DRN-3546052

The complaint

Ms Z complains that Revolut Ltd didn't do enough to protect her when she was the victim of a cryptocurrency investment scam. Ms Z lost her life savings of £50,200. She wants her money back.

Ms Z is being supported by a representative, but for ease, I'll refer to Ms Z throughout this decision.

What happened

In early April 2021 Ms Z saw an advert on social media about investing in cryptocurrency. She completed the necessary forms and was contacted by an agent, who she believed to be from a legitimate cryptocurrency investment company, who helped her set up a Revolut account and an account with an online cryptocurrency exchange (which I'll refer to here as 'B') to facilitate the investment. Both accounts were in Ms Z's name. With the help of the scammer, Ms Z transferred money from another bank account (the originating bank) to her newly opened Revolut account. Between 2 April and 24 May 2021 Ms Z transferred eight payments from her Revolut account to 'B' - ranging from £800 to £10,000. The money was then forwarded from 'B' to the scammers.

Upon becoming suspicious, Ms Z contacted Revolut on 7 July 2021. It contacted 'B' on 7 March 2022 to try and recover the funds on Ms Z's behalf. But it received no response.

Ms Z complained to Revolut. It didn't think it had done anything wrong – and in particular, it said no fraud had taken place on Ms Z's Revolut account as the money was transferred to another account in her name 'B'. Revolut accepted it had stopped the first payment of £10,000 due to its size and because it cleared Ms Z's account. Revolut didn't think any further intervention would've made a difference, given Ms Z continued to make payments to 'B'.

Ms Z remained unhappy and so referred her complaint to the Financial Ombudsman. Our Investigator considered the complaint and upheld it. She didn't think Revolut had acted fairly and reasonably in the circumstances. In essence, she said the warning Revolut issued in respect of the first payment wasn't sufficient, and if it had contacted Ms Z, she thought the scam would've been uncovered and the loss avoided.

Revolut didn't agree. It wasn't persuaded that Ms Z was at any time pressured into making these payments – so had time to consider any warnings given before deciding to proceed. And that she could've carried out due diligence at any time during the course of the eight payments if she had any concerns her money was at risk. So essentially, Revolut didn't think any warning it provided to Ms Z would've made a difference.

Revolut added that if it had contacted Ms Z about the first payment, she would've said the payment was going to her own account with 'B'. Revolut said it would've considered this as a legitimate payment – given B is '*a legitimate cryptocurrency exchange platform'.* Revolut added that:

'It is the customer's right to send as much money as they see fit to that platform. In fact, Revolut accounts are often used for precisely that purpose. Revolut could not have known what the funds would be used for after they had been sent to the customer's ['B'] *account, and it is not our job to question that'.*

Revolut said the fraud only took place when funds were transferred from 'B' to the scammer. It said it shouldn't be held accountable for Ms Z loss, and that 'B' should refund the money.

As we have been unable to resolve matters, the case has been passed to me to consider. As part of my review, I put my initial thoughts on the case to Revolut for its comments. In summary, it didn't think it was liable for Ms Z's loss, arguing that no fraud took place at the point Ms Z's funds left her Revolut account. It maintained that 'B' should be held accountable as it was from this account the funds were transferred to the scammer.

Whilst Revolut accepted my view that it should be doing more to investigate payments that are flagged on its systems, it questioned whether Ms Z's payment of £10,000 should've flagged at all given there was no payment history for her and she was making the payment to an account in her own name. With that in mind, Revolut thought Ms Z's originating bank from where she transferred the £10,000 to Revolut should also be held accountable for her loss.

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'm upholding this complaint. And for largely the same reasons as our Investigator. I want to assure Revolut that I've thought carefully about the further points it's put to me as part of my review. But I can't say it's treated Ms Z fairly.

I've read and considered the whole file. But I'll concentrate my comments on what I think is relevant. If I don't mention any specific point, it's not because I've failed to take it on board and think about it, but because I don't think I need to comment on it to reach what I think is a fair and reasonable outcome.

Is Revolut accountable for Ms Z's loss?

Revolut's main point is whether it should be accountable in any way for Ms Z's loss. I recognise the losses occurred later than the transfer from Revolut, involved other financial institutions, and possibly required further action by Ms Z. But I don't have the power to consider a complaint about 'B' in respect of this complaint. And Ms Z hasn't raised a complaint about the originating bank.

Revolut had an obligation to protect Ms Z from financial harm, irrespective of where the money came from or what happened to it after if left her Revolut account. And so, I'm considering Ms Z's complaint about Revolut on that basis.

Is Revolut responsible for Ms Z's loss?

I accept the transactions Ms Z made were authorised payments, even though she was the victim of a sophisticated investment scam. So, although she didn't intend the money to go to the scammer, under the Payment Services Regulations 2017 and the terms and conditions of her account, Ms Z is presumed liable for the loss in the first instance.

However, taking into account what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 financial institutions 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Revolut identified the first transaction of £10,000 as suspicious. I accept the account was only recently opened, so there was no history to compare this transaction to. And I recognise that Revolut accounts are often used for one-off high value transfers. But this was a high value transfer to a cryptocurrency exchange after the account was recently opened. These are all common indicators of cryptocurrency scams. So, I think that this combination of factors, alongside the fact the transaction *did* flag as part of Revolut's own fraud systems, suggests to me that Revolut ought to have intervened.

Revolut has since questioned whether the payment should've flagged at all given Ms Z was making the payment to an account in her own name. Even though it's the case that with cryptocurrency scams the first payment is often made to accounts in the customer's name, in almost all cases we're satisfied firms wouldn't have known this – so the usual triggers apply in terms of out of character or unusual payments. Revolut has told us this isn't true. It says 'B' will only accept deposits from accounts in the customer's name. But, even in those cases, a financial institution won't know the circumstances surrounding a payment. So, if a transaction stands out as being remarkable, as I think the £10,000 should have, an intervention should still normally take place.

Revolut also said the fact someone would empty their account by sending money to a cryptocurrency exchange platform would seem like an obvious scam pattern if we were talking about a normal bank account. But it said that in the case of Revolut, this is a common occurrence, as many customers use their Revolut accounts as a safe intermediary between their savings and their various investment attempts. I would argue that by this logic, Revolut ought to be more up to date with common investment scams than many banks – including cryptocurrency scams - and it ought to be informed enough to provide meaningful warnings to its customers.

And I would argue also that Revolut should be assessing the risk to each customer on the *specific merits* of the payments that are made and whether they flag as suspicious, as it did in the case of Ms Z – rather than applying an approach based on the how its accounts are used more generally.

So, as I've outlined above, I think Revolut was right to flag the £10,000 payment as suspicious. What I've gone on to consider is whether Revolut did enough in response to the risk it identified.

Did Revolut do enough when it identified the risk?

Revolut has explained that it blocked the first payment and displayed a message which said:

'Review transfer

Our systems have identified your transaction as highly suspicious. We declined it to protect you.
If you decide to make the payment again anyway, you can, and we won't decline it. As we have warned you this payment is highly suspicious and to not make the payment, if the person you pay turns out to be a fraudster, you may lose all you your money and never get it back.
You can learn more about how to assess this payment and protect yourself from this link: https://takefive-stopfraud.org.uk/'

Revolut has accepted it should do more to investigate the circumstances surrounding the payments it flags as suspicious. But this didn't happen in Ms Z's case. And as a matter of good industry practice, I think Revolut ought fairly and reasonably to have done more here.

While I appreciate Revolut is generally expected to follow payment instructions, that isn't an unfettered duty. Reasonable checks and balances are also required as part of the broad regulatory landscape to treat customers fairly and to safeguard against the risk of fraud or financial harm. I accept there's a limit to what can reasonably be done. But in this case, I'm conscious that Revolut had already disrupted the payment journey by blocking the payment – regardless of the fact it is now saying the payment shouldn't have been stopped. And I'm not persuaded that the subsequent action it took was enough to meet its obligations to protect Ms Z from financial harm from fraud.

I appreciate that Revolut warned Ms Z that it considered the transactions to be '*highly suspicious*'. But it didn't give any further information about why the payment appeared suspicious – or any information about the type of scam Ms Z was at risk from (or really any scams). Without that information, Ms Z couldn't be expected, from this warning alone, to understand why the payment was suspicious or that a scammer might be involved. Yet Revolut allowed her to re-make the blocked transaction immediately afterwards, despite knowing nothing more about the purpose of the payment or the circumstances surrounding it.

I think Revolut should have done more in relation to the risk it identified. For example, after blocking the payment, it would've been more appropriate to contact Ms Z or require her to get in touch, so it could make further enquiries before deciding how to proceed.

Would appropriate intervention have made a difference?

Revolut doesn't think any more interaction with Ms Z when the first payment was blocked would've made a difference. And that it's not obliged to question a customer on why they're sending funds to a legitimate exchange platform in their own name.

I'm afraid I don't agree. Even if intervention between Revolut and Ms Z would've identified that the payment was going to her own account for the purposes of a cryptocurrency investment, the conversation shouldn't have stopped there on the basis that the money appeared to be going somewhere safe and within her control. This is because by January 2019, we think firms had, or ought to have had, a good enough understanding of how these scams work – including that the consumer often moves money to an account in their own name before moving it on again to the scammer - to have been able to identify the risk of harm from fraud.

In these scenarios, we'd have expected firms to ask additional questions. While it is not up to us to dictate which questions firms should ask, they could've, for example, asked how the customer had been contacted, whether they'd parted with personal details in order to open a trading account, whether they were being helped by any third parties e.g. a broker, whether

the investment opportunity was linked to a prominent individual, advertised on social media etc. These are typical features of cryptocurrency scams.

Ms Z wasn't an experienced investor and hadn't invested in cryptocurrency before. She'd seen the advert enticing her to invest on social media and been advised by the scammer to set up both a Revolut account and an account with 'B' to facilitate the investment. This was all done by the scammer having taken control of Ms Z's computer, using documentation he'd asked her to provide to him. She was also never provided with a contact number for the scammer and was guaranteed she could invest without losing any money. Nor was she provided with a cover story by the scammer in the event she was asked about the reason for the transfer.

So, taking all this into account, if Revolut had responded appropriately to the risk it identified from the first transfer by contacting Ms Z, I think it's more than likely she would've told Revolut exactly what the scammer had told her to do and what she'd been promised. At that point the scam would've been revealed, and the first payment, along with all subsequent payments, wouldn't have happened. I therefore believe appropriate action by Revolut would've prevented Ms Z's entire loss.

Should Ms Z hold some responsibility for her loss?

I've considered carefully whether Ms Z should hold some responsibility for her loss by way of contributory negligence. I think a reasonable person, having spoken to who she thought was an experienced cryptocurrency investor, might be persuaded that the investment was legitimate. Particularly bearing in mind the social engineering and persuasion tactics used by the scammer (coaching her through the process, assuring her of his investment experience and speaking to her in her native language). All of which would make it hard for Ms Z to identify and reflect on any warning signs or carry out any checks before deciding to invest. I don't think Ms Z acted unreasonably here.

Ms Z continued to make payments over a period of time – but she was unaware her money was at risk. She was in constant contact with the scammer, who called her regularly about her investment, advising her on what to do and reassuring her of the gains she could make. And the scammer used a particular type of software that allowed Ms Z to physically see her investment and the gains she was making. She was completely caught up in the scam, and I don't think she ought to have reasonably known she was being scammed or alerted to anything that would have prompted her to carry out any due diligence checks whilst the payments were being made. It was only at the point she wanted access to her gains, and was asked for more money to facilitate this, that she became suspicious.

For the reasons I've set out above, I also don't think the warning – with no details about why the first payment was suspicious or about the scam – would have reasonably alerted Ms Z to the risk. Considering her circumstances and the tactics of the scammer, I consider it reasonable that she was still persuaded that the payment was legitimate – and so went on to make another seven payments oblivious to the scam.

In all the circumstances, I don't think there was contributory negligence here. Ms Z was simply a victim of a sophisticated cryptocurrency investment scam and wasn't partly to blame for what happened.

Putting things right

Revolut should have done more to protect Ms Z from the risk of financial harm from fraud. So, it should refund her £50,200, and pay her interest at the rate she was receiving on her

account with the originating bank (0.1%) from the date of the first payment to the date of settlement.

My final decision

My final decision is that this complaint is upheld. Revolut Ltd should:

- Refund the £50,200 Ms Z transferred to the scammer.

- Pay 0.1% interest (the account interest from the originating bank) on this amount, per year, from the date the first payment left the account (2 April 2021) to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms Z to accept or reject my decision **before 7 October 2022**.

Anna Jackson
Ombudsman