DRN-5053711

The complaint

Ms G has complained that Revolut Ltd ("Revolut") failed to protect her from falling victim to an investment-related scam.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Ms G has used a professional representative to refer her complaint to this service. For the purposes of my decision, I'll refer directly to Ms G, but I'd like to reassure Ms G and her representative that I've considered everything both parties have said.

Ms G has explained that after seeing an advert to invest on a popular social media site, she filled in a contact form and received a message from an individual ("the scammer") in relation to the advertised investment. The scammer gave Ms G some information about the investment, including that it involved trading in cryptocurrency. Ms G has provided a copy of the advertisement she saw, which says *"Anyone who invests £250 will receive £6,930 weekly"* alongside a picture of a well-known financial commentator.

Ms G was given the opportunity to start trading with a low deposit of £250, and she says the scammer was in regular contact to assist her with making the right decisions regarding when to buy or sell particular cryptocurrency, and they appeared to have extensive professional knowledge about investments.

Ms G says the scammer used remote desktop software to connect to her home computer and to set up a wallet with a cryptocurrency exchange for her. Then the payments Ms G made were to her wallet at the cryptocurrency exchange, where she then converted pounds into cryptocurrency. She then forwarded the cryptocurrency on to a cryptocurrency wallet directed by the scammer.

Ms G was given access to an investment platform which showed her alleged trades and the profit she was making. This in turn persuaded her to invest more, and ultimately resulted in her making nine sterling and four Euro payments from her Revolut account to the cryptocurrency exchange.

All of the transactions were debit card payments. The payments were as follows:

	Date	Amount
1	14/02/2023	£1,000
2	15/02/2023	£5,000
3	15/02/2023	£5,000
4	21/02/2023	£25,000
5	23/02/2023	£16,600
6	07/03/2023	£12,000
7	11/03/2023	£5,000
8	08/03/2023	€5,000
9	08/03/2023	€5,000
10	08/03/2023	€5,000
11	08/03/2023	€5,000
12	11/03/2023	£5,000
13	16/03/2023	£2,000

Ms G realised she'd been scammed when she couldn't afford to make a requested payment in order to withdraw funds from her investment account. She applied for a loan to cover the payment, but then after speaking to her sister she came to the realisation that the investment, and the payments she was being asked to make, weren't legitimate.

Ms G made a complaint to Revolut. She said that Revolut should've intervened before the payments were made as they were significantly out of character compared with the usual activity on her account. She said that had Revolut intervened, the scam would've been exposed, and her losses prevented. Revolut didn't uphold the complaint. It referred to its terms and conditions, particularly in relation to customers' responsibilities to keep their security details and Revolut card safe. It also said it couldn't raise a dispute as the merchant had provided the services that Ms G had paid for, albeit as part of the scam.

Ms G remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that although she thought Revolut had several opportunities when it ought to have intervened and didn't, she didn't think that made a difference in this case. She thought this based on the fact that Ms G had said that she wasn't in direct contact with Revolut, but the scammer was discussing the payments with it on Ms G's behalf. With this in mind, she didn't think that any intervention would've been successful, as Ms G wouldn't have been given the opportunity by the scammer to understand and take notice of any warnings Revolut might've given.

As Ms G didn't accept the investigator's opinion, the case has been passed to me to make a decision.

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'm sorry to disappoint Ms G but having considered everything I'm afraid I'm not upholding her complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Ms G authorised these payments from leaving her account. It's accepted by all parties that Ms G gave the instructions to Revolut and Revolut made the payments in line with those instructions, and in line with the terms and conditions of Ms G's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

What did Revolut do to intervene and was it enough?

Revolut has given details on several ways it intervened throughout this scam. It says that it initially restricted Ms G's account on 9 February 2023 when it detected suspicious activity in the form of the Revolut account being credited, with an equivalent payment immediately being attempted to a cryptocurrency exchange. Ms G was directed to contact Revolut using its in-app chat at that point. Revolut asked Ms G several questions relating to the payment, and she confirmed that she hadn't downloaded any remote desktop software and that she hadn't been asked by someone else to either open her Revolut account or promised "too good to be true" returns on an investment. She was also asked to confirm that the cryptocurrency wallet where the payment was being made to was in her name and she had full control of it, which Ms G confirmed as true. During the chat Ms G also told Revolut that nobody had asked her to make any payments and she'd opened her Revolut account for the convenience of purchasing cryptocurrency.

As part of this chat Revolut also said to Ms G "Take your time before making an investment decision. You should try to verify that this is a genuine investment company / opportunity. If someone is asking you to make the transfer quickly, it is likely that they are scamming you and we may not be able to help you recover these funds." Ms G responded with "No one is asking me, everything is alright, I simply want to use your bank because you have a good reputation and I know you are the best internet bank in the UK".

Following this chat Revolut unrestricted Ms G's account and she was able to make the transaction to the cryptocurrency exchange, as well as several more in the following days.

On 17 February 2023 Revolut restricted Ms G's account again after declining three payments to the cryptocurrency exchange. Ms G was again required to contact Revolut using the in-app chat and it's clear from that chat that she was annoyed at the restriction. She again made it clear that she wanted to make the payments and she reminded Revolut she'd already been through a similar experience previously, as well as verifying her identity when she opened her account. Given the previous chat, and Ms G's insistence on this occasion, Revolut unblocked her account and allowed her to make the three previously declined transactions.

Keeping the above in mind, I don't think Revolut acted reasonably in this scenario. It's clear it had systems in place to detect and try to prevent suspicious payments, and it asked Ms G some questions to enable it to understand more about the payments she was making, but it didn't give any specific written warnings in relation to the questions it asked or scam education based on Ms G's answers.

Revolut hasn't provided details on any other interventions it made after this point and given the increase in size and frequency I don't think Revolut did enough to prevent the scam from going further than it did.

I think it would've been reasonable for Revolut to step in when Ms G made payment four. This payment showed a significant increase in size and was again being made to an identifiable cryptocurrency provider. By the time this payment was made, in February 2023, there was enough information available to financial services institutions to know that cryptocurrency-related transactions carried an elevated level of being related to fraud, and I think Revolut ought to have recognised that here.

In this case, owing to the size and pattern of the payments, I would've expected Revolut to establish human contact with Ms G to further discuss the payment with her. It could then have asked probing questions based on her answers, and given tailored and specific warnings based on the information she provided.

Would further intervention by Revolut have made a difference?

I've gone on to consider whether better intervention by Revolut at payment four would've prevented the scam from taking place. And having carefully considered everything, I don't think it would.

It's evident from Ms G's testimony and the chats between her and the scammer that she wasn't in contact with Revolut – but in fact the scammer was. Although Revolut asked Ms G to provide a selfie to verify her identity during the chats, Ms G says she sent the selfie to the scammer, who sent this to Revolut, and chatted to it under the guise of Ms G.

With this in mind, I don't think anything Revolut could've done would've prevented the payments from being made. Although it appeared Ms G knew what the scammer was doing, the scammer was able to continue operating her Revolut account, and making payments, by answering questions and dealing with Revolut's interventions on behalf of Ms G. So whilst I understand this doesn't take away from the seriousness of what's happened to Ms G, or the significant amount of money she's lost, I can't hold Revolut responsible for that, as I'd need to think it could've prevented the financial harm Ms G has experienced, and that's not the case here.

I'm also mindful that when Ms G's account was first opened – which was on the same day as the first payment was made – she told Revolut she'd be using it for "crypto" and "stocks". Although I understand this answer was possibly given to Revolut by the scammer, the way the account was being used when Revolut restricted it was indeed related to cryptocurrency, so it was in line with what Ms G had initially told it. This, alongside Ms G's consistent testimony and insistence on the payments being released, left Revolut in a position where it doesn't appear there was any further reason for it not to release the payments in line with Ms G's instructions.

It's also important to note in this case that the funds Ms G lost were sent to her own account at the cryptocurrency exchange before being forwarded on to the scammer. So it was at that point that Ms G lost the funds, and not when they left her Revolut account. Whilst this doesn't absolve Revolut from its responsibility to be alive to potential fraud and scams on its customers' accounts, it does mean that Ms G may wish to consider contacting her cryptocurrency account provider to pursue the matter further.

I'm firstly mindful that it's not conventional to be introduced to an investment opportunity by social media, and to then discuss that investment on a messaging app without ever meeting or discussing the investment with the advisor in some way. And I'm also not aware that Ms G received any form of paperwork or correspondence related to the investment – such as what she'd invested or what she could expect to receive in return.

This, as well as allowing an unknown third party to access your computer to make payments on your behalf isn't a failsafe way to make an investment, and I think this should've caused Ms G sufficient concern that she should've stopped before allowing the payments to be made.

I've also considered whether things might've been different if Revolut has spoken to Ms G, as opposed to the scammer, during its in-app interventions. In doing this I've reviewed information from the bank Ms G sent the funds to her Revolut account from. That bank spoke to Ms G on the phone seven times before payments were made. In summary, although the payments were being made to Ms G's Revolut account to send on to her cryptocurrency wallet as part of the scam, she told the other bank she was making the payments as she planned to visit a relative in Australia. She was very clearly warned about scams and confirmed – multiple times – that nobody had asked her to make the payments or contacted her using social media or messaging apps. The calls Ms G had with the other bank included various warnings, and very specific scam-related advice, but Ms G chose to proceed with the payments regardless. So although I understand these interventions weren't performed by Revolut, I'm satisfied that they give a good indication of how Ms G would likely have responded had Revolut done even more to intervene, or if it has spoken to Ms G instead of the scammer.

I understand that Ms G was likely coached on how to answer Revolut's questions, and those of the other bank, as I've certainly seen cases where that's happened. But this also makes me think that even if Revolut had done more to warn Ms G about the risks, or to understand more about the payments she was making, it's unlikely those attempts would've been successful. Any interventions would either have been directed to the scammer, or to Ms G who was clearly "under the spell" of the scam, and consequently failed to identify with the many warnings and interventions that took place over the course of around a month.

I recognise there's been some discussion about the origin of the identity verification photos that were sent to Revolut as part of its interventions. Ms G's representative says these were added to the chat by the scammer, but Revolut says these were uploaded from Ms G's phone.

Whilst I can't conclusively say whether the selfies were uploaded by Ms G herself or the scammer, the evidence supplied by Revolut does suggest the photos were taken in real time using the phone that Ms G had registered to her Revolut account. And Revolut says that in order to upload a selfie, this needs to be taken live from within the app, and can't be uploaded from a device's photo gallery – which makes me think the scammer wouldn't have been able to complete this part of the process unless they were with Ms G and had access to her phone.

In any case I'm not persuaded this make a difference relevant to the outcome here. I'm satisfied that Revolut asking for a selfie of Ms G holding a piece of paper with a specific date and time stamp on it is a proportionate way for it to verify her identity. In this case it received what it asked for and the payments were made. It's important to also note that if it was the scammer that uploaded the selfies, they'd have answered Revolut's questions in a way to raise minimal suspicion and ensure the payments were released. But if Revolut had spoken directly to Ms G, from what I've seen, I don't think she'd have been honest with her answers to Revolut, in a similar way to how she answered the intervention questions her other bank asked.

So whilst I understand why this point was brought into question, the answer to it doesn't fundamentally change whether Ms G's losses would've been prevented or not. So it doesn't change my decision.

Recovery of the funds

In this case the payments were made using Ms G's debit card. So the chargeback process is relevant here. In simple terms a chargeback is a mechanism for a consumer, via their card provider, to reclaim money from a retailer's bank when something has gone wrong, provided the transaction meets the eligibility criteria. It's for the card provider to decide whether to raise a chargeback, and it only needs to do so if it has a reasonable prospect of success.

It's also relevant to note that raising a chargeback isn't a legal right, and it's for the debit or credit card provider to decide whether to make a chargeback request to the retailer's bank. The process for managing these claims is determined by a set of rules by the card payment networks and there are no guarantees the card provider will be able to recover the money through the chargeback process.

Revolut says it raised chargeback claims for all the payments, but these were unsuccessful. It was advised that it didn't have chargeback rights in this case as the debit card payments were effectively used to purchase money, as they were used to fund Ms G's cryptocurrency account. As this was completed as expected, the merchant fulfilled its obligation to provide what Ms G paid for. So there's nothing else I'd have expected Revolut to do here as there was no realistic prospect of pursuing a successful chargeback.

I'm very sorry that Ms G has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Revolut responsible for that.

My final decision

I don't uphold Ms G's complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms G to accept or reject my decision before 13 February 2025.

Sam Wade
Ombudsman