DRN-5313923

The complaint

Mrs R 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 August 2022, Mrs R saw an advert on social media for an investment company which I'll refer to as "R". She completed an online enquiry form and was contacted via WhatsApp by someone who I'll refer to as "the scammer", who said he could assist her to make money by investing in cryptocurrency.

Mrs R was satisfied the opportunity was legitimate, noting R's website appeared professional and the rate of return seemed reasonable. She searched for R on Trust Pilot and didn't see any negative reviews or anything to suggest it was operating a scam.

The scammer told Mrs R to open accounts with Revolut and a cryptocurrency exchange company which I'll refer to as "C". He asked her to first purchase cryptocurrency through C and then load it onto an online wallet. She transferred funds to Revolut from an account she held with Bank N, and between 30 August 2022 and 13 February 2023, she made nine faster payments to C totalling £63,491.08. On 17 October 2022 she received £307.36 into the account from the scam.

Mrs R realised she'd been scammed when the scammer said her funds were locked within the Blockchain, and that she'd need to pay further to release them. She complained to Revolut with the assistance of a representative who said it ought to have questioned her about the payments and had it done so she'd have explained she was investing under the guidance of a broker she'd found on social media, which would have been sufficient to indicate that she was being scammed. But Revolut refused to refund any of the money she'd lost, explaining the transactions were authorised via 3DS, and so there was no valid chargeback under the card scheme rules.

Mrs R wasn't satisfied and so she complained to this service. Her representative said Revolut failed to question her about the payments and provide relevant warnings. They said the payments were significantly higher than other payments on the account and she was paying a new payee. And funds were deposited into the account and then quickly transferred out to a high-risk cryptocurrency merchant.

They said Revolut should have asked Mrs R why she was sending the funds, whether she'd been approached by a third-party, and whether she'd made any withdrawals, and had it done so, it would have discovered that she was being assisted by an unregulated broker who she'd found though an advert on social media. And if Revolut had provided an impactful warning about the risk of scams she'd have undertaken further investigations and ultimately reconsidered proceeding with the transactions.

Responding to the complaint, Revolut explained that Revolut is an Electronic Money Institute (EMI) and accounts are typically opened and used to facilitate payments to cryptocurrency wallets, so the transactions weren't out of character with the typical way in which an EMI account is used. And the transactions aligned with the established purpose of the account.

It further explained that Mrs R was paying a legitimate cryptocurrency merchant and the account was newly created, so there was no historical transaction behaviour profile to determine normal activity, and it appeared she was purchasing cryptocurrency from a legitimate merchant.

It said the payments were authorised via 3DS and it was used as an intermediary to receive funds from Mrs R's external account before they were transferred to an account in her name on a legitimate platform from where she subsequently lost control of the funds, so it shouldn't be held responsible. It also cited the Supreme Court's judgment in Phillip v Barclays Bank UK plc where the Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, no enquires are needed to clarify or verify what the bank must do.

Finally, it argued that the transactions were self-to-self transactions and for this service to effectively apply the reimbursement rules to self-to-self transactions executed by Revolut is an error of law. It said it is irrational to hold it liable for Mrs R's losses in circumstances where it is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on the customer.

Our investigator didn't think the complaint should be upheld. He commented that Revolut ought to have known Mrs R was paying a cryptocurrency merchant and that it should have intervened when she made payment five on 4 January 2023. But he didn't think this would have made any difference because even if it had asked questions to establish the circumstances surrounding the payments, he thought she'd still have gone ahead.

He explained that on 7 February 2023, Mrs R received £10,000 and £1,800 credit into Bank N from her sister which she then moved to Revolut before making payment seven. The payments into Bank N had the reference 'holiday' and Mrs R explained that she told her sister the payment was for a holiday because she was embarrassed to tell it was for a cryptocurrency investment. Because of this, our investigator thought that if Revolut had asked her questions before she made payment five, she'd have misled it about the purpose of the payment, and it wouldn't have detected the scam. So, he didn't think its failure to intervene represented a missed opportunity to have prevented the scam.

Finally, he was satisfied that Revolut did what it could to recover Mrs R's money once it became aware of the fraud because she'd have received a service from the cryptocurrency exchange, so the chargeback attempts were bound to fail. And he didn't think she was entitled to any compensation.

Mrs R asked for her complaint to be reviewed by an Ombudsman. The representative argued that it is unfair to use what she said to her sister as evidence of what she'd have said if Revolut had intervened and that he showed little regard for the fact that an earlier intervention could have prevented her loss. They argued that Mrs R would have been honest about the circumstances of the payment because she didn't know she was being scammed.

My provisional findings

I explained that in deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of

practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

• The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.

• At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mrs R modified the starting position described in Philipp, by expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks".

The October 2017, BSI Code3, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

• Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, 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;

• 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 – (as in practice Revolut sometimes does); and • 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.

Should Revolut have recognised that Mrs R was at risk of financial harm from fraud?

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. 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 ought to have intervened to warn Mrs R 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 Mrs R from financial harm due to fraud.

The payments didn't flag as suspicious on Revolut's systems. This was a newly opened account, and all the payments were to a legitimate cryptocurrency exchange. The first two payments were for relatively low values, so there wouldn't have been any reason for Revolut to intervene. And by the time Mrs R made the payment of £4,995.02 on 22 October 2022, while the amount had increased, C was no longer a new payee.

However, while I accepted it's not unusual for customers to use Revolut accounts to send money to cryptocurrency merchants, I agreed with our investigator that, regardless of whether a payment to a cryptocurrency merchant aligned with the account opening purpose, Revolut ought to have intervened on 4 January 2023 when Mrs R transferred £7,981.72 to C because this was a significant amount and Revolut would have known Mrs R was paying a cryptocurrency merchant.

What kind of warning should Revolut have provided?

I thought a proportionate response would have been to provide a written warning covering some of the key features of cryptocurrency-related investment scans including:

• victims are usually targeted via social media or email.

• scammers will utilise fake positive reviews from other individuals to persuade victims the investment opportunity is legitimate.

• fake online trading platforms can appear professional and legitimate.

I thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss and, on the balance of probabilities, I thought it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs R's

payments, such as finding the investment through an advertisement on social media and being assisted by a third-party broker.

I hadn't seen any evidence that Mrs R was asked, or agreed to, disregard any warning provided by Revolut and I'd also seen no indication that she expressed mistrust of Revolut or financial firms in general. Neither had I seen anything to suggest she'd developed a close relationship with the scammer that Revolut would have found difficult to counter through a warning.

Our investigator expressed concerns that Mrs R told her sister that she wanted to borrow money for a holiday, but I didn't share those concerns because there could be several reasonable explanations for why she didn't want to tell her she was investing in cryptocurrency. I didn't think what she said to her sister is indicative of what she might have said to Revolut, and she wouldn't have been able to tell Revolut she was buying a holiday because she was sending funds to a cryptocurrency merchant.

I was persuaded that Mrs R was not so taken in by the scammer that she wouldn't have listened to some advice from Revolut, and I'd seen no evidence that she was provided with warnings by other firms. Therefore, on the balance of probabilities, had Revolut provided her with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believed it would have resonated with her.

Critically, Mrs R could have paused and looked more closely into the scammer before proceeding and as there was a warning about R on the Financial Conduct Authority ("FCA") website dated 21 November 2022, some basic research could have uncovered the scam.

Is it fair and reasonable for Revolut to be held responsible for Mrs R's loss?

I thought that Revolut should have recognised that Mrs R might have been at risk of financial harm from fraud when she made the fifth payment, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I was satisfied it would have prevented the losses she suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mrs R's own account does not alter that fact and I thought Revolut can fairly be held responsible for her loss in such circumstances. I didn't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I was also not persuaded it would be fair to reduce Mrs R's compensation in circumstances where the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I set out above, I was satisfied that it would be fair to hold Revolut responsible for Mrs R's loss from the fifth payment.

Should Mrs R bear any responsibility for her loss?

I considered whether the settlement should be reduced for contributory negligence, but I didn't think it should.

Mrs R had explained that R had a professional-looking website and she genuinely believed this was a genuine investment opportunity. Having considered the circumstances of the scam, I was satisfied it was sophisticated and I didn't think it was unreasonable for Mrs R to have thought it was genuine. She's said she did some basic online research, and this had left her feeling confident about the investment.

I'd seen no evidence that Mrs R was an experienced investor and so and she wouldn't have known that genuine investment companies don't advertise on social media, and I wouldn't expect her to have known how to search for a warning on the FCA website without having been advised to do so by Revolut. And in any event the warning wasn't published until November, which was after the start of the scam.

Consequently, whilst there may be cases where a reduction for contributory negligence is appropriate, I didn't think this is one of them.

Recovery

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

Mrs R'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 R'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.

Compensation

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

Developments

Mrs R's representative has indicated that she agreed with the findings in my provisional decision and Revolut hasn't responded.

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.

Because neither party has submitted any additional comments or evidence for me to consider, the findings in my final decision will be the same as the findings in my provisional decision.

Putting things right

My final decision is that Revolut Ltd should:

- refund the money Mrs R has lost from the fifth payment onwards.

- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Mrs R with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 6 March 2025.

Carolyn Bonnell
Ombudsman