DRN-5169752

The complaint

Mrs F complains that Revolut 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 June 2022, Mrs F was looking online for investment opportunities when she came across an investment company which I'll refer to as "T". She checked T's website and was satisfied it looked genuine, noting it featured About Us, FAQs, and Contact Us sections.

She completed an online enquiry form and was contacted by someone I'll refer to as the scammer who was calling from a UK landline number. She was required to provide photo ID and proof of address, and noted the scammer's emails included the company phone number, website link, and a logo.

Mrs F paid an initial deposit of £300, and the scammer sent her a link to activate her trading account. The scammer told her to open an account with Revolut and to download AnyDesk remote access software to her device. He told her first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Mrs F deposited funds into the Revolut account from another of her accounts and between 2 June 2022 and 1 December 2022, she made fifteen debit card payments and one faster payment to five different cryptocurrency exchanges. Two of the payments were declined, and the faster payment bounced back.

In November 2022, Mrs F asked the scammer if she could make a withdrawal from her trading account and he said she'd have to pay capital gains tax and other fees, which she paid. She realised she'd been scammed when the scammer continued to ask for further payments.

Mrs F complained to Revolut with the assistance of a representative who said it should have intervened because the payments were high value, and it should have asked probing questions and provided tailored warnings which would have prevented her loss.
Revolut refused to refund any of the money she'd lost, stating there was no trace of fraudulent activity on the account, and the transactions had been authenticated in its app. It said the disputed card transactions were money orders, and once a money order is processed, the service is considered provided, so there were no chargeback rights. It also said the account was newly created, and the transactions were made were to investment platforms and a cryptocurrency exchange, so they weren't suspicious.

Mrs F wasn't satisfied and so she complained to this service with the assistance of her representative who said Revolut should have intervened on 27 June 2022 when she made the payment for £3,500 because she was making a high value payment to a new high-risk payees linked to cryptocurrency. The said it should have contacted her to ask why she was making the payment, who she was trading with, how she found out about the company,

whether she'd done any research, whether she'd been promised unrealistic returns, whether she'd made any withdrawals and whether she was under pressure to make the payment.

Had it done so, Mrs F would have fully explained what the payments were for and that everything had originated from a broker, in response to which Revolut ought to have provided a scam warning.

Revolut explained that the first payment was identified as suspicious and declined. Mrs F was given a new beneficiary warning before each new beneficiary, and it flagged payments on 7 June 2022 and 27 June 2022 when she said the payments were for an 'investment' and 'something else' before being given tailored warnings related to the answers she gave.

It intervened again on 30 November 2022 when Mrs F tried to make a payment for £10,100. The transaction was held after Mrs F acknowledged the initial transfer review warning. She then received a set of dynamic educational story messages to warn her about the risks Mrs F was paying an account in her own name with a genuine cryptocurrency merchant, the account was newly created so there was no transaction history to compare the payments with, and the account opening purpose was to 'gain exposure to financial assets,' so the payments were in line with the reason given.

It concluded that its warnings were proportionate, the payments weren't made in the heat of the moment, and Mrs F failed to conduct appropriate due diligence.

Our investigator thought the complaint should be upheld. He thought Revolut should have intervened on 7 October 2022 when Mrs F made a £10,000 payment and that she should have been questioned by an agent via its live chat facility. He said it should have asked Mrs F about the circumstances of the payments, why she was using multiple payees, what due diligence she'd performed, whether she was acting alone and given information modern-day cryptocurrency scams and how they operate.

He said there was no evidence that Mrs F had been coached to lie and so he was satisfied this type of intervention would have uncovered the scam, so he thought it should refund the money from that payment onwards. However, he thought the settlement should be reduced by 50% for contributory negligence because Mrs F had gone ahead with the payments having been warned the transactions could be linked to a scam.

Mrs F was happy with the outcome, but Revolut asked for the complaint to be reviewed by an Ombudsman arguing that the fraudulent activity didn't take place on the Revolut platform as the cryptocurrency exchanges were the final stage before Mrs F lost control of the funds. It explained that it is an Electronic Money Institute (EMI) which is typically opened and used to facilitate payments of a specific purpose and often not used as a main account. Therefore, the type of payments weren't out of character, or unexpected with the typical way in which an EMI account is used.

It also cited the recent reliance of this service on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) arguing that it is relevant to consider other bank interventions, as the funds that originated with Revolut came from Mrs F's external bank account.

My provisional findings

I issued a provisional decision on 27 February 2025 in which I said as follows:

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 consumer modified the starting position described in Philipp, by – among other things – 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" (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks. In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in October 2022 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

· using algorithms to identify transactions presenting an increased risk of fraud;

· requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;

· using the confirmation of payee system for authorised push payments;

· providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified. For example, it is my understanding that in October 2022, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

· Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)2.

· Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".

· Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

· 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.

· The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

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 October 2022 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.

Prevention

I've considered whether the payments were unusual or suspicious and I agree with our investigator that Revolut should have intervened on 7 October 2022 when Mrs F made the payment for £10,000 because it was a large payment to a new, high risk cryptocurrency merchant.

Revolut processed a payment on 7 June 2022 after having shown Mrs F a new beneficiary warning and a warning that there was a high probability that the payment was a scam. While I think this intervention was proportionate to the risk presented by that payment, I think it should have done more on 7 October 2022 because of the value of the payment and the fact it would have known she was sending funds to a cryptocurrency merchant.

I think a proportionate response would have been for Revolut to ask Mrs F about the purpose of the payment and to provide a written warning which was 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 think it would have.

There were some key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs F's payments, such as being assisted by a broker, being asked to download remote access software and to make onwards payments from the cryptocurrency wallets. And I haven't seen any evidence that she ignored any tailored warnings from Revolut or the bank from which she sent the funds to Revolut. Therefore, on the balance of probabilities, had Revolut provided Mrs F with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her and that she would have paused and looked more closely into the investment before proceeding, as well as making further enquiries into cryptocurrency scams.

Consequently, I'm satisfied that Revolut's failure to intervene on 7 October 2022 represented a missed opportunity to prevent her loss and so I think it should refund the money she lost from that point onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mrs F was to blame for the fact she didn't foresee the risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mrs F to have believed what she was told by the broker in terms of the returns she was told were possible and I haven't seen any evidence that there was much information available online about T which would have raised concerns. Mrs F hadn't invested in cryptocurrency before and so this was an area with which she was unfamiliar.

She wouldn't have known how to check the information she'd been given without being told how to do so by Revolut. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact she trusted the scammer and the fact she believed the trading platform was genuine. And I haven't seen any evidence that she lied to Revolut or that she ignored warnings from Revolut or her other bank. So, I don't think she can fairly be held responsible for her own loss.

Compensation

The main cause for the upset was the scammer who persuaded Mrs F 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.

Recovery

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

Mrs F's own testimony supports that she used cryptocurrency exchanges to facilitate the card 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 F'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 raise a chargeback request against the cryptocurrency exchange companies was fair.

Developments

Mrs F has indicated that she accepts my provisional findings 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 evidence or arguments for me to consider, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

My final decision is that Revolut Ltd should:

- refund the money Mrs F lost from the payment she made on 7 October 2022 onwards, less any credits received.
- 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 F with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 14 April 2025.

Carolyn Bonnell
Ombudsman