DRN-4997501

The complaint

Mr L is unhappy Revolut Ltd didn't refund payments he made as part of a scam.

Mr L brings his complaint via professional representatives, but for simplicity I've referred to the actions of Mr L throughout this decision.

What happened

In September 2023 Mr L came across an advert for a cryptocurrency investment opportunity on social media, offered by a company I'll call "U". He submitted an enquiry and was called by a 'broker' who showed him a sophisticated website and trading platform. Mr L had dabbled in cryptocurrency previously, but was looking for professional help with trading. He was pointed to an entry for U on Companies House, and a statement on its website that said it was regulated by the Financial Conduct Authority (FCA). Having been persuaded it was legitimate, he decided to invest. The conversation then moved to an instant messaging app.

The broker guided Mr L to set up an account on the platform, via screen-sharing software. He sent a small tester amount from his main bank account; at a bank I'll call "L". Mr L saw his profits increase on the platform, and says U's agents pressured him into investing larger amounts. The first four payments using his Revolut card were supposedly made directly to the platform to fund his trading account, but actually went to what appears to be a digital marketing agency, I'll call "G".

Mr L was then introduced to a further opportunity by U which required him to send cryptocurrency to the platform to be traded. Under instruction from U's broker, Mr L set up an account with a cryptocurrency exchange, I'll call "B". He then bought cryptocurrency from B using his existing Revolut account (which he topped up using his main bank account at L), and send that onto the platform so it could be traded on his behalf. Mr L later used a different exchange to buy cryptocurrency, which I'll call "C", and was encouraged by the scammers to use others at different points. Revolut's fraud prevention system didn't identify Mr L was at risk, and so it didn't intervene to warn him on any of the payments.

During the period in question, Mr L made the following payments from his Revolut account as part of the scam:

Payment	Date	Time	Type/Payee	Amount
1	7 September 2023	19.58	Debit card payment to G	£429.49
2	7 September 2023	20.01	Debit card payment to G	£858.92
3	7 September 2023	20.06	Debit card payment to G	£858.99
4	7 September 2023	20.11	Debit card payment to G	£429.59
5	8 September 2023	07.11	Debit card payment to G	£859.84

6	18 September 2023	07.44	Debit card payment to B	£250
7	18 September 2023	08.51	Debit card payment to B	£1,000
8	25 September 2023	10.28	Debit card payment to C	£5,000
9	26 September 2023	13.30	Debit card payment to B	£630
10	4 October 2023	13.44	Debit card payment to C	£1,442.18
11	12 October 2023	12.09	Debit card payment to B	£4,350
			Total:	£16,109.01

When Mr L requested a withdrawal from the trading account he was told to 'set the technical position' to allow for that to happen, using instructions from U's broker. However all of the funds seemed to disappear and the scammer blamed Mr L for not setting things up correctly. He was told he needed to pay a fee to recover the balance, which he settled using the amount sent to C on 4 October 2023. After that Mr L was told he needed to pay tax on his profits, which he paid using the amount sent to B on 12 October 2023. Having been reassured that would be the final cost to pay, he was then asked again for more charges – and that led him to realise he'd been scammed.

Mr L reported the fraud to Revolut and the police at the start of November 2023. Chargeback claims were raised for the first four payments, but those were unsuccessful as Revolut could find no evidence of unauthorised fraud on his account. A complaint was made to Revolut about the outcome of his fraud claim, via representatives, which said the transactions ought to have looked concerning and prompted warnings. But Revolut's final response maintained it wasn't required to refund the transactions. As Mr L wasn't happy with the response, he referred matters to our service for review.

One of our investigators looked at the complaint and thought it should be upheld. In his view, Revolut ought to have been concerned Mr L might be a risk of financial harm when he made payment 8 (for £5,000). The investigator thought a warning tailored towards cryptocurrency investment scams ought to have been shown before allowing that transaction to go through. He believed that would have resonated with Mr L and prevented further losses. The investigator didn't think Mr L had acted negligently either, so recommended that Revolut refunded the full amount (from payment 8 onwards).

Mr S accepted the investigator's opinion, but Revolut didn't agree. In summary, it said:

- The disputed transactions were 'self-to-self' payments, going to another account in Mr L's name and under his control. So, the fraud did not occur on the customer's Revolut account.
- Revolut was an Electronic Money Institution ("EMI") at the time, and the type of account Mr L had was often opened to facilitate payments of a particular purpose (it's not a bank account). So these payments weren't out of character nor unexpected when compared to the typical way an EMI account is used.

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

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 EMI's like Revolut are 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 L 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 September 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 September 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 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

[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.

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 in September 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-

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

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

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

It isn't in dispute that Mr L fell victim to a cruel and sophisticated scam. It's also accepted that he authorised the card payments going to G, B and C. For some of the disputed transactions the money was paid to a cryptocurrency exchange, rather than to the scammers directly. It was then the cryptocurrency purchased using those funds that was transferred to the scammers and lost. I'm also mindful that Revolut had far less information at its disposal than has subsequently come to light (and has been set out in this decision). So I've rightly concentrated on what it did know (or ought to have known) at the time it processed the payments.

On 7 September 202 there were four card payments made in a short space of time. The first and last payment in that sequence are also for similar amounts, as are the middle two. But the transactions are all relatively small in value, and not significantly out of kilter with the previous spend on the account (which tended to be at most in the low hundreds of pounds). The amounts go up and then down too – so doesn't form a concerning pattern, like one that indicates things could be escalating or a known scam pattern. The merchant doesn't carry an elevated risk, like the later ones identifiably going to a cryptocurrency exchange. So, I wouldn't have expected Revolut to intervene to give a warning on that day prior to processing any of those payments, and the same goes for the relatively low transaction sent to the same merchant the following day.

Ten days later Mr L makes two payments to a new cryptocurrency exchange on the same day, about an hour apart. Since opening the account he'd largely used it to make low value cryptocurrency and foreign currency transactions. So, even though these went to a new payee, and the second payment was for £1,000 (the highest on the account), I don't think this activity ought to have indicated Mr L might be at risk of fraud. That's because I don't consider it significantly out of character for the account, or a serious escalation on the previous spend (in the hundreds of pounds) that was seen.

A week later Mr L send £5,000 to another new cryptocurrency exchange. The value of the payment was by far the highest on the account (five times the previous highest one, made the week before). It was going to a new payee, and a different cryptocurrency exchange. Though I'm aware that cryptocurrency exchanges like C generally stipulate that the name on the card used to purchase cryptocurrency at its exchange must be the same as the one on account. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that payment was going to an account in Mr L's name.

By September 2023, when most of 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 significantly over the last few years. 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 reached record levels in 2022. During that period, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions. But 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.

I accept that Revolut itself offers cryptocurrency services, and the restrictions put in place by high street banks meant people would be more likely to use an EMI like Revolut for cryptocurrency related transactions. But Revolut will also have been aware of the growing trend for fraudsters to get their victims to pass money from their high street bank account to an EMI account, in order to take advantage of the fewer restrictions in place for sending funds to cryptocurrency providers. It would have been well understood by Revolut that victims of cryptocurrency scams don't generally lose their money at the exchanges – it's lost when it's sent on from there (e.g. to a fake investment platform). So the fact the accounts at B and C were likely to be in Mr L's name wouldn't have been as reassuring a factor that he wasn't at risk.

Taking into account all of the above, I am satisfied that Revolut ought to have been on notice Mr L was at risk of financial harm by payment 8, and intervened. I've considered that Revolut needs to tread a delicate line between protecting against fraud and not unduly hindering legitimate transactions. But the size of this one represented a serious escalation compared with Mr L's prior cryptocurrency related activity, which had really only been to dabble with small amounts. It was the second new external provider used in recent history, where previously exchanges had mostly been done within Revolut. I also think a pattern had formed of funds moving through the Revolut account from a high street bank, solely to facilitate increasingly larger payments to cryptocurrency, which was indicative of muti-stage fraud.

Revolut didn't warn Mr L on any of the payments, or otherwise intervene to carry out fraud checks. So, bearing in mind I've found Revolut should have identified he was at risk by payment 8, I've considered what intervention would have been appropriate in the circumstances.

What kind of intervention should Revolut have provided?

I've thought carefully about what a proportionate warning, in light of the risk presented, would have been 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.

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 September 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam for both APP and card payments. I understand in relation to Faster Payments it already had

systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described. I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by September 2023, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

Revolut would have identified the payment was going to cryptocurrency from the merchant's details. Had it asked a series of automated questions to establish the potential scam risks involved I think it's likely Mr L would have answered accurately and honestly. I say that because I've not seen any evidence in the correspondence with the scammer that he was coached to mislead his bank or Revolut. I've also not seen an especially high level of trust evidenced in the conversations, like communication becoming particularly friendly or casual. Mr L had also carried out several cryptocurrency transactions on the account previously, and believed Revolut to be crypto-friendly. So I think he would have likely shared what he was involved in, and a warning tailored to cryptocurrency investment scams would have been shown.

The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf, but not on the FCA register; the use of remote access software and a small initial deposit which quickly increases in value.

I accept that under the relevant card scheme rules Revolut cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Revolut ought to have initially declined payment 8 in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Mr L attempted the payment again, should Revolut have made the payment. Revolut did have systems in place by September 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time.

If Revolut had provided an intervention of the type described, would that have prevented the losses Mr L suffered from payment 8?

I've thought very carefully about this question, as to whether a tailored cryptocurrency investment scam warning would have stopped Mr L from making the payment, and uncovered the scam. U was a clone of a genuine FCA authorised firm, with a professional looking website and platform, so the scam was a convincing one. He'd also seen an entry on Companies House (for the real one) which would have added to air of legitimacy. Mr L had some experience with cryptocurrency too, though he hadn't been involved in an investment like this previously.

However, I'm persuaded, on balance, that a warning of this kind would have worked, as the circumstances involved were very stereotypical for a cryptocurrency investment scam. Mr L was therefore likely to recognise his situation in pretty much all the key features that would have been highlighted by the warning (found on social media, involvement of a broker, use of screensharing software, and a small deposit that quickly increases in value etc). He was fairly confident with cryptocurrency, but new to trading and seeking help with it, and not

under the scammer's spell particularly – so not likely to ignore this advice, based on what I've seen. This transaction also would have been easily the largest amount Mr L had invested since starting to dabble with cryptocurrency, so was already likely to be giving him some cause to pause before sending. I think the warning would have resonated with Mr L, to the extent that he was concerned enough to do some further research on the opportunity to reassure himself, or he have tried to withdraw his funds (and wouldn't have been able to).

What sways things here, and leads me to believe the scam would have been uncovered when Mr L carried out those further searches, is the FCA had just put up a warning about U being a clone of a legitimate firm three weeks before this transaction. It wasn't up when he started investing, but I think he would likely have seen it at this point and realised what was happening. The warning would therefore, to my mind, have prevented further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account Mr L paid C (and B) to purchase cryptocurrency, rather than making a payment directly to the fraudsters. So, he had some control over the money after he made the payments from his Revolut account, and it required further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. Revolut says it is merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have also taken into account that payment 8 was made to another financial business (one offering cryptocurrency services) and that the Revolut account was funded by another account at a regulated financial business prior to each transaction.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr L might have been at risk of financial harm from fraud when he made payment 8, 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 L suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was paid to consumer's own cryptocurrency account does not alter that fact and I think Revolut can fairly be held responsible for Mr L'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 L 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 L could instead, or in addition, have sought to complain against those firms. But Mr L 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 L's compensation in circumstances where: he has only complained about one respondent from which he is entitled to recover his 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 L's loss from payment 8 (subject to a consideration below of whether Mr L has contributed to his losses).

Should Mr L 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.

Mr L can't remember exactly what the promised rate of returns were, these were discussed in a call. But he had made some gains in cryptocurrency himself previously and what was offered through U was better than that. I also haven't seen what level his 'investment' had reached when he tried to withdraw, but I know it must have increased significantly if he was prepared to pay over £4,000 in tax and fees to release it. I consider the likely large increase Mr L saw over a relatively short space of time ought to have been a red flag that things might be too good to be true (given he had some awareness of what could usually be achieved).

I've also considered the fee that Mr L paid towards the end to recover his funds after it was lost through not 'setting up the technical position correctly'. I'm sure the scammers bamboozled him with a convincing explanation, but as someone who had some experience in cryptocurrency I would have expected that situation to have struck him as odd/unusual.

Overall, though, I've found this scam to have been particularly persuasive – and I don't consider there were enough significant warning signs Mr L ignored that would amount to negligence on his part. As I've mentioned, the scammers cloned a legitimate regulated financial business, and there weren't any warnings up or negative reviews online when Mr L found the opportunity. U mimicked typical onboarding processes and had a professional looking website. The communication was also formal and seemingly expert – with receipts being given after each transaction. He set his own password for the platform and (I think fairly) assumed that a degree vetting had been done prior to allowing the advert he saw to be shown on social media. Mr L invested cautiously to start with, and I think would reasonably have been expecting to pay tax on his profits – so those costs wouldn't have seemed too out of the ordinary.

So, even though there were a couple of warning signs that this might not be a legitimate opportunity, I consider the persuasive elements far outweigh those flags. In the circumstances I think Mr L acted reasonably, but unfortunately fell victim to a cruel and sophisticated scam. That means I don't think Mr L has contributed to his losses enough to warrant a reduction in the award, or him sharing the liability for what happened. Revolut, as the financial/fraud experts, had the best opportunity to prevent the loss, and are responsible in this case for not intervening to warn Mr l when it should have.

I've thought about whether Revolut ought to have done more to recover the payments, once alerted to the fraud, and I haven't found that it should have. It considered the chargeback route for the first five payments sent to G, and said those claims weren't successful. I think that assessment was fair, as the scheme rules don't cover a refund in this scenario. The payments were authorised, and the goods or services paid for were likely provided (just not to Mr L). There's also a specific exclusion under the 'goods not received' reason code in the scheme rules for payments made as part of a scam. Same goes for the later payments to buy cryptocurrency – the goods were received, just sent on to the scammer.

I've also thought about whether any additional compensation is warranted, for distress or

inconvenience, and I've decided it's not. Both Revolut and Mr L were the victims of a third party's actions here (the scammer), and although I have no doubt the whole ordeal has affected him greatly, I think the majority of that impact was caused by the fraud itself rather than Revolut. I haven't seen any other service failings that I consider would warrant a further award, and I think the calculation I've directed below fairly redresses any mistakes on Revolut's part.

Putting things right

To remedy the mistake, Revolut should refund in full the transactions it allowed from payment 8 (inclusive) onwards. It should apply 8% simple interest yearly to that refund, from the date each refunded transaction was made (effectively the date of the loss, as it was sent onto the scammer straightaway after being exchanged) until the date of settlement. That interest is to compensate Mr L for the time he's been deprived of the use of his own funds. If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr L how much it's taken off. It should also give Mr L a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

My final decision is I uphold Mr L's complaint, and direct Revolut Ltd to settle matters in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 7 July 2025.

Ryan Miles
Ombudsman