cryptocurrency Exchange
31	26 April 2023	16:33	£950.00	Debit Card Payment	To Cryptocurrency Exchange
32	26 April 2023	16:34	£950.00	Debit Card Payment	To Cryptocurrency Exchange
33	2 May 2023	14:04	£950.00	Debit Card Payment	To Cryptocurrency Exchange

34	2 May 2023	14:06	£950.00	Debit Card Payment	To Cryptocurrency Exchange
35	2 May 2023	14:07	£950.00	Debit Card Payment	To Cryptocurrency Exchange
36	2 May 2023	14:11	£950.00	Debit Card Payment	To Cryptocurrency Exchange
37	2 May 2023	14:12	£950.00	Debit Card Payment	To Cryptocurrency Exchange
38	2 May 2023	14:13	£950.00	Debit Card Payment	To Cryptocurrency Exchange
39	2 May 2023	14:15	£80.00	Debit Card Payment	To Cryptocurrency Exchange

Mr W realised he'd been scammed when he was asked to pay increasingly larger sums to be able to make withdrawals. He reported the matter to Revolut, but it didn't uphold his complaint. In summary, it said there were no Chargeback rights for the disputed transactions and that Mr W displayed a lack of due diligence.

Unhappy with Revolut's response, Mr W referred his complaint to this service, with the help of a professional representative. One of our Investigator's looked into things and thought the complaint should be upheld in part. In summary, it was our Investigators view that Revolut should have recognised that Mr W could have been at a heightened risk of financial harm when he was making transaction 16 (the payment for £3,000 at 11:30 on 24 April 2023 in the table above) and that it should have provided a warning. Our Investigator thought that warning should have been related to cryptocurrency investment scams, but they didn't think this would have resonated with Mr W, given he was falling victim to a job scam, rather than to a cryptocurrency investment scam.

But our Investigator thought that when, just two minutes later, Mr W made another payment for £3,000 Revolut's should have intervened further and that a member of its staff should have contacted Mr W, before allowing the payment to be progressed. It was our Investigators view that had an intervention taken place the scam could have been prevented and Mr W wouldn't have lost his money from this point.

But our Investigator also thought Mr W should bear some responsibility for his loss. Overall, our Investigator thought Revolut should refund Mr W 50% of his outstanding loss, from and including transaction 17, and that it should pay 8% simple interest on this amount from the date of the loss.

Mr W accepted our Investigator's opinion. Revolut disagreed, in summary it set out the following points;

- The payments Mr W made were "Self-to-Self", so Mr W owned and controlled the beneficiary accounts he was paying from his Revolut account, and his funds were lost from these cryptocurrency platforms and accounts.
- Revolut was merely an intermediary in the process. As the payments were self to self, there is no Authorised Push Payment (APP) fraud as defined in DISP rules. The transfers also don't meet the Contingent Reimbursement Model Code (CRM Code) definition of APP fraud or the definition in the PSR mandatory reimbursement scheme.
- For this service to effectively apply the reimbursement rules to such self-to-self transactions executed by Revolut is an error of law. Alternatively, this service has irrationally failed to consider that the transactions are self-to-self payments.
- Revolut isn't able to obtain information from sending banks about the warnings they provide when customers credit Revolut accounts. But the rules under which this service operates allows us to get this information. Any warnings provided by external banks need to be considered.
- Overall, it is irrational and illogical of this service to hold Revolut responsible in these circumstances when there are other financial institutions in the payment chain that have comparatively greater data on a customer than Revolut that are not being held responsible in the same way.

As an agreement couldn't be reached the complaint has 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.

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 W 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 April / 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 April / 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 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

[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] 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.

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 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 that during the period of these payments, between April 2023-July 2023, that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and

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

- 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 during the period of these payments, between April 2023-May 2023, Revolut should in any event have taken these steps.

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

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

I'm aware that cryptocurrency exchanges, like the ones Mr W made his payments to here, 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 W's name.

By April 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. And by April 2023, when these payments began, further restrictions were in place. 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 PSPs, 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 W made from April 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm. In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before they processed such payments. And as I have explained Revolut was also required by the terms of their contract to refuse or delay payments where regulatory requirements meant they 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 the fact payments in this case were going to an account held in Mr W'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, they ought to have identified that Mr W might be at a heightened risk of fraud that merited its intervention.

While, in the individual circumstances of this case, it is finely balanced due to the number of transactions – I don't think Revolut needed to intervene on transactions 1-15. I say that as there are no obvious patterns around the value of the payments escalating and Mr W had received a credit back into his account, from the same payee, the value of which only fell slightly shy of the value of the first six transactions that were made.

But that said, there is a pattern starting to emerge around the frequency of the payments and I consider at the point transaction 16 was being made Revolut should have been concerned and provided a warning to Mr W. The value of this payment represented a sharp uplift, in comparison to previous payments and coupled with the pattern that was emerging of frequent payments and that the payments were going identifiably to a cryptocurrency merchant, there was enough going on that ought to have given Revolut some cause for concern.

Further, by the time Mr W then went on to make a further transaction (number 17 in the table above), I think there was enough going on that ought to have given Revolut further cause for concern. This was the second payment of £3,000 within a couple of minutes and meant cumulatively he had sent over £10,000 within a short period of time. At this point there is a noticeable uplift in both the frequency and value of the payments – to the point where I think Revolut ought reasonably to have had serious concerns that its customer may have been at risk of financial harm and its intervention here should have extended to more than an automated warning.

What did Revolut do to warn Mr W?

From what I've seen, steps were taken as part of the 3DS authentication process. As well as this, ahead of transaction 8 (for £235) Revolut stopped the payment and provided a 'pop-up' message to Mr W. The message gave Mr W the opportunity to confirm whether the payment was safe or suspicious – Mr W confirmed the payment was safe and so the payment was able to be progressed.

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

Taking that into account, I think Revolut, when Mr W attempted to make transaction 16, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, a proportionate response would have been for it to have provided a tailored warning that was specifically about the risk of cryptocurrency investment scams, given how prevalent they had become by the end of 2022.

However, I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss at this point and on the balance of probabilities, I don't think it would have.

I say that as here Mr W was sending the funds under the belief that he was carrying out legitimate work – the completing of tasks – as part of a job with a genuine employer. He wasn't therefore sending the funds to simply invest but rather, he thought it was a requirement to receive the remuneration the scammer told him he would receive. Because of this, I'm not persuaded that the characteristics of a cryptocurrency investment scam, that I think could reasonably have been laid out in a warning, would have resonated with him, as they wouldn't have reflected what he was experiencing.

However, by the time Mr W went on to make a further transaction (number 17 in the table above), I think the intervention ought to have gone further than an automated warning. I think, given the risk that would have been apparent to Revolut, a proportionate response from Revolut at this point would have been for the payment to be stopped, until Revolut had carried out checks with Mr W around the purpose of the payment. I'm persuaded this should have been a human intervention, for example through Revolut's in-app chat or through speaking to Mr W.

If Revolut had intervened as described, would that have prevented the losses Mr W suffered from the seventeenth transaction?

I've carefully considered what I think would have most likely have happened, had Revolut intervened, as I've described above, ahead of the seventeenth payment.

I've no reason to think Mr W wouldn't have been open or honest with Revolut about the purpose of the payment had it questioned him. I say that as I haven't seen any evidence to suggest that Mr W was asked, or agreed to, disregard a warning provided by Revolut. And I note that I've also seen no evidence that Mr W was provided with any tailored warning by the firm from which the funds used for the scam appear to have originated. And so, had Revolut contacted Mr W to establish the circumstances surrounding it, I think they would've most likely prevented his loss.

This is because I think it's more likely than not Mr W would have explained that he was purchasing cryptocurrency for work purposes. Revolut ought to have recognised this as a 'red flag' and I consider further probing would've most likely uncovered that Mr W had come across this job opportunity through being messaged on an instant messenger app. And that he was purchasing cryptocurrency to send to a platform for it to be used to complete tasks, which involved using the funds to optimise apps to improve their ratings.

From this, Revolut ought to have recognised that Mr W was falling victim to a scam and given him a very clear tailored scam warning. I've no reason to think Mr W wouldn't have been receptive to such advice and so, on balance, I think it would have resonated with him and he wouldn't have gone on to make this seventeenth payment (or those that followed).

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr W purchased cryptocurrency which credited e-wallets 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.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr W might have been at risk of financial harm from fraud when he was making the seventeenth transaction, 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 W suffered from that point.

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 W's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr W'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 W 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 W could instead, or in addition, have sought to complain against those firms. But Mr W 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 W'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 W's loss from payment seventeen, subject to a deduction for his own contribution which I will consider below.

Should Mr W bear any responsibility for their 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.

Mr W has already accepted the Investigator's opinion that any refund provided should be reduced to account for his own actions as part of the scam and as I agree with this point, I won't dwell on it, except to say that I think there were a number of things that ought to have led Mr W to proceed with more caution than he did.

While I accept Mr W believed that these payments were being made in connection with a legitimate employment opportunity, I'm not persuaded that belief was a reasonable one. There was no formalisation of the arrangement between him and the employer – for example, there was no written contract and indeed no clear setting out of the terms of his employment.

At its heart, the scam appears to have been fairly implausible. While I haven't seen and heard everything that Mr W saw, the scammer's explanation for how the scheme worked is implausible and I think Mr W ought reasonably to have questioned whether the activity he was tasked with carrying out (which does not appear to be particularly time-consuming or arduous) could really be capable of generating the returns that were being promised. I think the level of salary and commission being offered, seemed inflated, considering the nature of the work that was being carried out.

In addition to that, the arrangement was an inversion of the normal employer-employee relationship. In most circumstances, people expect to be paid by their employer, rather than the other way around. As far as I can see, there wasn't really any attempt to explain this uncommon arrangement.

Overall, I think it's fair and reasonable for Revolut to make a 50% deduction from the redress payable to Mr W.

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

The payments were made by card to legitimate cryptocurrency exchanges. Mr W 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 the cryptocurrency exchange provided cryptocurrency to Mr W, which he subsequently sent to the fraudsters.

Putting things right

For the reasons explained, I uphold this complaint in part and now ask Revolut Ltd to:

- refund Mr W £10,932.50 (which I calculate to be 50% of the sum of transactions 17-39).

- pay interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement (if Revolut Ltd deducts tax from this interest, it should provide Mr W with the appropriate tax deduction certificate).

My final decision

For the reasons given above my final decision is that I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 10 April 2025.

Stephen Wise
Ombudsman