DRN-5252750

The complaint

Mrs H complains that Revolut Ltd ('Revolut') won't refund the money she lost to a safe account scam.

What happened

The background is known to both parties, so I won't repeat all the details here.

In summary, in December 2023, Mrs H received a call from someone claiming to be from her personal bank (I'll call 'B'). She says she was led to believe that her money was at risk. And that she needed to move it to her Revolut account to keep it 'safe'. She later discovered she'd been contacted by a scammer – pretending to be from B's fraud team.

When she reported the scam to Revolut, she said she'd held many calls with the scammer, between 12 and 16 December 2023. And she initially said that, although she'd moved funds from B to Revolut, she didn't make any of the payments that were then made from there to various merchants. She reported she didn't recognise the payees – and that the payments were unauthorised. Revolut declined to refund any of the disputed payments. It considered them to have been 'authorised'. A complaint was then raised and referred to our Service.

Our Investigator considered it and didn't uphold it. She accepted Mrs H had been scammed. But she too thought the payments should be treated as authorised. She noted only Mrs H's device was used to access the account. And concluded there was sufficient evidence that Mrs H would have been aware of payments being made out of her account – either because she'd approved them *in-app,* had keyed in the transfer details, or had given her card details /OTPs to the scammer and asked Revolut to unblock her account at relevant times.

The Investigator also concluded that Revolut took proportionate steps when it contacted Mrs H (through its *in-app* chat) to question her about some of her payments. And that it wasn't at fault for then processing them in line with the instructions it had received.

Below are the payments in dispute. There were several payment/card blocks during this period which aren't listed but I've considered them in reaching my decision.

Date	Time	Payee (ref)	Method	Amount	Auth
12-Dec-23	19:09	Binance	Card Payment	£2,999	3DS
12-Dec-23	19:41	Coinbase	Card Payment	£999	3DS
12-Dec-23	19:43	Coinbase	Card Payment	£2,999	3DS
12-Dec-23	20:46	Kucoin	Card Payment	£1,300	3DS
12-Dec-23	14:16	Moonpay	Card Payment	£999	3DS
13-Dec-23	16:45	Moonpay	Card Payment	£500	3DS
14-Dec-23	17:08	Mrs H	Transfer	£600	*In-app*
15-Dec-23	10:52	Argos	Card Payment	£1,199	Apple Pay
15-Dec-23	12:32	Argos	Card Payment	£799	Apple Pay
15-Dec-23	13:04	Argos Fosse	Card Payment	£1,199	Apple Pay

15-Dec-23	14:25	Swas Fosse	Card Payment	£1,798	Apple Pay
15-Dec-23	14:42	Asda Petrol	Card Payment	£60.40	Apple Pay
15-Dec-23	20:47	Co-Op Group	Card Payment	£500	Apple Pay
16-Dec-23	12:06	Argos	Card Payment	£799	Apple Pay

As the matter couldn't be resolved informally, it's 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.

Has Revolut acted fairly in treating the disputed payments as authorised?

The relevant law here is the Payment Services Regulations 2017 (PSRs). These set out the circumstances in which a payer (Mrs H) and a payment service provider (Revolut) are liable for payments. And the starting point is that Mrs H is liable for payments she's authorised while Revolut should reimburse her for unauthorised ones.

As mentioned above, when Mrs H made her claim she said she knew nothing about the disputed payments out of her Revolut account and that they hadn't been authorised by her. She also said she didnt recall sharing her log in details and no remote access software was downloaded. When the Investigator pointed to the technical evidence showing how the payments were made, she said the scammer manipulated her to follow their instructions. And that, while the payments seem to have been authorised on her device, she didn't knowingly approve them. She added that the scammer convinced her to share the OTPs used to add cards to a new device but she didnt understand the significance of doing so.

In more recent correspondence, Mrs H has said that the scammer was instructing her to do *"certain things"* and that she was led to believe she'd lose all her money if she didn't follow their instructions. She's explained that when she questioned the scammer about the money she'd seen being paid to crypto-platforms and other merchants, she continued to be told that *"everything was fine and my money would all be back in my account by that weekend".*

For the card payments made on 12 and 13 December 2023, Revolut has provided evidence to show only Mrs H's device, which was in her possession, was used to access her account at that time. It has shown the payments were authenticated in Mrs H's *app,* through 'stronger verification' (known as 3DS). I've reviewed the payment screens Mrs H would have seen when 'authenticating' those payments *in-app* and I think it would have been clear the steps she was taking would result in payments out of her account. I've also seen that when payments to a crypto-platform were blocked on 12 and 13 December 2023, Revolut brought Mrs H into 'live' chat – and she confirmed it was her trying to make the payment.

On this evidence, while the scammer probably initiated those payments (using Mrs H's card on the merchant's site), I think Mrs H was likely aware she was approving payments to leave her account – considering the steps she must have taken *in-app*, the screens she'd have seen, and her messages to Revolut saying she was trying to make a payment. Even if I'm wrong about that, the screens she'd have seen *in-app* were clear in that by choosing 'confirm' she was agreeing to payments out of her account. So I'd still think it'd be fair for Revolut to rely on such a representation and treat the payments as authorised.

For the transfer on 14 December 2023, Mrs H would have had to enter the beneficiary sort code and account number in her *app*. I again note that, when a payment was blocked that day, she told Revolut (in 'live' chat) that she wanted to send money to her *"savings"* at

another bank. She provided an explanation around the payment reference she'd used. As before, no one else but Mrs H could have carried out those actions on her device. So, I'm again satsfied it's reasonable for Revolut to treat the transfer as authorised also.

As for the card payments on 15 and 16 December 2023, these were made using Apple Pay. It's agreed these were made after Mrs H had provided the scammer with her card details and OTPs. I'm mindful of Mrs H's comments that *"the scammers convinced her to provide the OTPs, making it seem like a necessary step to resolve the issue they had fabricated"* – and that she's also said she didn't understand the significance of sharing OTPs.

At the same time, I note that when reporting the scam Mrs H told Revolut she'd received *"various codes to add Apple Pay"* and that she kept "freezing" cards because she'd become *"suspicious of the caller".* A 'live' chat interaction on 15 December 2023, further shows Mrs H asking Revolut to *"release my own money"* and *"unblock my account".* I think it's significant she's also now told us that the scammer "...*kept telling me my money would end up back where it should be"* and *"money would be back in my account by that weekend".*

For me, all this again indicates Mrs H was likely aware that her actions (the sharing of card details/ OTPs and her concerns around that, the unfreezing of cards, and the contact with Revolut asking it to *"release"* her money) could result in payments out of her account. To be clear, I recognise Mrs H was manipulated by a scammer and that she didn't think she'd lose this money in the way she did. But, for the purposes of the PSRs, I think these payments too should fairly and reasonably be treated as authorised.

Did Revolut miss an opportunity to prevent Mrs H's losses?

In broad terms, the starting position at law is that a firm (like Revolut) is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer's account.

But taking into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice, it should have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

I think there was certainly enough, considering some of Mrs H's payments and the account activity, for Revolut to have stepped in on concerns that she might be at a heightened risk of financial harm from fraud. But, as referred to by the Investigator (and as I touched on earlier), Revolut did intervene on some payments to find out more.

The first time was on 12 December 2023 on a payment to a crypto-exchange. I can see Mrs H was brought into 'live' chat and, in response to a series of questions, she confirmed the name of the platform she wanted to pay, that she owned and had access to the platform; that she'd previously withdrawn from it; that her partner used the platform; and that she had *"two years knowledge of crypto investing".* She confirmed no-one had told her the option to choose for her 'payment purpose' and that she hadn't been told her account wasnt safe. In turn, Revolut warned Mrs H that it was important she provided honest answers to protect her from scams; that scammers use sophisticated techniques to trick customers into making payments; and that if she was at all suspicious she shouldn't continue.

There was another 'live' interaction on 13 December 2023. When Mrs H confirmed she was attempting further payments to cryptocurrency, she was told she'd reached the limits and had to wait before she could make any more such payments. Mrs H replied *"I cannot wait for 7 days".* It seems payments to cryptocurrency were then automatically blocked. But transfers were instead attempted to personal accounts. For the one on 13 December 2023, Mrs H told Revolut she was *"sending to my sister*", that the sister was "*waiting for it",* that she hadn't

asked for help unexpectedly; that she was repaying her for something she'd bought. When asked for invoices/receipts, Mrs H replied *"No...I trust my family...I don't have that with me".*

When more transfers were attempted on 14 December 2023, Revolut again warned *"It's important that you answer these warnings honestly – they are here to protect you from scams and keep your money safe...You've confirmed that nobody has told you your account isn't safe, is guiding you through these questions...or told you to ignore these warnings. Are you sure this is correct or would you like me to cancel this transfer for you while you double check anything".* Even though Mrs H was warned that scammers may impersonate Revolut or another bank and that someone instructing her on what to do was a red flag for scams, Mrs H confirmed the payment was *"...definitely for christmas gift for my grandchildren".*

I'm again mindful Mrs H was manipulated by the scammer into what to do and say. I don't underestimate the tactics used and I don't imagine she'd have gone along with any of it if she thought she'd lose her money. But her actions show a pattern of cooperation with the scammer. They were able to create a significant level of trust in the relationship such that Mrs H was prepared to follow their instructions, move past warnings, and mislead Revolut about what was really happening. Even if I were to say Revolut could have probed more at times (as might reasonably be expected given some of Mrs H's responses), I think it's unlikely things would have played out very differently given the 'spell' Mrs H was under.

In reaching this view, I note the scammer had also asked Mrs H to put any calls with her bank on speakerphone so they could *"hear and monitor the call*". And I can't overlook that when B intervened, it too was misled about what was going on. In a call, on 12 December 2023, B questioned Mrs H about a payment to Revolut. She confirmed at the outset that no-one was helping her with answering questions and *"nobody has asked me to do anything"*. She was warned that *"customers had been contacted by fraudsters claiming to be from B and that fraudsters had coached customers into not telling the truth around the purpose of payement".* When asked if she'd received any such call or request, Mrs H replied *"Absolutely not".* Importantly, despite a clear warning that frausdters had tricked customers to send money to a *"safe account"* elsewhere, Mrs H confirmed no-one had asked her to do that.

I again recognise Mrs H was an innocent victim in all this and that the scam has affected her deeply. I'm very sorry she's been through this experience. But, on the evidence, I think it's unlikely proportionate steps by Revolut could have prevented the scam. As a matter of causation, I can't reasonably hold it liable for her losses in these circumstances. And in terms of recovery, there was little Revolut could have done. For the card payments, it's unlikely a chargeback based on fraud or good/services not received would have succeeded, as the merchants would have likely been able to evidence that goods/services had been provided as intended (albeit to the scammer, not Mrs H). For the transfer, it's unlikely any funds would have remained to be recovered by the time the scam was reported.

My final decision

For the reasons I've given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 23 October 2025.

Thomas Cardia
Ombudsman