DRN-5002984

The complaint

Mrs H complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an investment scam, 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.

In January 2023, Mrs H saw an advertisement on social media for an opportunity to invest in cryptocurrency with a company I'll refer to as "K". She wasn't an experienced investor and struggled to conduct any due diligence beyond checking K's website, but the advert was endorsed by a well-known celebrity, which further reassured her.

She completed an online enquiry form and received a call from someone I'll refer to as "the scammer" who claimed to be an account manager. The scammer seemed professional and articulate, and Mrs H thought the rate of return seemed reasonable.

Once Mrs H had confirmed that she wanted to invest, she paid an initial deposit of £250. The scammer told her to download AnyDesk remote access software to her device which would allow him to place trades on her behalf. He also gave her log in details for her trading account and told her to open accounts with Revolut, and a cryptocurrency exchange company.

The scammer asked her to first purchase cryptocurrency and then load it onto an online wallet. Mrs H opened a Revolut account on 3 January 2023 giving the account opening purposes of spending abroad, vaults, overseas transfers, crypto, and transfers. She then sent funds to Revolut from an account she held with Bank H, and between 9 January 2023 and 19 July 2023, she made 23 transactions to the scam. This included 21 payments and four transfers to four different cryptocurrency exchanges. She also made two exchanges to cryptocurrency on the Revolut platform and withdrew cryptocurrency from Revolut direct to the scammer. Two of the transfers were sent back by the merchant, leaving a total loss of £198,088.

Mrs H monitored her investment on the trading portal and followed the scammer's instructions concerning when to invest more funds. She realised she'd been scammed when her account went into a negative balance, and she was unable to make a withdrawal.

She complained to Revolut when she realised she'd been scammed, and it recovered £14,850 via the chargeback process. But Mrs H wasn't satisfied and so she complained to this service with the assistance of a representative. She said she was motivated to continue investing by the daily increase in her profits, and Revolut should have given her clear scam warnings and encouraged her to carry out further checks. She said she wouldn't have gone through with the payments if she'd known she was falling victim to a scam and that Revolut missed multiple opportunities to stop the payments.

Her representative said Revolut should have intervened because Mrs H was sending multiple unusually high payments to a new high-risk payee in quick succession from a newly opened account, having funded the account immediately on opening with several high value credits. They said Revolut should have contacted Mrs H and asked her whether there were any third parties involved, whether the rate of return was plausible, and if she'd received any withdrawals. And as she was confident the investment was genuine and hadn't been coached to lie, she'd have explained she was investing in cryptocurrency with the assistance of an account manager, and it would have immediately recognised that the investment had the hallmarks of a scam.

Responding to the complaint, Revolut said its controls were proportionate and appropriate and it acted promptly to recover any potential losses once the scam was reported. It said it raised eighteen chargeback requests, twelve of which were rejected, because they were out of time. Three were successful due to the merchant's inability to respond within the timeframe, and three were lost as the merchant successfully showed the money orders had been correctly processed.

It said each transfer to a new beneficiary was authenticated by Mrs H within the Revolut app and the funds were transferred to cryptocurrency accounts in Mrs H's name, so the fraudulent activity didn't occur on the Revolut platform.

It said new beneficiary warnings and educational stories were triggered by four of the payments, warning about the risks associated with the payments. She chose 'investment' as the payment purpose which resulted a further set of tailored warnings based on the stated purpose.

On 7 July 2023, Mrs H acknowledged the initial transfer review warning, and she was asked to select the purpose of the payment and to answer a series of automated questions. Mrs H selected 'investment' and stated that she hadn't been asked to ignore scam warnings, she hadn't been promised returns which seemed too good to be true, she'd done research, and she hadn't been encouraged to invest by someone she didn't know. She then chose to start a chat with a Revolut agent during which she stated she wasn't being pressured to act quickly at risk of missing out on an investment opportunity, she hadn't been promised returns which were too good to be true, she had conducted research, she wasn't been encouraged to invest by someone she'd recently met online and she hadn't been asked to download AnyDesk.

Revolut said the account was newly created and so there was no account history to compare the payments with, there was a gap of four days between the account top up and first transfer, around two months between some of the transactions, so she wasn't rushed or coerced, and the transactions were not out of character considering the account started with a credit from a cryptocurrency merchant, and "crypto" and "transfers" were among the stated account purposes. Mrs H had also received funds back from the cryptocurrency merchants, which indicated an established relationship between the accounts.

It said the messages between Mrs H and the scammer showed she'd gone ahead with the investment having seen negative reviews about K, and that she was asking for guidance from the scammer during its security checks and during the loan applications. She said she could see £6,000,000 in her account after investing under £200,000, which was unrealistic, and there were negative results on Trust Pilot from January 2023. And the use of 'WhatsApp' should have been a red flag because investment companies don't communicate via WhatsApp.

It concluded that Mrs H was asked relevant questions and given with multiple warnings, but she was totally under the scammer's spell and provided misleading information which prevented it from detecting the fraud.

Our investigator didn't think the complaint should be upheld. He explained this service can consider the cryptocurrency exchanges as part of the complaint because they are considered an ancillary act that is within jurisdiction, but we can't consider the withdrawals.

He felt Revolut ought to have been concerned when Mrs H made payment two because the payment was going to a cryptocurrency provider, and it was higher than the previous payment. But he didn't think it could have uncovered the scam, noting that when it asked if she'd downloaded AnyDesk, she said she hadn't. She also said hadn't been contacted and encouraged to invest by someone that she'd recently met online, she'd conducted research, and she hadn't been pressured to act quickly.

He also referenced a call Mrs H had with Bank H on 5 January 2023 when she said no-one had offered her an investment opportunity, and on 29 June 2023 she told Bank L she planned to use the money for her travels and holidays as there aren't any charges with Revolut. Bank L told her scammers tell customers to use Revolut for cryptocurrency and warned her that if the money was subsequently lost, they wouldn't be able to get it back.

Our investigator further explained that on 7 July 2023, Mrs H told Bank H that the £16,500 payment that she was trying to make was because she was hoping to buy a new property overseas. She also said no one had contacted her about an investment opportunity, and she wasn't being coached. And in a call with Lloyds on 19 July 2023, she again said that she was selling a property in overseas.

Our investigator explained that these funds were eventually sent to the scam, and he didn't think that any intervention that reasonably could have been expected of Revolut would have uncovered the scam or prevented her loss, because she was following the scammer's guidance to mislead her banks.

Finally, he was satisfied that Revolut did what it could to recover Mrs H's money once it was aware of the fraud. He explained that for the three chargebacks that were defended, there was no prospect of a successful chargeback because she would have received a service which would have involved changing her payments into crypto before sending it to the wallet address. He noted Revolut had sought recovery of the transferred funds on 23 October 2023, but Mrs H had sent funds to accounts in her own name and moved the funds onwards from there, so there was no prospect of a successful recovery. And he didn't think she was entitled to any compensation.

Mrs H has asked for her complaint to be reviewed by an Ombudsman. Her representative has commented that our investigator has said that Revolut ought to have intervened when Mrs H made the second payment on 26 January 2023 and the evidence relied on to show intervention wouldn't have prevented the scam occurred after 31 May 2023 from Revolut, and after 29 June 2023 from Bank H. They've argued that during this time, Mrs H built a rapport with the scammer and had become vulnerable to the fact she'd already put so much money into the scam and didn't want to risk losing it.

They've argued that an earlier effective intervention would have led to open and honest answers from Mrs H as the rapport with the scammer wasn't yet built and she hadn't yet invested such a substantial amount.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mrs H has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I'm satisfied Mrs H '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, she is presumed liable for the loss in the first instance.

There's no dispute this was a scam, but although Mrs H 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.

Jurisdiction

Our service can consider a wide variety of complaints about financial services, but we can't consider all the matters referred to us. The Dispute Resolution Rules (DISP) set out the complaints that fall within our remit and are found in the Financial Conduct Authority's (FCA) handbook. Mrs H's complaint arises from her customer relationship with a UK based firm, which is regulated by the FCA. But there are other factors which affect whether our service can consider a complaint – and DISP includes limits on the activities we can review.

According to the rules, we can consider a complaint under our Compulsory Jurisdiction if it relates to an act or omission by a firm in carrying on one or more of the activities listed under DISP 2.3. Having reviewed those activities, I've decided we can't look into the part of Mrs H's complaint which relates to the transfer or withdrawal of cryptocurrency from the Revolut platform. I hope the below explanation of why is helpful.

Mrs H had an account with Revolut which allowed her to trade in cryptocurrency. But the operation of cryptocurrency services isn't currently a regulated activity, or one that's listed under DISP 2.3 – so we aren't able to look into complaints about it. Cryptocurrency isn't electronic money or 'fiat currency' according to the FCA – instead it classifies cryptocurrency, and similar crypto-assets, as 'exchange tokens'. So, while Revolut is also a Payment Services provider, the withdrawal of cryptocurrency doesn't concern e-money or a payment account – and so doesn't fall under our remit as being about a payment service. However, our service can look into complaints about activities that are ancillary to the ones covered by us (those listed under DISP 2.3). The steps leading up to the transfer/withdrawal of cryptocurrency also includes both the acceptance of funds into Mrs H's account and then a subsequent request for Revolut to exchange fiat money into cryptocurrency.

I am satisfied that these earlier steps amount to payment services, and in the case of the exchanges, at the very least an activity which is ancillary to payment services. Given the broad nature of this complaint, I'm satisfied that the exchange to cryptocurrency is an activity our service can consider.

For the reasons I've given, our service doesn't have the remit to consider the element of Mrs H's complaint which relates to the transfer/withdrawal of cryptocurrency from the Revolut platform.

Prevention

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in January 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

I've 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've seen, the payments were made to genuine cryptocurrency exchange companies. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough to warn Mrs H when she 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 H from financial harm due to fraud.

The payments did flag as suspicious on Revolut's systems and so I've considered whether it intervened at the appropriate time and whether those interventions were proportionate to the risk presented by the payments.

Mrs H was shown new beneficiary warnings before each new payee, and for payments dated 31 May 2023, 29 June 2023, 29 June 2023, and 30 June 2023, she was asked to provide a payment purpose which resulted a further set of tailored warning messages based on the stated purpose. On 7 July 2023, Mrs H was engaged in a live chat before the payment was processed.

I've considered the fact this was a newly opened account and that Revolut would have known that Mrs H was sending funds to a cryptocurrency merchant, and I agree with our investigator that it should have intervened when she made the second payment on 26

January 2023. Based on the value of the payment and the fact she was sending funds to a high-risk payee, I would expect Revolut to have presented Mrs H with a written warning tailored to cryptocurrency investment scams.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case, and, on the balance of probabilities, I don't think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs H's payments, such as finding the investment through an advertisement on social media, being assisted by a broker, and being asked to download remote access software. But I don't think a written warning would have been impactful enough to have stopped the scam because its clear Mrs H trusted the scammer to the extent that she was following his guidance to mislead her banks and to ignore scam warnings, and I think this would have been difficult to counter through a written warning, especially as there are several examples of her having gone ahead with payments after having been presented with relevant scam warnings.

In reaching this conclusion I've considered Mrs H's representative's argument that the examples of her having provided misleading information and ignoring warnings occurred much later in the scam period when she'd invested a lot more money and was desperate not to lose the money she'd already invested. I accept Mrs H would have been under less pressure at the start of the scam, but I note she went ahead with the investment having seen negative reviews on Trust Pilot, and she has also explained that she trusted the scammer because he seemed professional and articulate.

Further, I've listened to a call Mrs H had with Bank H on 5 January 2023 when she said she was trying to make a payment to her Revolut account for her travels. I note she says she said no-one had offered her the investment opportunity because she found the investment herself, but I'm satisfied that the funds being discussed during the call were later sent to the scam and that this is evidence that she was coached from the outset.

I've also considered what would have happened if Revolut had questioned Mrs H sooner, or indeed, if it had intervened again after 7 July 2023. But based on what happened on 7 July 2023, I don't think this would have made any difference.

On 7 July 2023, Mrs H said she hadn't been asked to ignore scam warnings, she hadn't been promised returns which seemed too good to be true, she'd done research, and she hadn't been encouraged to invest by someone she didn't know. Then, in a live chat with a Revolut agent, she stated she wasn't being pressured to act quickly at risk of missing out on an investment opportunity, she hadn't been promised returns which were too good to be true, she had conducted research, she wasn't being encouraged to invest by someone she'd recently met online, and she hadn't been asked to download AnyDesk. I'm satisfied these responses were misleading and that it prevented Revolut from detecting the scam and preventing her loss. And based on the fact I'm satisfied Mrs H was being coached to lie from the beginning of the scam, I think she'd have provided these responses if Revolut had intervened sooner. So, I don't think an earlier (or later) intervention would have made any difference.

In reaching this conclusion I've also thought about the interactions Mrs H had with Bank H and Bank L which I consider further evidence that she was determined to make the payments, and that she trusted the scammer and was prepared to follow his guidance to mislead her banks and to ignore relevant warnings.

While I think Revolut could have intervened sooner, I don't think this represented a missed opportunity to stop the scam and I'm satisfied that when it did intervene its actions were relevant and proportionate to the risk.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mrs H paid accounts in her own name and moved the funds onwards from there.

I've also thought about whether Revolut could have done more to recover the three card payments which were rejected by the merchant. Mrs H's own testimony supports 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 Mrs H's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to pursue the chargeback claims was fair.

As for the claims that were out of time, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mrs H's case, the claims were referred outside of this timeframe.

Compensation

The main cause for the upset was the scammer who persuaded Mrs H to part with her funds. I haven't found any errors or delays to Revolut's investigation, so I don't think she is entitled to any compensation.

I'm sorry to hear Mrs H 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

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 Mrs H to accept or reject my decision before 23 April 2025.

Carolyn Bonnell
Ombudsman