DRN-4531642

The complaint

Miss K complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by two investment scams, or to help her recover the money once she'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.

Miss K was looking for some additional income and came across a company on social media which I'll refer to as "C". She was contacted by someone I'll refer to as "the scammer" who said she could make money by investing in cryptocurrency and was added to a WhatsApp chat with other investors.

The scammer told Miss K to open an account with a cryptocurrency exchange company I'll refer to as "B" and that she could start by making a small initial investment which would bring good returns. He told her the more money she invested the more profit she would make and that she could join a VIP group if her investment reached £50,000.

Miss K was part of the WhatsApp group for a month before investing. She did some research, finding only positive reviews and she checked the scammer worked for C and noted it had a customer support facility and its website seemed professional.

The scammer advised Miss K to open an account with Revolut and to first purchase cryptocurrency through B and then load it onto an online wallet. Between 11 April 2023 and 17 April 2023, Miss K made 10 payments totalling £29,970. Seven of those payments were debit card payments to B and three were transfers to individuals.

Around the same time Miss K was also the victim of a job scam having been approached on WhatsApp regarding a job opportunity, working from home with flexible hours. The job required her to complete tasks online and once she agreed to take on the job, she had professional and comprehensive onboarding. She was also added to a WhatsApp group with others doing the same job. The job required her to use cryptocurrency to purchase tasks for which she would earn commission upon completion of 'sets' of tasks. Between 27 April 2023 and 10 May 2023, she made twelve transfers to B from her Revolut account totalling £13,062.19.

She realised the job was a scam when she was unable to withdraw her commission. And she discovered the investment was also a scam when she tried to make a withdrawal from the platform and wasn't able to access her investment.

She complained to Revolut and it refused to refund any of the money she'd lost. It explained its chargeback team had contacted B who had disputed the claim and provided valid documentation, so the claim wasn't pursued. And it was unable to raise a scam claim for the transfers because she hadn't provided evidence of a scam.

Miss K wasn't satisfied and so she complained to this service with the assistance of a representative. The representative said the account was created for the sole purpose of the scam which is a known fraud trend, and the pattern of payments should have been cause for concern. They said Miss K had never bought cryptocurrency before, so the frequent payments to a new, high risk merchant was a drastic change in account usage and the movement of money in and out of the account should have raised concerns.

They accepted Revolut had done a source of funds check on the first payment, but they argued she was given no warnings or education and that if it had intervened properly it would have seen there were red flags present and exposed the scam. They have explained Miss K didn't understand the reason for the security checks, she doesn't remember saying she wasn't buying cryptocurrency and she didn't know the involvement of a broker was important. They further explained Miss K had continued to make payments after receiving a warning on 13 April 2023 because she thought she'd spoken to others who had made money. And they argued the fact she denied buying cryptocurrency when it was clear she was paying money to a cryptocurrency merchant should have been a red flag.

Revolut said that when Miss K opened the account, cryptocurrency featured in the list of declared purposes and there was no account history to determine what was normal account activity. It said she should have realised the job offer was too good to be true and questioned why she was being asked to make payments in cryptocurrency for tasks that she was supposed to be earning money to complete and that she had sufficient time to perform due diligence.

It said the account triggered an alert on 13 April 2023 and it asked Miss K whether she used any finance managing or shared wallet applications and whether she'd recently downloaded any screen sharing applications e g. AnyDesk. She was also asked about the purpose of the account, whether she'd received any calls from anyone telling her to create a Revolut account and encouraging her to make an outbound transfer.

She was then asked to explain why she was paying B, to which she responded "this is my own money that I am responsible for. If there is any loss I will bear it myself I think I am entitled to use my money without explaining every single detail. Please if you can't lift the restrictions allow me to transfer my money back to the original bank account."

It also asked whether she was being pressured to act quickly because she was at risk of missing out on an investment opportunity, whether she'd been promised returns which seemed too good to be true and whether she'd been contacted or encouraged to invest by someone she didn't know or had met online recently.

It said Miss K chose to ignore four separate warnings about the transfers, she'd received a warning each time she set up a new payee and a tailored warning when she made payment 6 on 15 April 2023. On that occasion the payment was put on hold and she was shown a message about the purpose of the payment, followed by educational screens regarding the type of potential scam.

It said its chargeback team was unable to recover the card payments because they were verified by 3DS using Miss K's trusted device and she had paid a genuine merchant. It also said the card payments were transferred to an account in her own name and control and the fraudulent activity didn't occur via Revolut as the funds were sent to a legitimate cryptocurrency exchange and then lost as a result of sending the funds to cryptocurrency wallets.

My provisional findings

I thought about whether Revolut could have done more to recover the debit card payments when she 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. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Miss K).

Miss K's own testimony supported that she used cryptocurrency exchanges to facilitate the transfers. 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 Miss K 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.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss K says she's fallen victim to, in all but a limited number of circumstances. The CRM code didn't apply to the payment Miss K made to an account in her own name. And two of the transfers were to individual accounts, but Miss K received the cryptocurrency she paid for, so the Code wouldn't apply.

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

There's no dispute that Miss K was scammed, but although she didn't intend her money to go to scammers, she 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 emoney/money remittance provider 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 a genuine cryptocurrency exchange company. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of wider scams, so I needed to consider whether it did enough to warn Miss K when she tried to make the payments.

Revolut had explained that Miss K was presented with the following written warning each time she set up a new payee: "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"; "Does this offer seem too good to be true" ; "Was the product or service you are paying for advertised on a social media platform or has a small number of reviews"? This warning was presented for each of

the four new payees and based on the size of the payments and the information Revolut had available to it, I was satisfied the warning was relevant, proportionate and effective.

On 12 April 2023 Miss K tried to make a payment of £19,954, which was declined. The following day, she tried to make further payments and contacted Revolut because her account was still restricted. During the live-chat Miss K was asked if she was using any screen sharing applications, what was the purpose of her account, and whether she'd been told to open the account or to make any outbound transfers. She was also asked whether she was buying cryptocurrency, whether she'd been promised returns which were too good to be true and whether she'd been encouraged to invest by someone she didn't know or who she'd met online recently.

Miss K said she hadn't been told to open the account and the transaction was to pay for services. She initially said she wasn't buying cryptocurrency and when pressed, she said she'd bought USDT and intended to purchase more. She also said she hadn't been promised unrealistic returns, she hadn't been encouraged to invest and she knew about scams.

I considered the nature of the questions Miss K was asked and I was satisfied they were sufficiently probing and relevant and that Revolut did probe when she denied buying cryptocurrency. Significantly it was clear that she was being guided by the scammer when she wasn't open about her intention to invest in cryptocurrency and didn't disclose that she was taking advice from a third party. And this meant it was prevented from identifying that she was being scammed.

Revolut warned Miss K about the risk of sophisticated scams, and based on the limited information it had, I was satisfied this was reasonable and that taking into account the answers she gave to the questions and the fact she had included buying cryptocurrency in the list of reasons for opening the account, it couldn't reasonably have been expected to have provided a more tailored warning. And I didn't think it was unreasonable for it to have lifted the restriction on the account.

On 15 April 2023, Miss K made two further payments to B for £5,000 and based on the cumulative value of the payments, I thought Revolut ought to have intervened. I explained I would expect it to have contacted Miss K again via the live chat facility and to have asked her why she was making the payments, whether there was a third party involved and if so how she met them, whether she'd been told to download AnyDesk to her device, whether she'd been promised unrealistic returns and whether she'd been allowed to make any withdrawals. But, based on the answers she gave on 13 April 2023, the fact she'd been coached to lie by the scammer and the fact she'd ignored the previous warnings from Revolut, I didn't think she'd have been honest in her responses and so it wouldn't have had enough information to identify that she was being scammed.

Miss K was clearly convinced the scam was genuine to the extent that she was prepared to lie to her bank. She had explained that this was compounded by the fact she truly believed she'd been speaking to other people who had made money from their investments and that she'd done what she believed was reasonable due diligence. I accepted there were red flags present including the fact she'd been contacted on WhatsApp, she had been instructed to open the account for the purpose of the scam and she was being asked to send funds to a third party wallet. But Miss K's willingness to mislead Revolut meant it wasn't made aware of these red flags and so even though I thought it missed an opportunity to intervene on 15 April 2023, I didn't think this represented a missed opportunity to have stopped the scam.

I considered the payments that followed and as B had become an established payee and none of the later payments exceeded £5,000, I didn't think Revolut missed any further opportunities to intervene.

Compensation

I stated Miss K isn't entitled to any compensation or legal costs.

Recovery

I didn't think there was a realistic prospect of a successful recovery because Miss K paid accounts her own name and moved the funds onwards from there. And she wouldn't have been able to recover the funds she paid to individuals because she received the cryptocurrency she paid for.

Developments

Miss K has responded to say that she doesn't agree with my provisional findings. She has explained that she was coerced into making the payments and described the impact the scam had on her.

She accepts that Revolut did intervene, but she has suggested it should have closed her account to protect her from financial harm. She has also explained that the scammer influenced her to mislead Revolut and that they told her it had restrictions in place regarding the purchase of cryptocurrency.

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 considered Miss K's additional comments but I'm afraid the findings in my final decision will be the same as the findings in my provisional decision. There is no dispute that the payments were made in relation to a scam, but Revolut would only be required to provide a refund in circumstances where it could have done more to prevent the scam from occurring altogether.

Miss K has argued that it could have prevented her loss by closing her account. But as I've explained above, I'm satisfied the warnings it gave each time she set up a new payee were relevant, proportionate and effective. During the call she had with Revolut on 13 April 2023, it was prevented from identifying that she was being scammed because she didn't disclose that she was taking advice from a third party. And I maintain that any later intervention would have had the same outcome.

I accept that closing the account might have prevented Miss K's loss, but based on the information Revolut had available to it, this wouldn't have been reasonable or proportionate and I don't think it erred in allowing her to continue to make payments from the account.

Overall, I remain satisfied that Revolut took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Miss K has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss K to accept or reject my decision before 1 April 2024.

Carolyn Bonnell
Ombudsman