DRN-5413922

The complaint

Ms M complains that Revolut Ltd hasn't protected her from losing money to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, I understand that in August and September 2023 Ms M made seven payments totalling £10,441 from her Revolut account as a result of what she thought was a legitimate job opportunity.

Ms M subsequently realised she'd been scammed and got in touch with Revolut. Ultimately, Revolut didn't reimburse Ms M's lost funds, and Ms M referred her complaint about Revolut to us. As our Investigator couldn't resolve the matter informally, the case has been passed to me for a decision.

I sent Ms M and Revolut my provisional decision on 5 March 2025. Now both parties have had fair opportunity to respond, I'm ready to explain my final decision.

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.

Ms M's representative responded to my provisional decision and requested that compensatory interest be added to the settlement figure as Ms M fully intends to repay the funds borrowed from her daughter, friend and brother. But this hasn't persuaded me that it would be appropriate to award compensatory interest in this case. I explained in my provisional decision that our normal interest award would be to compensate the customer for having been deprived of the use of the money they lost from the date of loss to the date of settlement – but it wouldn't be fair to award this here where Ms M wouldn't have had use of the funds in the first place but for the scam. I haven't changed my mind about this. And Revolut didn't respond to my provisional decision. So, in the absence of evidence or arguments persuading me otherwise, I've reached the same conclusions as in my provisional decision, and for the same reasons. I've explained my reasons again 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 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 Ms M 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*".

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***
>
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
>
> - *If legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks;*
> - *…"*

So Revolut was required by the implied terms of its contract with Ms M and The Payment Services Regulations to carry out her instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in August and September 2023 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And, I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But 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 August and September 2023 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 do 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 is my understanding that in August and September 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).

[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_/

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).

- 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 Code[2], 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).

- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[4].*

---

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

[3] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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 August and September 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 – (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.

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

---

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

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

It isn't in dispute that Ms M has fallen victim to a scam here, nor that she authorised the payments.

I'm aware that cryptocurrency exchanges like the one Ms M paid generally stipulate that the card used to purchase cryptocurrency at its exchange 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 these payments would be credited to a cryptocurrency wallet held in Ms M's name.

By August and September 2023, when these transactions took place, firms like Revolut had 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 purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[6]. And by August and September 2023, when these payments took place, further restrictions were in place[7]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I 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 also mindful that 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 consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Ms M made in August and September 2023, Revolut ought fairly and reasonably to have recognised that 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 consumer's own name.

To be clear, it is the specific risk associated with cryptocurrency in August and September 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

---

[6] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

[7] In March 2023, both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice, and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Ms M's name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Ms M might be at a heightened risk of fraud that merited its intervention. And I think that at the point of Ms M's fourth payment from her Revolut account made as a result of the scam – the card payment of £3,000 on 3 September 2023 to a cryptocurrency provider – Revolut ought to have intervened.

What did Revolut do to warn Ms M?

Revolut has said it declined several card payment attempts due to the reason "suspicious activity" during the scam incident. It says Ms M would also have received a standard "adding new beneficiary" warning upon instructing her final payment (which was a transfer, unlike the first six payments which were card payments), which would have then been followed by educational-stories-scam-warnings. It says Ms M would first have seen general scam warning screens, and then she would have been prompted to select an intended purpose of the payment, and once this was done, Ms M would have been presented with more granular information that specifically warned against scam patterns typical for the given payment purpose declaration. Revolut says that in this case Ms M declared the push to card payment in question was being sent for "Cryptocurrency" – and therefore would have been presented with educational stories, which cannot be skipped, while the transfer was put on hold, around scam patterns involving crypto in particular. Revolut says that despite the relevant and appropriate warning, Ms M decided to approve the transaction, hence it was completed.

Revolut also says that Ms M would have received an educational email informing her about current fraud patterns, as well as educating her on how to keep her account safe. It says, from its records, it can see Ms M received such an email on 19 May 2023 but that unfortunately it is unable to determine if the email was opened (and read).

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying

the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by August and September 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam for both APP and card payments. I understand in relation to Faster Payments it already had systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by August and September 2023, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that Ms M's payments were being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victims' money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I am satisfied that, by August and September 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Ms M made the fourth payment, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Ms M was at risk from.

In this case, Ms M was falling victim to a 'job scam' – she believed she was making the payments in order to receive an income.

As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Ms M gave. I'd expect any such warning to have covered off key features of such a scam, such as making payment to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Ms M wouldn't have done so here.

I accept that there are a wide range of scams that could involve payments to cryptocurrency providers. I am also mindful that those scams will inevitably evolve over time (including in response to fraud prevention measures implemented by banks and EMI's), creating ongoing challenges for banks and EMI's.

In finding Revolut should have identified that the fourth payment presented a potential scam risk and that it ought to have taken steps to narrow down the nature of that risk, I do not suggest Revolut would, or should, have been able to identify every conceivable or possible type of scam that might impact its customers. I accept there may be scams which, due to their unusual nature, would not be easily identifiable through systems or processes designed to identify, as far as possible, the actual scam that might be taking place and then to provide tailored effective warnings relevant to that scam.

But I am not persuaded that 'job scams' would have been disproportionately difficult to identify through a series of automated questions (as demonstrated by Revolut's current warnings – which seek to do exactly that) or were not sufficiently prevalent at the time that it would be unreasonable for Revolut to have provided warnings about them, for example through an automated system.

Whilst Revolut may say no evidence has been presented on the prevalence of 'job scams' in August and September 2023, I remain satisfied that this was a sufficiently common scam by this time. For example I'm aware, from my own experience of considering complaints involving scams, that:

- In March 2023, several months before Ms M's payments, another EMI offered "paying to earn money by working online" as a payment option as part of its system designed to (1) identify the purpose of the payments and (2) provide tailored warnings to the common scam types associated with those payment reasons. Where the consumer selected this option, the EMI then provided a warning about job scams (like the one Ms M fell for). It encouraged the consumer to 'stop' as 'this is a scam'. Those warnings involved APP not card payments, but they support my view that job scams of this nature were sufficiently common and well known to feature in scam prevention systems in August and September 2023.

- Versions of job scams have been around for some years (and in many countries). For example, one such example – about which the Financial Ombudsman Service received complaints at the time – featured in an article in The Sun in March 2022 https://www.thesun.co.uk/money/18068901/five-ways-crooks-cost-living/ and a very similar scam was described in a Which? article in June 2023 https://www.which.co.uk/news/article/job-scams-fraudsters-are-posing-as-employers-and-recruiters-on-indeed-and-linkedin-a7NNv8L84n97. And data from Ofcom published in March 2023 found that of 43 million adults who have encountered scams or fraud online, 30% have come across content related to fake employment scams.

- The Financial Ombudsman Service has issued numerous final decisions relating to this type of scam, including some against Revolut, many of which relate to events which pre-date August and September 2023.

- Regarding the overall feasibility of providing a warning using the automated systems example I have referred to (and being mindful that other options are available to establish the purpose of a payment – including human intervention), I note:
    - Revolut itself was able to introduce a similar process in October 2023 (just one month after the payments were made).
    - Its own representations are that in August and September 2023 it could have declined the payment to provide warnings through its chat function (whether or not in practice it did); and
    - As I have explained above, the Consumer Duty (which came into force on 31 July 2023 after an extended implementation period), required Revolut to take steps to avoid foreseeable harm – for example by having adequate systems in place to detect and prevent scams from 31 July 2023.

As I've set out, I accept that under the relevant card scheme rules Revolut cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Revolut ought to have initially declined the fourth payment in order to make further enquiries and with a view to providing a specific scam warning of the type I've

described. Only after that scam warning had been given, if Ms M attempted the payment again, should Revolut have made the payment.

And as I've set out above it did have systems in place in August and September 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time. So, bearing in mind Revolut did intervene but it didn't narrow down the scam risk as I would expected it to have as I've explained above, I've considered what I think most likely would have happened if Revolut had acted as I think it fairly and reasonably should have.

If Revolut had provided a warning of the type described, would that have prevented the losses Ms M suffered from this payment onwards?

I think that a warning of the type I've described would have identified that Ms M's circumstances matched an increasingly common type of scam.

I've read the messages exchanged between Ms M and the fraudsters. I'm persuaded from these messages that Ms M likely wasn't being coached by the scammers on how to interact with Revolut. Nor do I think, from what I've seen, that Ms M was likely so much under the spell of the scam that she wouldn't have been open to Revolut's tailored warnings. Bearing in mind I would have expected, therefore, Revolut's warnings to have narrowed down the scam risk to a job scam, and the type of clear warning it ought to have been able to give about that type of scam, I think it's likely Ms M would have found a number of points about such a warning concerning.

Ms M later sent some payments from another account she opened with a third-party "EMI M", but that EMI has confirmed it didn't intervene in Ms M's payments out of that separate account, so there's no evidence of Ms M being provided with a warning about job scams and ignoring it. I also note that Ms M's complaint about EMI M wasn't upheld at our service on the basis that the payments from that account were insufficient to (and didn't) trigger intervention.

I also note that much of the money paid into Ms M's Revolut account that funded her payments to the scam was paid to her from friends/family which Ms M has explained she borrowed from them. It's difficult to see how the actions of those sending banks could be relevant here. There's no suggestions Ms M's family or friends were falling victim to a scam or that Ms M would have seen any warnings those banks provided. So even if those banks did provide relevant warnings to Ms M's family/friends, it's very unlikely that could have any impact on my finding as to whether Ms M is likely to have decided not to go ahead with the payments from the fourth payment onwards had Revolut provided a warning of the nature I've described.

While Ms M may have topped-up her account at Revolut with £1,000 on 3 September 2023, the value and nature of this payment makes it very unlikely that any warnings would have been provided to Ms M that would have alerted her to the possibility she was being scammed.

Therefore, on the balance of probabilities, had Revolut provided Ms M with an impactful warning that gave details about cryptocurrency job scams and how she could protect herself from the risk of such fraud, I believe it would have resonated with her. She could have paused and looked more closely into things before proceeding further, as well as making further enquiries about such scams. It also appears that when Ms M later mentioned things to friends/family they thought she was being scammed. So it's likely she would have referred to them at this earlier stage instead and the scam would have been uncovered. So I'm

satisfied that a timely warning to Ms M from Revolut would likely have caused her to take the steps she did take later – revealing the scam and preventing her further losses.

Is it fair and reasonable for Revolut to be held responsible for Ms M's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that six of the seven payments were made from Revolut to a crypto exchange before only then being transferred on to the scammers from there. It also appears these funds were borrowed from other people and as I've mentioned above perhaps £1,000 of the money was paid into Ms M's Revolut account from another account of hers.

But as I've set out in some detail above, I think that Revolut still should have recognised that Ms M might have been at risk of financial harm from fraud when she made the fourth payment, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Ms M suffered from the fourth payment onwards. 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 M's own account does not alter that fact and I think Revolut can fairly be held responsible for Ms M's loss in such circumstances. I don'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've also considered that Ms M has only complained further against Revolut and accepted the non-uphold outcome on her complaint about EMI M. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Ms M's compensation in circumstances where: the consumer has only pursued her complaint to this stage about one respondent from which they are entitled to recover their losses in full; would be unlikely to recover any amounts apportioned elsewhere; 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 have set out above, I am satisfied that it would be fair to hold Revolut responsible for Ms M's loss from the fourth payment onwards (subject to a deduction for Ms M's own contribution which I will consider below).

Should Ms M bear any responsibility for her losses?

I've thought about whether Ms M should bear any responsibility for the loss of the £8,521 I've said Revolut should have prevented (that's the total of payments four to seven; the fourth payment is the first payment I think Revolut ought to have prevented; the seventh payment is the final payment Ms M made from her account to the scam). In doing so, I've considered what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

In this case, I don't think it's unfair to say Ms M wasn't as careful with her payments as she reasonably ought to have been. I acknowledge the points Ms M has made about why she thought the job opportunity was genuine. And, for the reasons I've explained above, I do think Ms M most likely wouldn't have made these payments had Revolut warned her appropriately as it should have. Nevertheless, Ms M has said she borrowed this money. And Revolut did provide some warnings to Ms M even if they weren't completely on point. Such

that I think it's fair that Ms M shares responsibility for the loss with Revolut, such that Revolut should pay Ms M 50% of the £8,521 loss, and so £4,260.50.

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

For completeness, I'll address recovery. After the first six payments were made, because they were debit card payments, the only potential avenue to recover them would have been via the chargeback scheme. However, Ms M didn't make the debit card payments to the scammers. Instead, she made them to a legitimate crypto exchange, which would have provided her with the services intended. So Revolut could only have brought chargeback claims against the crypto exchange (and not the scammers) but these wouldn't have succeeded given the circumstances. I also understand that Revolut tried to recover Ms M's seventh (final) payment which was a "push to card" payment, but unfortunately wasn't able to do so, which unfortunately I don't think is surprising given the circumstances. So I can't say Revolut therefore hindered recovery of the funds.

Interest

Ms M appears to have borrowed from friends/family this money that she lost to the scam, such that I'm not persuaded Revolut should be required to pay Ms M interest on the compensation I've said it should pay her. I say this because our normal interest award would be to compensate the customer for having been deprived of the use of this money from the date of loss to the date of settlement. However, as Ms M borrowed this money, whilst I understand it is still a loss because she still owes this money, she hasn't suffered any loss of use because she wouldn't have borrowed or had use of the funds in the first place but for the scam.

My final decision

For the reasons explained, I uphold this complaint in part and I direct Revolut Ltd to pay Ms M £4,260.50.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 17 April 2025.

Neil Bridge
Ombudsman