DRN-5210740

The complaint

Mr R complains Revolut Ltd didn't do enough to protect him when he lost money to an impersonation scam.

What happened

Mr R says that on 19 October 2023 he inadvertently clicked on a phishing link within a message he'd received advising him he needed to pay a postage fee. As his initial payment wasn't successful, Mr R tried again with different debit and credit cards.

On 20 October 2023, Mr R received a call from what he believed at the time to be his credit card provider (which I'll refer to as "A") informing him that by clicking on the phishing link his phone had been infected and as a result all his bank details were compromised. He was also told that fraudulent transactions had been attempted on his credit card. He was told one of the banks he held an account with, and which he also worked for, (which I'll refer to as "H") would co-ordinate a fraud investigation and would ensure his funds were kept safe.

Mr R has explained that what followed was a *"very elaborate and extremely convincing"* scam, where scammers spoofed legitimate phone numbers for H and referenced real employees from its fraud department that Mr R could find on internal databases. Mr R has said that because of the sophistication and professionalism of the scam he was convinced he was speaking to H.

Mr R has explained that over the following hours he was instructed to transfer his available balance – including an overdraft balance - from an account held with a different bank (which I'll refer to as "N") to Revolut. He says he was initially told his Revolut account was the only account that was not compromised.

Mr R said he was told that having clicked on the phishing link, his phone was compromised which meant the fraudsters could see everything on his phone and could see all the transactions he was making. So, he says he was told he needed to make payments that would appear legitimate – which included payments to a crypto exchange, a money remittance company and an unknown merchant – so the fraudsters did not realise he knew they were watching. He has explained he believed these actions would ultimately protect his funds. This was in fact all a scam, and the money Mr R paid away from his account was lost to scammers impersonating H and A.

In total, Mr R lost £33,466.31 from his Revolut account. I have set out below the successful and attempted transactions from the day of the scam (20 October 2023):

Transaction number	Time	Amount	Payment method	Merchant Category Code (MCC)*/ Payee	Payment successful
1	17:49:35	£8,300	Card payment	6051	Yes
	17:55:11	*£7,500*	*Card payment*	*6051*	*Declined*

	18:35:27	*£7,500*	*Card payment*	*6051*	*Declined*
	18:42:27	*£8,050*	*Transfer*	*Named individual*	*Declined*
	18:45:17	*£8,050*	*Transfer*	*Named individual*	*Declined*
	20:13:58	*£7,540*	*Transfer*	*Named individual*	*Declined*
	20:45:43	*£7,400*	*Card payment*	*6051*	*Declined*
2	20:50:18	£4,950	Card payment	5411	Yes
3	21:31:03	£1,742.16	Card payment	7922	Yes
4	21:58:59	£4,951.99	Card payment	4829	Yes
5	22:06:53	£3,501.99	Card payment	4829	Yes
	22:23:10	*£3,251.99*	*Card payment*	*4829*	*Declined*
6	22:24:42	£3,251.99	Card payment	4829	Yes
7	22:26:25	£3,151.99	Card payment	4829	Yes
	22:34:37	*£3.49*	*Card payment*	*4829*	*Declined*
8	22:34:59	£3.49	Card payment	4829	Yes
9	22:35:33	£1,501.99	Card payment	4829	Yes
10	23:05:39	£703.57	Card payment	7922	Yes
11	23:10:58	£703.57	Card payment	7922	Yes
12	23:14:39	£703.57	Card payment	7922	Yes

* MCC key - 6051 – Quasi cash: Merchant; 5411 – Grocery Stores, Supermarkets; 4829 – Money Transfer; 7922 – Theatrical Producers (Except Motion Pictures), Ticket Agencies

Mr R has explained that having transferred all his available funds from N, including his available overdraft, the scammers tried to encourage him to take out a £20,000 loan. Mr R said when he refused the scammers became aggressive and eventually gave up. He said he then received another call from what he again believed to be A, asking him to share a verification code and pin to stop a £5,000 payment from leaving that account. Mr R said he shared the code but not the pin. He then called A to confirm what was happening and was advised he'd been the victim of a scam.

Mr R immediately contacted Revolut and asked that it stop any pending payments as he'd been the victim of a scam. Revolut arranged to cancel Mr R's existing cards and advised him to submit a chargeback form in relation to the payments he disputed. Although it subsequently confirmed the chargebacks were not valid, as Mr R had authorised the payments through an extra layer of security – 3DS.

Mr R complained to Revolut that it hadn't done enough to protect him from financial loss due to the scam. He said it ought to have recognised his payments towards the scam were both unusual and suspicious. He said despite this Revolut never provided him with any warnings about the risks associated with impersonation scams. Revolut maintained that it could not pursue chargeback claims, as Mr R had authorised the payments, but that it had tried to protect him from fraudulent transactions as it had repeatedly blocked payments. It noted on each occasion Mr R had unblocked his card and repeated the transactions.

Mr R remained unhappy and referred his complaint to the Financial Ombudsman. Our Investigator didn't uphold the complaint. While she considered Revolut ought to have done more to intervene before processing Mr R's payments, she was not persuaded proportionate intervention from Revolut would have prevented his loss. She noted that Mr R had contacted Revolut when two payments were declined and confirmed that he was buying crypto and wanted help making the payment. As part of this interaction, Mr R denied having clicked on a

phishing link or having shared any account information. The investigator concluded that if Revolut had intervened further, Mr R would most likely not have provided it with accurate information that would have enabled the scam to be revealed, as it was clear he was being coached on what to say.

Mr R disagreed. He thought the scammers had targeted his Revolut account as it knew it had less rigorous scam protections than his other bank accounts. He said Revolut ought to have noticed his unusual account activity (including the significant number of times he logged on to his online banking over the course of a day) and the series of payments was completely out of keeping with his usual account usage. Mr R said Revolut should have asked him about the payments, including whether he'd been directed to make them by his bank, and should then have provided him with relevant warnings. He disputed the Investigator's assumption that this sort of intervention would not have broken the spell of the scam. He pointed to the fact the scam unravelled after he received a warning from A telling him not to share a security code.

The case has therefore been passed to me to decide.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I want to make it clear from the outset that there is no doubt that Mr R has been victim of a cruel and sophisticated scam. I do not underestimate the impact this has had on him. Sadly, impersonation scams are increasingly widespread and are becoming ever more sophisticated – which in some circumstances can make it harder for banks and Electronic Money Institutions (EMIs) (like Revolut) to spot that customers may be at risk of financial harm. While there are certain obligations on banks and EMIs to protect consumers and prevent losses to scams in certain circumstances, these are not absolute. And so, there are unfortunately occasions where a consumer will lose out due to a scam but have no recourse to a refund.

So, while I accept Mr R has lost a significant amount of money due to the deception of scammers, I must consider whether Revolut is responsible for the loss he's suffered. I know this won't be the outcome Mr R is hoping for, but for similar reasons to our Investigator, I don't think they are. So, I don't think Revolut has acted unfairly by not refunding the payments. I'll explain why.

I appreciate Mr R has gone to considerable effort when providing his submissions in support of his complaint – providing significant detail as to what he says happened and why he thinks Revolut is responsible for the loss he suffered. I want to reassure him that I've given everything he's said careful consideration. And so, while I've summarised his points, and in far less detail than he provided, I want to stress that no discourtesy is intended by this. If there is a submission or point that I've not addressed, it isn't because I've ignored it. Instead, it's simply because I've focussed on what I consider to be the central issues in this complaint – that being whether Revolut can be fairly held responsible for the loss Mr R suffered due to the scam.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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

In broad terms, the starting position at law is that an EMI, such as Revolut, is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Service Regulations (in this case the 2017 regulations) (PSRs) 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 October 2023 that Revolut should:

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

While I think Revolut ought to have recognised that Mr R was at heightened risk of financial harm from fraud when making some of the payments to this scam, I don't think any proportionate intervention by it would have prevented his loss. I'll explain why.

First, it's important to set out that I'm in agreement with our Investigator that these payments should be treated as authorised. While Mr R may not have completed all the payments steps himself – he was of the understanding that the scammer could and would be making payments from his account – as evidenced by his chat with Revolut where he twice confirmed that he was trying to make payments. So, under the PSRs, these payments would be considered authorised and so Mr R is liable for them.

However, considering the values involved in Mr R's successful transactions, the number of declined transactions, and what Revolut could see from the MCCs (i.e. a large payment going to a known, identifiable crypto merchant), I think Revolut ought to have recognised that Mr R was at a heightened risk of financial harm from fraud. So, I do think Revolut needed to contact him to try and determine what he was doing. It could have done this by, for example, directing Mr R to its in-app chat to discuss the payments further.

But significantly I do not think it would have been immediately apparent to Revolut, based on the information it had available to it (which is outline in the table above), what the specific risk was. I don't think the pattern of payments would have necessarily given it cause to believe Mr R was falling victim to an impersonation scam. As such, I do not agree with Mr R that Revolut ought to have specifically asked him if he was being asked to make payments on the instruction of his bank, as I do not think it had any reason to suspect that at the time. Instead Revolut would have been reliant on the information Mr R provided to understand the actual scam risk so it could then provide him with relevant scam warnings.

If Revolut had attempted to establish the circumstances surrounding the payments, would the scam have come to light and Mr R's loss been prevented?

It's impossible to know with any certainty how Mr R would have responded to Revolut's questions. I've therefore considered the overall circumstances of what happened - along with what Mr R has told us about how the scam unfolded and what persuaded him to believe he was speaking to H – in order to reach a conclusion, on balance, on what I consider most likely to have happened.

Mr R has explained that as part of the scam, he was led to believe that fraudsters were in the process of taking over his account and could see everything on his screen. Mr R was therefore advised to make payments from his account that appeared legitimate, so he didn't reveal to the fraudsters that he knew he'd been hacked. It seems from everything I have been told that Mr R genuinely believed he was speaking with someone at H, and genuinely believed the actions he'd been instructed to take would ensure his money was kept safe. I'm also mindful that Mr R has explained he was in constant contact with the scammers by telephone and was doing exactly as he was told. This is demonstrated by the fact Mr R informed Revolut, through its in-app chat function, that he was buying crypto, even though he's told us this isn't what he thought was happening.

This leads me to conclude that Mr R was prepared to provide answers that made his payments appear legitimate, as he'd been advised to do, rather than providing the answers he believed to be accurate. There is further evidence of this when Mr R answered *"no"* when Revolut asked if he had shared any *"account details through a phishing link/suspicious text"*, even though he knew he had. In fact, this scam was perpetrated on the guise that Mr R's account was compromised by the fact he had clicked on a phishing link.

As a result, even if Revolut had intervened in the way I would have expected it to, I do not think it would have led to the scam being uncovered. I think Mr R would most likely have provided Revolut with answers, as guided by the scammers with whom he was speaking with, that made his payments appear legitimate – as his primary goal at the time was to not tip off the fraudsters, in order to keep his money safe.

Even if Mr R's answers did not completely satisfy Revolut that he was not at risk from financial harm, I don't consider it would reasonably have concluded the mostly likely risk was an impersonation scam. Given the initial payments, I think Revolut may have had concerns Mr R was falling victim to an investment scam. Later payments may also have had the hallmarks of a romance scam, but I do not think Revolut ought to have recognised that the scam risk here was an impersonation scam. As such, any scam warnings I think it would likely have provided would not have resonated with Mr R, as they would not have reflected the true nature of the scam he was in fact falling victim to.

In the circumstances, I'm therefore unable to fairly conclude that proportionate intervention from Revolut would most likely have prevented Mr R's loss.

Could Revolut have done more to recover Mr R's losses

As Mr R's losses originated from debit card payments, the only potential route to recovering the money he lost was via a chargeback. However, Mr R paid legitimate merchants and it isn't in dispute here that the services were provided, just not for the benefit of Mr R. Due to this I don't consider a chargeback claim would've succeeded, so Revolut wasn't wrong to refuse to pursue this for Mr R.

I appreciate Mr R has also expressed concern that Revolut didn't stop his payments when he first notified it that he'd been victim to a scam, even though the payments were showing as pending. But I'm satisfied that there was in fact nothing further Revolut could do to stop the payments once they had been approved by Mr R. A debit card payment shows as pending once the sending bank has processed and approved it, but the merchant hasn't yet requested the funds. There are only limited circumstances in which a pending payment can be cancelled. As Mr R authorised the payments and had sufficient funds available, I don't think Revolut made an error in allowing the merchant to collect the funds. The merchant wasn't the perpetrator of the scam, a third party was.

In conclusion, I have a great deal of sympathy with Mr R being the victim of what was clearly a cruel scam that has had a significant and long-lasting impact on him. But it would only be fair for me to direct Revolut to refund his losses if I thought it was responsible for them – and I'm not persuaded that this was the case here. Everything considered, I cannot fairly and reasonably hold Revolut liable in these circumstances. It follows that I will not be asking it to take any further action.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint. Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 13 March 2025.

Lisa De Noronha
Ombudsman