DRN-4457717

The complaint

Mr P complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On 12 January 2023, Mr P was on social media when he saw an advert about an investment opportunity which was endorsed by a well-known celebrity. He thought investing would be a good way to generate an income, so he clicked on the link in the ad and completed an online enquiry form. Shortly afterwards, he was contacted by someone claiming to work for a company I'll refer to as "A" who said they would refer him to a senior broker at an investment company I'll refer to as "L".

The broker explained that L specialised in cryptocurrency and commodities and that Mr P would be able to start with a small deposit. He was required to submit photo ID to verify his identity, and L's website had a secure URL and included educational materials and information about the company. He also googled A and learned it was a company hired by investment companies to generate business.

Mr P deposited £250 from another account and the broker told him to open accounts with a cryptocurrency exchange company I'll refer to as "B" and a payments platform I'll refer to as "S". He also told him to download AnyDesk remote access software to his device. Between 18 January 2023 and 13 February 2023, Mr P made 2 transfers to S and 20 debit card payments to B totalling £115,765. There were 11 other transactions which were either reversed or declined.

Each time Mr P made a payment, the broker used Anydesk to move the funds into cryptocurrency wallets on L's trading platform. The broker also encouraged him to take out a loan to cover the negative trades. He realised he'd been scammed when the broker told him he would need to pay £55,000 to release his funds. He complained to Revolut about the payments he'd made to B (the transfers to S were transferred back to the Revolut account), but it refused to refund any of the money he'd lost. It also said he didn't have any chargeback rights.

Mr P complained to this service with the assistance of a representative. He said he wasn't given any effective warnings and the general pop-ups he received simply asked if he was sure he wanted to make the payments, which he was because he thought the investment was genuine. He said he had no investment experience and struggled to conduct proper due diligence and if he'd any indication that the investment was a scam he wouldn't have gone ahead with the payments.

His representative said Revolut should have raised a chargeback request. They also said it should have intervened as Mr P made multiple payments to two new cryptocurrency payees

within the space of one month and that it failed to provide him with an effective warning. They said there was a Financial Conduct Authority ("FCA") warning against B which pre-dated the first payment and there were several serious and obvious fraud indicators.

They said Mr P was required to provide source of funds when he told Revolut the payments to B were for cryptocurrency, but it didn't ask any further questions. They said it should have asked him why he was making the payment, who he was trading with, how he found out about the company, whether he'd researched the company, whether he'd checked the FCA register, whether he'd been promised unrealistic returns, whether he'd received any withdrawals and whether anyone was pressuring him to invest. And as there was no evidence he'd been told to lie, he would have explained what he was doing and it would have realised he was falling victim to an investment scam.

It could then have warned Mr P about the risks associated with paying B and how cryptocurrency accounts are manipulated by scammers telling victims to move funds to various wallet addresses. It could also have told him that scammers often instruct people to open accounts with Revolut for the purpose of investing.

Revolut further commented that it acted promptly to recover any potential losses once Mr P had reported the scam. It said all the transfers were fully authorised and the funds were transferred from Revolut to accounts with cryptocurrency exchanges in Mr P's name and control, so the fraudulent activity didn't occur via Revolut. And the payments weren't covered under the Contingent Reimbursement Model ("CRM") code because he was paying accounts in his own name and control.

It said its security system was triggered on 19 January 2023 and Mr P spoke with an advisor via its live-chat function. He said he'd used Anydesk in the past, the account was intended for keeping part of his money separate from his main account, all transactions were actioned by him, and he understood there was a risk with any investment which is why he was doing it in separate amounts. Revolut said Mr P was given tailored warnings relating to investment scams and he continued with the payment.

On 31 January 2023, it intervened again when Mr P made a payment to S. On that occasion, he was warned about the risks and told that Revolut might not be able to recover the funds if the beneficiary turned out to be fraudulent. He was given a written warning stating: "Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment." Additionally, he received a set of dynamic educational story messages warning him about the risks associated with the payment. He said the payment was for an investment, before being sent more warning messages which warned him there was a high probability that the payment was a scam.

Finally, on 9 February 2023, Mr P confirmed he was investing in cryptocurrency and that he was transferring funds from his own account to an account in his own name.

Revolut argued that the account was newly created, so there were no historical transactions to compare the payments with, but it was clear Mr P wasn't rushed or coerced into making the payments as they were authorised within a period of 26 days. Further, he'd received funds back from S indicating an established relationship and that he was a legitimate user of cryptocurrency platforms. It argued that he had failed to complete reasonable due diligence and when it asked him about the account activity, he misled it by stating that he'd been investing on his own initiative and nobody had asked him to create the account or to make the transfers.

Finally, it said a further intervention wouldn't have been successful as Mr P was strongly under influence of the scammer. He had disregarded warnings from Revolut and provided misleading information. He wasn't concerned when the investment made losses and he made further payments having asked for a copy of the contract with L, which he didn't receive.

My provisional findings

I explained the CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr P says he's fallen victim to, in all but a limited number of circumstances. Revolt had said the CRM code didn't apply in this case because Mr P paid accounts in his own name, and I was satisfied that's fair.

I thought about whether Revolut could have done more to recover the card payments when Mr P reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolt) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr P).

Mr P's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers to L. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr P's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I was also satisfied Mr P 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, he is presumed liable for the loss in the first instance.

There was no dispute that this was a scam, but although Mr P didn't intend his money to go to scammers, he did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

Revolut is an Electronic Money Institution ("EMI") and at the time these events took place it wasn't subject to all of the same rules, regulations and best practice that applied to banks and building societies. But it was subject to the FCA's Principles for Businesses and BCOBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

I thought about whether Revolut could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I'd seen, the payments were made to genuine cryptocurrency merchants. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it did enough to warn Mr P when he tried to make the

payments. If there are unusual or suspicious payments on an account, I'd expect Revolut to intervene with a view to protecting Mr P from financial harm.

Mr P opened the account on 17 January 2023 and the following day he made two payments to B for £450 and £4,500. Those payments went through with no intervention from Revolut and based on the fact he was paying a legitimate cryptocurrency exchange and the payments were low value, I didn't think it missed an opportunity to intervene.

The next day he made several attempts to pay B, which were blocked by Revolut. In the subsequent live-chat conversation, he was asked if he'd recently downloaded AnyDesk, the purpose of the account, whether he'd been told to create the Revolut account and if he'd been encouraged to make an outbound transfer. In response to these questions, Mr P said he'd used AnyDesk in the past and the account was intended for keeping some of his money separate from his main account. The agent pressed him on whether AnyDesk had been used for any of the transactions and he confirmed it hadn't. The agent also asked him to confirm AnyDesk wasn't used to access his Revolut account and he confirmed it wasn't. He was then warned to take time before making investment decisions, that he should try to verify the investment was genuine, and that if he was asked to make transfers quickly it could be a scam. He confirmed he understood the risks and the payment was processed.

I was satisfied Mr P was asked relevant questions during the live-chat and that the agent encouraged him to make further checks on the investment company/opportunity before going ahead with the payments. I was also satisfied that the agent asked probing questions when his responses around the use of AnyDesk were unclear and that they kept questioning him until he confirmed that AnyDesk wasn't involved in the transactions or used to access his Revolut account. Significantly, while it would have been obvious that Mr P was paying a cryptocurrency merchant, the agent was prevented from identifying that the payments were being made to a scam because Mr P wasn't open about the purpose of the account, and he didn't disclose the fact he was being assisted by a broker who had told him to use AnyDesk and to create the Revolut account. Because of this I was satisfied the warning he was given was appropriate based on the information Revolut had and it couldn't reasonably have done anything further to prevent the scam at that point.

On 24 January 2023, Mr P made further payments to B for £5,000 and £15,000. These payments were processed without any intervention from Revolut. As the £15,000 payment was significantly higher than the previous payments Mr P had made to B, even though B was becoming an established payee, I thought Revolut should have intervened. I also thought it should have asked more questions on 1 February 2023 when he was required to provide source of funds for payment of £40,000.

On both of these occasions, Revolut should reasonably have contacted Mr P either by phone or via its live-chat facility and asked him some probing questions about the purpose of the payments including whether there was a third party involved and if so how he met the third party, whether he'd been told by anyone to open the Revolut account, whether he'd been using AnyDesk, whether he'd been allowed to make any withdrawals and whether he'd been promised unrealistic returns.

However, based on the responses Mr P gave to the questions he was asked on 19 January 2023, I didn't think he'd have disclosed any more information about the investment if he'd been asked probing questions on either 24 January 2023 or 1 February 2022. So Revolut wouldn't have discovered anything else about the circumstances of the payments, meaning there would have been no reason for it to have given a more tailored warning. And I didn't think it would have made a difference if he'd been given another scam warning. This is because he didn't do more research when he was advised to do so on 19 January 2023, and

he made more payments to the scam having been given warnings on 19 January 2023 and 31 January 2023 when he'd tried to make a payment to S.

I was satisfied that Mr P had clearly trusted the broker to the extent that he was prepared to mislead Revolut and ignore the warnings that it gave him on 19 January 2023 and 31 January 2023. He was satisfied that L's website and trading platform were professional and well-presented, and that the website had a secure URL and L had London address. So, while I accepted Revolut missed further opportunities to intervene, I didn't think they represented missed opportunities to prevent to scam.

The final intervention happened on 9 February 2023 when again the account was put under review and Mr P was required to provide source of funds. During this interaction, he told Revolut that he had taken out a loan which he'd paid into the account and that he was investing in cryptocurrency. Having considered what happened during this interaction, I thought Revolut ought to have asked Mr P some more questions about why he was using loan money to fund a cryptocurrency investment and had it done so it might have uncovered some more information about the scam.

I explained that I'd seen evidence that Mr P began to have doubts about the investment on 14 February 2023 as he sought documentation from the scammer to show the nature of the arrangement. But I hadn't seen any evidence that he was any less convinced that the investment was genuine on 9 February 2023 and so even though I thought Revolut ought to have asked more questions about why he was using loan money to fund the investment, I didn't think this represented a missed opportunity to have prevented his loss.

There were further payments to B on 13 February 2023, but by this time it was an established payee and the payment amounts that day were lower than previous payments Mr P had made to the scam, so there would have been no reason for Revolut to intervene at that point.

Overall, while I accepted there were occasions when Revolut ought to have done more during the scam period, I didn't think this represented a missed opportunity to have prevented Mr P's loss and so I wasn't minded to ask it to do anything further to resolve this complaint.

Recovery

I didn't think there was a realistic prospect of a successful recovery because Mr P paid an account in his own name and moved the funds onwards from there.

Developments

Mr P's representative has indicated that he disagrees with the findings in my provisional decision. They have further argued that the complaint should be upheld even though Mr P had been coached on what to say and that Revolut ought to have done more given the high value of the payments which were made in quick succession. They have also suggested the payments should have been stopped completely.

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've reviewed my provisional findings in light of the further comments made by Mr P's representative but I'm afraid the outcome will remain the same. While I accept there were occasions where Revolut failed to intervene or could have asked more questions, I don't think those occasions represented missed opportunities to have prevented the scam and I don't think it should have stopped the payments completely.

I remain satisfied that Mr P was asked probing questions during the live chat on 19 January 2023 and that his responses meant Revolut was prevented from identifying that the payments were being made to a scam. Significantly, he didn't do any more research when he was advised to do so and he made more payments to the scam having been given warnings on 19 January 2023 and 31 January 2023.

Mr P's representative has suggested that Revolut ought to have done more given the high value of the payments and the fact they were made in quick succession. I'm satisfied the questioning and warnings it gave on 19 January 2023 were appropriate based on the information it had. And even if it had intervened again, asking more questions and giving a more tailored scam warning including more information about cryptocurrency scams, I don't think it would have made a difference. This is because Mr P was so convinced that the investment was genuine that he was prepared to mislead Revolut about the circumstances of the payments and he ignored the warnings it did give, so I don't think there was anything it could reasonably have said to change that.

Further, even though I accept Revolut could have done more on 9 February 2023, I don't think this would have made a difference to the outcome because at this point the circumstances hadn't changed and Mr P was still convinced the investment was genuine.

So, while I understand he will be disappointed, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

For the reasons I've outlined above, 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 P to accept or reject my decision before 15 March 2024.

Carolyn Bonnell
Ombudsman