DRN-5188572

The complaint

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

Mr W is being represented by solicitors in this complaint.

What happened

The detailed background to this complaint is well-known to the parties and has been previously set out by our investigator.

Briefly, Mr W fell victim to a cryptocurrency investment scam in 2023. Between February and May, he made several payments (debit card transactions and electronic transfers) totalling around £360,000 from his existing Revolut account to cryptocurrency providers. These were made in connection with an opportunity Mr W came across online. He's explained it was recommended to him by a close friend who he'd known for over ten years and who had a history of extremely successful investments in various fields.

Mr W transferred money from his account with bank "H" into Revolut, before purchasing cryptocurrency from cryptocurrency providers. It was then transferred into wallets as instructed by the scammer, albeit at the time Mr W believed he was making a deposit into his own investment account. Encouraged by the profits he saw were being made, Mr W agreed to 'upgrade' his investment account and continued making payments.

Mr W ultimately realised he'd been scammed when he kept being asked to make further payments before he could access his bonuses and make withdrawals.

Our investigator initially upheld the complaint in part. But after considering additional information, they weren't persuaded that additional steps taken by Revolut would have impacted Mr W's decision to go ahead with the payments. Mr W didn't agree and asked for an ombudsman to make a decision.

From the information available, Mr W initially purchased cryptocurrency directly from his account with H before switching to Revolut. This decision solely relates to Mr W's complaint about Revolut's acts and omissions. But where appropriate, I've taken account of actions that took place in relation to payments made from H – including the funds that were transferred to Revolut.

Mr W made the following payments from his Revolut account in connection to the scam –

	Date	**Method**	**Merchant/Payee**	**Amount ($, €, £)**
Payment 1	1 February	Debit card	Cryptocurrency provider 1	$500.00
Payment 2	2 February	Debit card	Cryptocurrency provider 2	$617.00
Payment 3	2 February	Debit card	Cryptocurrency	$1,040.00

			provider 1	
Payment 4	3 February	Debit card	Cryptocurrency provider 1	$871.00
Payment 5	8 February	Debit card	Cryptocurrency provider 1	$1,200.00
Payment 6	9 February	Debit card	Cryptocurrency provider 1	$241.00
Payment 7	9 February	Debit card	Cryptocurrency provider 1	€46.35
Payment 8	11 February	Debit card	Cryptocurrency provider 1	$2,500
Payment 9	11 February	Debit card	Cryptocurrency provider 1	$524.64
Payment 10	13 February	Debit card	Cryptocurrency provider 1	$2,000.00
Payment 11	13 February	Debit card	Cryptocurrency provider 1	$7,706.32
Payment 12	16 February	Debit card	Cryptocurrency provider 2	$100.00
Payment 13	24 February	Debit card	Cryptocurrency provider 1	$7,991.00
Payment 14	27 February	Debit card	Cryptocurrency provider 1	$6,040.00
Payment 15	28 February	Electronic transfer	Cryptocurrency provider 3	£10.00
Payment 16	28 February	Electronic transfer	Cryptocurrency provider 3	£4,967.00
Payment 17	1 March	Electronic transfer	Cryptocurrency provider 3	£5,000.67
Payment 18	2 March	Electronic transfer	Cryptocurrency provider 3	£5,000.00
Payment 19	3 March	Electronic transfer	Cryptocurrency provider 3	£5,000.00
Payment 20	17 March	Electronic transfer	Cryptocurrency provider 3	£49.19
Payment 21	21 March	Electronic transfer	Cryptocurrency provider 3	£25,000.00
Payment 22	22 March	Electronic transfer	Cryptocurrency provider 3	£51,500.00
Payment 23	29 March	Electronic transfer	Cryptocurrency provider 3	£24,400.00
Payment 24	25 April	Electronic transfer	Cryptocurrency provider 3	£34,500.00
Payment 25	27 April	Electronic transfer	Cryptocurrency provider 3	£34,000.00
Payment 26	28 April	Electronic transfer	Cryptocurrency provider 3	£35,000.00
Payment 27	2 May	Electronic transfer	Cryptocurrency provider 3	£80,250.00
Payment 28	2 May	Electronic transfer	Cryptocurrency provider 3	£250.00

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.

Having done so, I've reached the same outcome as our investigator. I'll explain why.

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.

But, 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 February 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 including in relation to card payments); 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.

It isn't in dispute that Mr W has fallen victim to a cruel scam here, nor that he authorised the payments he made to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer). He's therefore presumed liable for the loss incurred from those payments in the first instance.

But by February 2023, there had been an increased prevalence of investment scams involving cryptocurrency. Both the financial services regulator, the Financial Conduct Authority (FCA), and Action Fraud had warned of cryptocurrency scams. So, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In light of the above, I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr W might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all the payments – both debit card transactions and electronic transfers – were going to a cryptocurrency provider. But I don't think Revolut should reasonably have suspected that Payments 1-10 might be part of a scam. They were

spread over nearly two weeks with individual amounts going up and down in value. So, in my view, there was no obvious pattern emerging that ought to have concerned the EMI.

However, Payment 11 was significantly larger than any other payment that had debited Mr W's account in the year leading up to the disputed transactions, and it was made on the same day as Payment 10. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led it to consider that Mr W was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

In the circumstances, and at that time, I consider that a proportionate response to that risk would have been for Revolut to have provided Mr W with a written warning about the most prevalent type of cryptocurrency scams, i.e., investment scams, tackling some of the typical features. We know that Revolut didn't provide any warnings at that time. But, had it done so, I'm not persuaded that the warning would have stopped Mr W from going ahead with the payment.

This is because Revolut did provide a written warning about cryptocurrency investment scams a couple of weeks later when an electronic transfer (Payment 16) had flagged as suspicious on its fraud detection systems. Mr W selected 'crypto currency' when he was asked for the payment purpose – the investigator mistakenly wrote 'investment' in their assessment. Mr W chose to continue with that payment after acknowledging Revolut's warning, which advised him to research if what he was investing in was a legitimate company or cryptocurrency, and to beware of any third-party having access to his account or asking him to download any software such as those granting remote access.

The warning didn't resonate with Mr W then and, on balance, I don't think it would have resonated with him when he attempted Payment 11 either. In making that finding, I've kept in mind that Mr W placed a lot of trust in his long-term friend's recommendation. He's told us he'd carried out some research before going ahead with the opportunity. That means he likely would have already seen adverse information about the company in question in the public domain and chosen to ignore it. Having carefully thought about what happened here, I'm not persuaded that a written warning about cryptocurrency investment scams when he made Payment 11 would have stopped Mr W in his tracks.

Mr W continued making scam payments over the course of the next few weeks, switching to electronic transfers. Revolut did stop Payment 16 (which I've referenced above) and provided a proportionate scam warning, but Mr W carried on. I don't think the next few payments warranted any intervention given they weren't that unusual compared to the previous ones. But when Mr W made Payment 21, given the significant jump in the value despite going to an existing payee by that point, I think Revolut ought to have been concerned and intervened. And I consider a proportionate response in that instance to have gone beyond a written warning, such as a direct intervention through Revolut's in-app chat.

But had Revolut done so, I'm not persuaded that Mr W's loss would have been prevented. This is because between February and May, Mr W's bank H spoke to him several times when payments flagged as suspicious. These included transfers Mr W made from H to his Revolut account, as well as payments he made directly to the cryptocurrency provider.

Our investigator shared a summary of the call recordings with Mr W's representative. But briefly, for the payments made directly to purchase cryptocurrency, H provided a scam warning to Mr W on 24 February and asked him – amongst other things – whether he'd been approached by people claiming to be crypto managers and assisting him with his investment. The agent also explained that it was a common tactic that smaller payments

were initially made to dupe the customer into making larger payments. Mr W reassured H that none of these scenarios applied to him.

In a later call on the same day, H said it was important that Mr W answered questions honestly. It asked him if anyone had contacted him online and asked him to make the payment into the account for an investment or if he was being offered higher returns. Mr W replied and said no.

Then in March, when transfers to Revolut were blocked, Mr W was asked about the payment purpose, and he said he was buying a flat and the deposit needed to be paid in Euros. In another call, H provided a scam warning to Mr W. This included investment scams and scenarios like investment adverts offering returns that are too good to be true. During a couple of calls, also in March, the agent asked Mr W if he'd been told to lie to the bank about the reason for the payment. He assured them that he hadn't.

It is clear from Mr W's responses to the H's intervention that he didn't want the bank to know why he was sending payments to Revolut. For the payments sent directly to the cryptocurrency provider, he didn't want H to know that a third party was involved, or that he was being assisted or guided with his investment.

Mr W's representative has informed us that on questioning him about the answers provided to H, he said he was vulnerable and under extreme pressure by the scammer to transfer the money – for fear that he would lose his investment. I've thought carefully about Mr W's explanation. Having done so, I'm not persuaded that a direct intervention by Revolut would have prevented him from going ahead with the payments he now disputes. This is not a finding I've made lightly. But the contemporaneous evidence shows that several direct interventions by H didn't work. Even when the payments went directly to the cryptocurrency provider. Mr W misled the bank even when some of the typical scenarios the agents mentioned applied to his circumstances (see above).

Mr W's representative argues that fraud didn't occur at the point he made payments from his account with H. And so, this service should be basing its decision on Revolut's action (or inaction), not H's. The representative submits that as Revolut didn't question the transactions, Mr W should be refunded in full.

But Mr W's representative has completely missed the point around causation. It isn't enough for me to make a finding that Revolut failed to appropriately intervene when I think it should have. I can only ask Revolut to reimburse Mr W if I find that any wrongdoing on its part caused his loss. This concept is one his representative should be very familiar with. Yet it has not sought to substantiate its arguments as to why better questioning would have resulted in Mr W acting any differently given contemporaneous evidence shows he misled another financial business – not just in relation to transfers to his own account with Revolut but also the payments sent directly to the same beneficiary he paid from his Revolut account. Mr W wasn't honest with H. Although he's explained why, for the same reasons, I don't think he would have been honest with Revolut either.

What this means is that I'm not persuaded Revolut could have prevented the transactions Mr W made in relation to the scam.

Thinking next about recovery of payments, given Mr W legitimately bought cryptocurrency from sellers before sending it on to the scammer, it's unlikely recovery would have been successful. This is because services were rendered (i.e., provision of cryptocurrency in exchange for fiat money).

In summary, I know that Mr W will be disappointed with this outcome. Not least because the matter has been ongoing for some time. I fully acknowledge that there's a considerable amount of money involved here. Despite my natural sympathy for the situation in which Mr W finds himself, for the reasons given, it wouldn't be fair of me to hold Revolut responsible for his loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 15 January 2025.

Gagandeep Singh
Ombudsman