DRN-5127054

The complaint

Ms Y complains that Revolut Ltd ('Revolut') won't refund the money she lost to a job scam.

What happened

The background to this complaint is known to both parties, so I won't repeat all the details here. In summary, Ms Y says:

- She was contacted on her messaging *app* by an individual (the scammer) claiming to be from a digital marketing platform (I'll call 'X') about a job opportunity. She searched online and thought she was dealing with a legitimate company.
- For the job itself, it was explained her role was to increase exposure to help associated merchants increase sales and that she'd receive a salary and commission for completing sets of 'tasks'. To make the scam more convincing she was given access to a fake 'work' platform and was added to a 'customer service' group with apparently other 'workers' carrying out a similar role.
- She was told that, as part of the process, she needed to deposit her own funds. These deposits were paid in cryptocurrency which she'd purchased by sending funds from accounts she held with two separate banks (I'll call 'N' and 'M'), to her newly opened Revolut account, and from there to her accounts with legitimate crypto-platforms (I'll call 'B' and 'P'). It was this cryptocurrency that was then sent and lost to the scam.
- She realised she'd been scammed when she tried to access her money but both the scammer and the 'customer service' group stopped responding.

Below are the payments I've considered as part of this complaint. To note, some payment attempts were declined (and don't represent a loss), but I've included them in the table below (*in italics*) as they're relevant to my decision.

	Date	**Method**	**Payee**	**Amount**
1	11-May-23	Card payment	Crypto-exchange - B	£30
2	12-May-23	Card payment	Crypto-exchange - B	£2,400
3	12-May-23	Card payment	Crypto-exchange - B	£650
4	14-May-23	Card payment	Crypto-exchange - B	£2,650
5	29-May-23	Card payment	Crypto-exchange - B	£630.24
	01-Jun-23	*Declined*	*Crypto-exchange - P*	*£150*
6	01-Jun-23	Card payment	Crypto-exchange - P	£150
	02-Jun-23	*Declined*	*Crypto-exchange - B*	*£1,900*
7	02-Jun-23	Card payment	Crypto-exchange - B	£1,900
8	05-Jun-23	Card payment	Crypto-exchange - B	£1,000
9	16-Jun-23	Card payment	Crypto-exchange - B	£900
10	16-Jun-23	Card payment	Crypto-exchange - B	£1,000
11	16-Jun-23	Card payment	Crypto-exchange - B	£2,000
	17-Jun-23	*Declined*	*Crypto-exchange - B*	*£2,025*

	17-Jun-23	*Declined*	*Crypto-exchange - B*	*£2,025*
12	17-Jun-23	Card payment	Crypto-exchange - B	£2,025
13	17-Jun-23	Card payment	Crypto-exchange - B	£75
14	27-Jun-23	Card payment	Crypto-exchange - B	£4,450
15	29-Jun-23	Card payment	Crypto-exchange - B	£4,000
16	04-Jul-23	Card payment	Crypto-exchange - B	£2,000

The scam was reported to Revolut in July 2023. A complaint was later raised and referred to our Service. Our Investigator considered it and upheld it.

In summary, he thought that Revolut ought to have intervened and questioned Ms Y directly about Payment 12 (as above) and that, if it had, then the scam would have likely come to light and Ms Y wouldn't have lost more funds. He said Revolut should therefore refund from Payment 12 onwards, plus interest. He also said that the refund can be reduced by 50% to take into account Ms Y's contributory negligence towards her losses.

Ms Y accepted that outcome. Revolut didn't. I've summarised its representations as follows:

- All the transactions were authenticated by Ms Y. There were no signs of account take over and the fraudulent activity didn't take place on the Revolut account. The funds were sent to accounts in Ms Y's name which she controlled. The purchase of cryptocurrency was legitimate and the funds were lost further in the chain.

- The payments were not out of character nor unexpected with the typical way an EMI account is used, particularly since high street banks have started to place restrictions on cryptocurrency transactions. The account was newly created, so there was no historical behaviour profile that it could have considered to determine normal activity.

- There was a significant gap between the first and last payments. Ms Y had time to perform due diligence and there's no indication she was making payments under pressure or duress. There were no signs of vulnerability and Ms Y didn't do enough to protect herself. And even if Revolut had warned Ms Y about crypto-investment scams, this wouldn't have resonated as she was falling victim to a job scam.

- It's relevant to consider possible interventions carried out by other banks to assess for example whether Ms Y was warned and acted negligently in disregarding warnings. It may also be applicable for our Service to exercise its power to inform the customer that it could be appropriate to make a complaint against another respondent firm if necessary.

As the matter couldn't be resolved informally, it's been passed to me to decide.

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 decided to uphold it for largely the same reasons as the Investigator.

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 (the 2017 regulations) and the terms and conditions of the customer's account. And, as the Supreme Court 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 Ms Y 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 with Ms Y to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's (FCA) Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly.

I'm 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'm 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, at the time of these payments, 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'm 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;[1]
- 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's my understanding that, by May 2023, 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'm also mindful that:

- EMIs 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 don't suggest Revolut ought to have had concerns about money laundering or financing terrorism here. I nevertheless consider these requirements relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017, BSI Code[3], 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 (Revolut was not a signatory), but the standards and expectations it referred to represent 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).

---

[1] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

- 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 that, at the time of these payments, 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 and 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.

Whilst I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in March 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Ms Y was at risk of financial harm from fraud?

It isn't in dispute Ms Y was scammed, nor that she authorised the payments to her cryptocurrency platforms (from where funds were then sent and lost to the scammer).

I'm also aware that cryptocurrency platforms generally stipulate that the card used to purchase cryptocurrency on their platform must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely

have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Ms Y's name.

But by May 2023, firms like Revolut would have been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022.

During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions. By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to buy cryptocurrency using their accounts or increase friction in relation to crypto-related payments, owing to the elevated risk associated with such transactions. And by May 2023, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed the use of their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I also recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm mindful a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our Service). However, our Service has also seen numerous examples of customers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of a fraud victim's money from their high street bank to a cryptocurrency provider, a fact Revolut is aware of.

So, taking into account all of the above, I'm satisfied that by the end of 2022, prior to Ms Y's payments from May 2023, Revolut ought, fairly and reasonably, to have recognised its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the customer's own name. And, considering all of the above, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think the fact that the disputed payments in this case were going to an account in Ms Y's own name should have led Revolut to believe there wasn't a risk of fraud.

I've therefore considered, taking account of what Revolut knew about the payments, at what point, if any, it ought to have identified Ms Y might be at a heightened risk of fraud.

I recognise that, at the time of the payments, Revolut knew much less than we do now about the surrounding circumstances. I'm also mindful that the account was newly opened so Revolut had limited information on which to assess what activity was 'typical' for Ms Y. But like the investigator, I think there was enough going on by Payment 12 for Revolut to have stepped in. I think that a suspicious pattern had emerged by that point looking, for example, at the increase in payment frequency and the multiple payments to the same payee over a relatively short period. I also note Revolut's own records show two earlier payments attempts were declined on that day for 'suspicious activity'. In my view, thinking about all these factors and what Revolut knew about the payment destination, there was enough for it to have been concerned Ms Y herself might have been at a risk of financial harm from fraud. And, in line with good industry practice and regulatory requirements, I think a proportionate response to the risk presented here would have been for it to have questioned Ms Y directly about the circumstances of Payment 12 (through, for example, its *in-app* chat).

For completeness, I think it's arguable Revolut should have shown Ms Y written warnings (tailored to crypto-investment scams, more commonly affecting many customers at the time)

on some of her earlier payments, but I agree it's unlikely these would have resonated and stopped her losses given the nature of the scam she was falling victim to.

If Revolut had attempted to establish the circumstances surrounding Payment 12, would the scam have come to light and Ms Y's losses prevented?

I've thought carefully about whether a discussion about Payment 12 would have likely prevented Ms Y's further losses in this case – and, on balance, I think it would have.

I'm satisfied that if Ms Y had told Revolut she'd been contacted on her messaging *app* by someone who was, for example, instructing her to send her own funds in cryptocurrency as part of a job offering an income for clicking through 'tasks' online and for which there was no contract; and that she was having to pay more during the process, then Revolut would have recognised she was likely falling victim to a scam. There's nothing in the evidence I've seen to suggest she was asked, or agreed to, mislead Revolut about what she was doing or to disregard its warnings. And, having considered the information available about the actions of other firms involved in the payment journey, I've seen nothing to show Ms Y was given (or ignored) any warnings that were relevant to her situation at the time.

In other words, on balance, I don't consider Ms Y was so taken in by the fraudster to the extent she wouldn't have been upfront about what she was doing if questioned and wouldn't then have paid attention to a warning from Revolut about what her particular situation looked like. I think it's more likely a live intervention would have unravelled the scam at that point and Ms Y wouldn't have continued to send more money.

Is it fair and reasonable for Revolut to be held responsible for Ms Y's losses?

In reaching my decision about what's fair and reasonable, I've taken into account that Ms Y first moved money from accounts with other banks, to her newly opened Revolut account, and to her accounts with legitimate crypto-platforms before the funds were lost to the scam.

But, as I've set out above, I think Revolut still should have recognised Ms Y might have been at risk of fraud when she made Payment 12 and that in those circumstances it should have declined the payment and contacted her about what she was doing. If it had taken those steps, I think it would have prevented her further losses. 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 Ms Y's own account does not alter that fact. And I think Revolut can fairly be held responsible for Ms Y's losses in circumstances where it should have done more to prevent them. I don't think there is any point of law or principle that says a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've taken account of Revolut's comments that it's relevant to consider possible interventions by other firms in the chain and that it may be appropriate for Ms Y to complain against other respondents if necessary. And, as noted above, I've reviewed the information we hold about the actions, such as possible interventions, of other firms in the payment journey when deciding what's fair and reasonable in this case. Again, I've not seen anything to evidence that other firms provided Ms Y with warnings relevant to her situation at the time and I'm satisfied Revolut can fairly and reasonably be held liable for her losses in circumstances where it could have done more to prevent them. I'd also note here that, as referred to by our Investigator, he did assess separate complaints from Ms Y about other firms in the chain and he concluded there wasn't more they could have done to prevent the scam.

Should Ms Y bear any responsibility for her losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

As referred to above, the Investigator upheld Ms Y's complaint and thought that Revolut should refund her from (and including) Payment 12. He also concluded the refund payable by Revolut can be reduced by 50%, for Ms Y's own contributory negligence. Ms Y accepted that outcome. I'll nevertheless explain why I too agree with this position.

I appreciate Ms Y says she checked the legitimacy of X online before sending funds and found nothing concerning. And I realise there were some relatively sophisticated aspects to this scam, including the platform which was used to manage the apparent earnings and tasks and a group chat where other 'members' messaged about their successes.

But, at its heart, the scam appears to have been fairly implausible. There was no contract or paperwork about the job itself. And I can't overlook that while Ms Y was offered the chance to earn money, she was asked to deposit her own funds and to pay more during the process. I can't see she was given a particularly plausible explanation as to why she had to finance the 'job' or why she needed to make deposits in cryptocurrency either. I think all this would strike most people as unusual and that if she had acted more cautiously than she did in light of the red flags she'd have likely found this was a scam. In the circumstances, weighing up the role both parties played in what happened, I think liability for Ms Y's losses can fairly and reasonably be shared equally and the refund payable by Revolut reduced by 50%.

Could Revolut have done anything to recover Ms Y's money?

All the disputed payments were made to Ms Y's cryptocurrency platforms and I'm satisfied it's unlikely a chargeback claim would have been successful given there's no dispute Ms Y was provided with the cryptocurrency which she subsequently sent to the scammer.

Putting things right

For the reasons I've given, I uphold this complaint and direct Revolut Ltd to:

- Refund the payments Ms Y lost to the scam from (and including) Payment 12 onwards.
- Reduce this amount by 50% in recognition of Ms Y's contributory negligence.
- Pay 8% simple interest per year on this amount, calculated from the date of the payments to the date of settlement, minus any tax lawfully deductible.

My final decision

For the reasons I've given, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms Y to accept or reject my decision before 9 May 2025.

Thomas Cardia
Ombudsman