DRN-4951365

The complaint

Ms C is unhappy Revolut Ltd didn't refund a payment she sent as part of a scam.

What happened

In February 2024 Ms C received a call from someone pretending to be from His Majesty's Revenue and Customs (HMRC) on a mobile number she didn't recognise. The scammer claimed she had an outstanding tax bill, but Ms C challenged this and said she wouldn't pay until she had something in writing. She was then called back from a number that she confirmed online as belonging to HMRC, and a copy of a letter detailing the amount owed was sent to her during the call via an instant messaging service.

The scammer knew details like Ms C's place of work and annual income, which made her believe the call was genuine. She also wasn't familiar with this country's tax process, and so the request seemed plausible. As a result, Ms C was persuaded to send a transfer for £2,976 (covering the fictitious bill) and told to put her own name in as the one on the beneficiary account, as the associated legal case was against her. She was also threatened with her accounts being frozen and legal action if she didn't comply.

Revolut provided a 'new payee warning' prior to processing the payment. That asked whether she knew and trusted the beneficiary, it gave a reminder to check the details, and warned that fraudsters can impersonate others. Revolut also ran a 'confirmation of payee' (CoP) check, and displayed the result was 'no match' – indicating the name on the recipient account didn't match what she'd entered. Ms C opted to proceed with the payment and Revolut didn't carry out any further fraud checks before processing it.

When the scammer asked for a second payment Ms C became suspicious, and said she wouldn't send any more money before speaking to her employer and HMRC. Once she made those enquiries the scam was uncovered. She then contacted Revolut to report the fraud and request a return of her funds. It attempted to recover the payment, but that was unsuccessful as there was no response from the beneficiary bank, despite several chasers.

Revolut investigated the fraud claim and declined to provide a refund. It said the transaction wasn't sufficiently out of character for the account, so its fraud monitoring system hadn't detected she was potentially at risk. Ms C complained that Revolut hadn't provided an effective scam warning or intervened prior to allowing the payment. She believed the size of the transfer, coupled with the name on the account not matching, meant it shouldn't have gone through without some kind of fraud alert. Revolut maintained its position that it wasn't responsible in its final response to the complaint, and so Ms C referred the matter to our service for review.

One of our investigators considered everything and didn't think the complaint should be upheld. In his view, the transaction wasn't unusual or suspicious enough in appearance to have warranted a fraud intervention from Revolut. The investigator added that the size of it, whilst the largest in the preceding months, was within the expected range for the account, and the destination (another UK bank account) wouldn't have prompted concerns either. He thought the new payee warning given, along with flagging that the account name entered

didn't match, was proportionate to risks apparent.

Ms C didn't accept the investigator's view, and asked for a final decision – so the complaint was passed to me.

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'm not upholding Ms C's complaint. I appreciate that will come as great disappointment to Ms C, who I know feels strongly that Revolut should have done more. I was also saddened to hear about how much the incident had affected her. There's no dispute that Ms C fell victim to a very persuasive scam. But what I must decide is whether Revolut ought to have been on notice she was at risk of financial harm, to the extent that it intervened before processing the payment. On balance, I don't think that was the case here – and I've explained my rationale below.

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 Electronic Money Institutions ("EMI's") such as Revolut are expected to process payments and withdrawals that a customer authorises them 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 March 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 their 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 do);

- 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.

Revolut have a difficult balance to strike in how they configure their systems to detect unusual activity, or activity that might otherwise indicate a higher than usual risk of fraud. There are many millions of payments made each day and it wouldn't be possible or reasonable to expect firms to check each one. In situations where they do (or ought to)

intervene, I would expect that intervention to be proportionate to the circumstances of the payment.

Ms C has rightly pointed out there were risks associated with this payment. It was to a new payee, it was for a larger amount than she would usually send on the account, and the CoP result showed the name she'd entered didn't match the one on the recipient account. Revolut gave a new payee warning, and alerted Ms C about the mismatch in account names – but she chose to continue. So, did Revolut do enough in the circumstances?

I've thought very carefully about that question – and whilst I'm in agreement there were some risk factors present, I don't think there were sufficient indicators Ms C was being scammed. The amount involved, although higher than her recent spending, wasn't so concerning large or out of character to have caused alarm. The payment also didn't drain the account completely, instead it left a balance in line with what was had been seen. Funds being paid in to the account and going out a few minutes later could be seen as riskier behaviour, but Ms C had previously topped up and then sent a payment straight out after a few times. She'd also paid new beneficiaries before. So, I don't think this sequence of activity was overly unusual for the account.

I think the risks inherent with paying someone for the first time were covered by the new payee warning. Revolut also warned Ms C the account name didn't match, and a CoP 'no match' result doesn't necessarily indicate fraud (you could still be paying the right person without knowing the exact name the recipient account is registered in). There wasn't a concerning or typical scam pattern emerging by the time the transfer was made. So, I haven't seen that Revolut missed clear signs it shouldn't be following Ms C's instruction, and instead should have intervened. I appreciate Revolut may have performed fraud checks on transactions prior to this one, and even on payments that Ms C feels were less risky – but I don't think it made a mistake by not doing that here.

I've also considered whether Revolut acted fairly once the fraud was reported, and I can see it contacted the beneficiary bank (in an attempt to recover the funds) within a few hours of Ms C's contact. Revolut also chased for a response several times, but it didn't hear back. So, I don't think any swifter action on Revolut's part would have produced a different result, given it would also have been relying on a quick response from the beneficiary bank (who didn't reply). Fraudsters also typically move funds on very quickly to evade recovery efforts.

Overall, and whilst I recognise that Ms C has lost this money to a cruel and sophisticated scam, I don't think Revolut ought reasonably to have prevented it. I also appreciate Ms C might have been more vulnerable to this type of scam, given she wasn't as familiar with this country's tax system. But I don't consider Revolut was on notice the fraud was occurring, or that it missed signs of her vulnerability in the circumstances. So, I'm not directing Revolut to refund the stolen funds.

My final decision

My final decision is I don't uphold Ms C's complaint about Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 30 May 2025.

Ryan Miles

Ombudsman