DRN-4865442

The complaint

Mrs P complains that Revolut Ltd ('Revolut') won't reimburse the funds she lost when she fell victim to a scam.

What happened

What Mrs P says

Mrs P says that she was looking for part time remote job opportunities when she was contacted by someone on a messaging app who claimed to be from a recruitment company. Mrs P's details were passed on to a representative of a company I'll call A in this decision. The representative of A explained the role and advised Mrs P that she could earn £1,600 a month and daily profit of £50 to £150.

Mrs P was provided with a link to A's website and then log in details to a demonstration account to learn what to do before creating her own account. The role involved completing sets of tasks to optimise products. Mrs P was told that if she received a 'merge' product her account would have a negative balance which she would need to clear, but the commission would be tripled. The possibility of getting a merge product was low.

Mrs P started to complete tasks on 1 June 2023 and received her first merge task two days later. To make payment, Mrs P was required to buy cryptocurrency from a cryptocurrency exchange using the peer to peer method and send it to the wallet address details provided by A. Mrs P could then see her payments on A's platform. She could also see the profits she was making. As Mrs P paid more money to the platform the value of the tasks she was asked to complete increased, and Mrs P says she felt compelled to continue so that she didn't lose the funds already paid.

On 10 June 2023 Mrs P was met with a merge task and made around 20 payments to top up her account. After this, Mrs P was advised that A's security system had detected some irregularities in her account, and she needed to pay over 50,000 USDT. Mrs P was concerned and refused to make this payment. After further communication with A, Mrs P realised she would not be able to withdraw her funds as she had been dealing with scammers.

Between 3 June and 13 June 2023 Mrs P made 62 debit card and faster payments on the advice of A's representative. I have set out in the table below these transactions. She paid multiple different payees to buy cryptocurrency via the peer to peer method (as well as cryptocurrency exchanges). I have only recorded whether Mrs P paid an individual or a company to buy cryptocurrency via the peer to peer method.

Transaction	Date	Payee	Payment method	Amount
1	03/06/23	Crypto exchange 1	Card	£200
2	03/06/23	Crypto exchange 1	Card	£250
3	03/06/23	Individual	Transfer	£300

4	04/06/23	Individual	Transfer	£89
5	04/06/23	Individual	Transfer	£120
6	04/06/23	Individual	Transfer	£106
7	04/06/23	Crypto exchange 1	Card	£150
8	04/06/23	Individual	Transfer	£640
19	04/06/23	Individual	Transfer	£403
10	06/06/23	Crypto exchange 1	Card	£1,550
11	06/06/23	Crypto exchange 1	Card	£1,859
12	06/06/23	Crypto exchange 1	Card	£2,000
13	06/06/23	Crypto exchange 1	Card	£2,850
14	06/06/23	Crypto exchange 1	Card	£2,950
15	06/06/23	Crypto exchange 1	Card	£2,980
16	06/06/23	Company	Transfer	£2,300
17	07/06/23	Crypto exchange 1	Card	£2,990
18	07/06/23	Crypto exchange 1	Card	£2,970
19	07/06/23	Crypto exchange 1	Card	£2,898
20	07/06/23	Crypto exchange 1	Card	£850
21	07/06/23	Crypto exchange 1	Card	£2,550
22	07/06/23	Crypto exchange 1	Card	£3,350
23	08/06/23	Crypto exchange 1	Card	£1,550
24	08/06/23	Crypto exchange 1	Card	£2,850
25	08/06/23	Crypto exchange 1	Card	£2,750
26	08/06/23	Crypto exchange 1	Card	£1,200
27	08/06/23	Crypto exchange 1	Card	£2,020
28	08/06/23	Crypto exchange 1	Card	£3,200
29	08/06/23	Crypto exchange 1	Card	£3,550
30	08/06/23	Crypto exchange 1	Card	£4,950
31	08/06/23	Individual	Transfer	£1,000
32	08/06/23	Individual	Transfer	£1,440
33	08/06/23	Individual	Transfer	£1,500
34	08/06/23	Crypto exchange 1	Card	£1,580
35	09/06/23	Individual	Transfer	£458.48
36	09/06/23	Individual	Transfer	£2,353
37	09/06/23	Individual	Transfer	£165
38	09/06/23	Crypto exchange 1	Card	£2,550
39	09/06/23	Crypto exchange 1	Card	£2,560

40	09/06/23	Crypto exchange 1	Card	£3,550
41	09/06/23	Crypto exchange 1	Card	£2,980
42	09/06/23	Company	Transfer	£969.83
43	09/06/23	Individual	Transfer	£1,416
44	10/06/23	Individual	Transfer	£2,500
45	10/06/23	Individual	Transfer	£1,600
46	11/06/23	Individual	Transfer	£1,402
47	11/06/23	Crypto exchange 1	Card	£2,850
48	11/06/23	Crypto exchange 1	Card	£2,701
49	11/06/23	Crypto exchange 1	Card	£3,750
50	12/06/23	Crypto exchange 1	Card	£3,570
51	12/06/23	Crypto exchange 1	Card	£2,750
52	12/06/23	Individual	Transfer	£1,779
53	12/06/23	Individual	Transfer	£402.32
54	12/06/23	Individual	Transfer	£368.13
55	12/06/23	Crypto exchange 1	Card	£2,575
56	12/06/23	Crypto exchange 1	Card	£3,450
57	12/06/23	Crypto exchange 2	Transfer	£1,800
58	13/06/23	Crypto exchange 1	Card	£2,695
59	13/06/23	Company	Transfer	£3,850
60	13/06/23	Company	Transfer	£3,850
61	13/06/23	Crypto exchange 2	Transfer	£1,000

Mrs P reported what had happened to Revolut on 5 July 2023 via its chat. She says she found Revolut's chat very difficult and asked to speak to someone, but this didn't happen, and she was provided with a link that didn't work. Given the difficulties she faced, Mrs P decided to appoint a professional representative to deal with Revolut on her behalf.

What Revolut says

Revolut didn't agree to reimburse Mrs P. It said that it provided warnings when each new payee was set up, and that its systems detected two payments to newly added payees were suspicious and asked Mrs P the payment purpose. Revolut says it then provided Mrs P with educational stories based on her chosen payment reason. In respect of the payments made by card, Revolut explained it had no chargeback rights. Finally, Revolut said it did what it could to recover the funds Mrs P transferred.

Mrs P was unhappy with Revolut's response and brought a complaint to this service. She said Revolut failed to protect her when the transactions were made.

Revolut told this service that Mrs P first notified it of a scam on 5 July 2023 but didn't respond to information requests, so it wasn't until it received a letter of complaint from her representative on 23 July that it was able to investigate. Revolut also said Mrs P's loss is £114.922.64 as she confirmed a £345 payment on 4 June 2023 wasn't related to the scam (not included in the table above) and £6,917.12 was recovered.

When providing its file Revolut said a significant proportion of fraudulent activity did not take place on Revolut's platform and it acted as an intermediary to receive funds from an external account and pass them on to legitimate external accounts held with various cryptocurrency platforms. Revolut also said the transactions took place over a ten day period which meant Mrs P had time to reflect on what she was being asked to do. And A published a warning on its website about job scams and being impersonated before Mrs P made her first payment. There were also multiple negative reviews in respect of A. Revolut pointed out other red flags, such as the lack of documentation, and said Mrs P didn't complete enough checks before making the payments.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in full. He said that when Mrs P made the first payment she chose 'Safe account transfer' which ought to have led Revolut to ask questions to satisfy itself this payment reason was chosen in error. Had Revolut done so, the investigator thought the scam would have been uncovered and all of Mrs P's loss prevented.

Revolut didn't agree with the investigator's findings, so Mrs P's complaint has been passed to me to decide. I have summarised the main points made by Revolut below:

- Whilst Revolut agrees that the safe account payment reason can be an indicator of potential fraud, it's important to recognise that a safe account transfer does not always mean the payment relates to a scam. Customers often choose this payment reason when transferring funds to another account they hold or inadvertently. For this reason, the payment reason alone should not trigger a human intervention.
- Mrs P was provided with effective and proportionate warnings, including being told that fraudsters may trick her into sending money with the promise of giving more back later.
- Further intervention would not have made a difference to the outcome of this case. It's clear from Mrs P's chats with the scammer that she was discussing Revolut's interventions, which suggests Mrs P would have been guided in how to navigate Revolut's additional security checks. The messages also indicate Mrs P wouldn't have taken any warnings Revolut provided seriously.
- Mrs P's actions have not been adequately addressed. Revolut say it is illogical for a legitimate job opportunity to require someone to pay over £100,000. Mrs P's decision to proceed without completing checks is indicative of a significant level of negligence. Revolut also noted that Mrs P admits she should have completed checks.
- The funds lost in the scam were credited from an account with another bank which held much more information about Mrs P's usual account activity. Revolut isn't able to obtain warnings obtained by other banks, but this service can do so – which may prove effective in this case.

Mrs P said that the £6,917.12 recovered by Revolut was a genuine peer to peer payment for cryptocurrency that should not have been recovered. The seller raised a dispute, and the amount was returned on 29 September 2023. So, Mrs P's claim also includes this amount.

I intended to reach a different outcome to the investigator, so I issued a provisional decision on 17 December 2024. In the 'What I've provisionally decided – and why' section of my provisional decision I said:

"I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

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 the consumer 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 the consumer and the Payment Services Regulations to carry out their 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 Revolut should in June 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.

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 June 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.

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

[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_/

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).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[3] 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 June 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and

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

[3] 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.

- 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 June 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mrs P has fallen victim to a cruel scam here, nor that she authorised the payments she made to her cryptocurrency wallet and to third parties to buy cryptocurrency via the peer to peer method (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in this decision the circumstances which led Mrs P to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mrs P might be the victim of a scam.

Many of the transactions Mrs P has asked me to consider were card payments to an identifiable cryptocurrency exchange. I am satisfied that by the end of 2022, prior to the payments Mrs P made in June 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.

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.

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 Mrs P might be at a heightened risk of fraud.

Mrs P opened he account with Revolut on 3 June 2023, the day she started to make payments related to the scam. When opening the account, Mrs P said it would be used for various purposes including transfers and cryptocurrency. So, when Mrs P started to make payments, Revolut had no information about her usual account activity.

The initial two transactions Mrs P made were to a cryptocurrency provider. These were low value card payments (£200 and £250) so wouldn't have caused Revolut to be concerned. Mrs P then made a transfer to an individual (transaction three). Whilst this transaction was also very low in value, and not one I'd usually expect Revolut to recognise as higher risk, Mrs P chose the payment reason safe account transfer. This payment reason can only apply if a customer is falling victim to a safe account scam or has chosen an incorrect payment purpose, so I think Revolut needed to satisfy itself Mrs P chose this payment reason in error. It could have done this by directing her to the chat.

Mrs P then made a series of low value transactions to individuals and a cryptocurrency exchange. Although the volume of transactions increased, they weren't at a level where I'd expect Revolut to take any additional steps. The payments ranged from £89 to £1,550 and were made over a three day period. And, as I've said above, the account was new, so Revolut didn't have a clear picture of Mrs P's normal account activity.

When Mrs P made payment twelve, I consider Revolut ought to have recognised that it carried a heightened risk and taken additional steps before processing it. This was because Mrs P had made a series of payments to a cryptocurrency exchange and the transactions were increasing in value. Given what I have said above, I consider Revolut needed to warn Mrs P of the increased risks associated with cryptocurrency payments. I think a proportionate response would have been to provide a written warning tailored to cryptocurrency investment scams (which I will discuss below).

As Mrs P continued to make multiple payments in quick succession to an identifiable cryptocurrency exchange, I think Revolut ought reasonably to have recognised a significant risk of harm and intervened again. I think this intervention should have taken place when Mrs P made payment 22. This was the ninth payment to an identifiable cryptocurrency exchange since the last intervention point and there was a pattern of increasing payments.

What did Revolut do to warn Mrs P?

Revolut says that each time a new payee was set up it provided Mrs P with a new payee warning that said:

"*Do you know and trust this payee?*

If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."

This warning was provided for payments 1, 3, 4, 5, 6. 7, 8, 9, 17, 31, 32, 35, 36, 37, 42, 43, 46, 52, 53, 54 and 59.

Revolut moved two transfers to pending – transaction three, and transaction 54 on 12 June 2023. When asked the payment purpose for these two transactions Mrs P chose safe account transfer for the first and something else for the later payment. Mrs P was then provided with a warning tailored to the payment reason chosen and was given the opportunity to get advice.

Revolut says its automated security system also identified nine payments as suspicious (transactions 9, 17, 31, 33, 52, 57,59, 60 and 61). All nine of these payments were bank transfers to individuals or companies. In respect of these transactions, Revolut provided educational stories which warned that victims lose millions of pounds a year to bank transfer scams and that fraudsters are professionals. Revolut then asked Mrs P to provide a reason for the payments. Mrs P chose goods and services in respect of all but one of the payments, when she chose something else (payment 9). Revolut say Mrs P was then provided with warnings tailored to the payment reason chosen.

In addition to the above, Revolut says that on 5 June 2023, two days after the account was opened, its systems flagged risks of inbound APP fraud which resulted in a manual account review and a request to Mrs P to verify the source of funds. A further source of funds review was completed on 12 June 2023. On both occasions Revolut say the account was cleared.

What kind of warning should Revolut have provided?

As I have said above, I don't think Revolut should have processed Mrs P's £300 payment request (transaction three) when she chose payment to a safe account as the payment purpose until it had taken appropriate steps to satisfy itself that Mrs P chose an incorrect payment reason. It could have done this by directing Mrs P to its in app chat to discuss the payment further or by calling Mrs P (after completing its usual verification).

When Mrs P attempted to make payment twelve, I think Revolut ought fairly and reasonably to have recognised there was a heightened possibility that the transaction was linked to a scam. In line with the good industry practice that I've set out above, I think a proportionate response to that risk would have been for Revolut to have provided a written warning tailored to cryptocurrency investment scams. The warnings Mrs P received up to this point weren't proportionate to the risk presented by payment twelve. The new payee warning was too general and lacked sufficient context to have been impactful and the warnings provided following educational messages weren't related to cryptocurrency.

I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mrs P by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

By payment 22 I think a proportionate response to the risk presented would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs P's account. I think it should have done this by, for example, directing Mrs P to its in-app chat to discuss the payment further rather than providing an on-screen warning.

If Revolut had provided a warning of the type described, would that have prevented the losses Mrs P suffered?

I'm not persuaded that intervention by Revolut when Mrs P made the £300 payment to an individual on 3 June 2023 would have made a difference. The intervention needed to be proportionate to the risk identified. In this case other risk factors which might indicate a safe account scam was in progress, like a confirmation of payee no match and a whole balance being moved from the account, weren't present. Mrs P had also just made two card payments to a cryptocurrency exchange. These payments aren't consistent with a safe account scam. In the circumstances, I consider Revolut should have taken steps to identify what the payment was for and warned Mrs P that if she had received unexpected contact from a third party telling her she needed to move money to protect it, she was being scammed.

After carefully considering the messages Mrs P exchanged with the scammer, I don't consider that intervention by Revolut of the type I have described above would have made a difference. Mrs P was following the advice of the scammer. In messages very soon after this transfer was made, Mrs P discussed transferring funds to her Revolut account. The scammer told Mrs P to say that she was transferring funds to her own account for future use and went on to say if she was asked anything she was unfamiliar with she should tell the scammer. The scammer was clear in multiple messages that Mrs P should not mention cryptocurrency.

I'm also not persuaded that a written warning covering the essential features of a cryptocurrency investment scam would have made a difference in the circumstances of this case. Mrs P wasn't investing. Instead, she was making payments in respect of a job. In the messages Mrs P and the scammer exchanged the scammer said on a number of occasions that Mrs P isn't trading or investing. So I don't believe that a warning about investment scams would have resonated with Mrs P or resulted in her not making further payments. Revolut's educational stories which were general in nature hadn't resonated with Mrs P.

When Mrs P made payment 22, I have said Revolut should have asked her questions about the payment she was making, so I've thought about what would most likely have happened if it had. By this stage Mrs P was paying a cryptocurrency exchange. If she'd have said she was making the payment for anything other than cryptocurrency, Revolut would have known Mrs P wasn't being open and should have probed further.

If Mrs P had said she was buying cryptocurrency I think Revolut should have asked her why she was buying it and where she was sending it to. At the same time, Revolut should have provided some context and discussed common scam scenarios related to cryptocurrency, including the involvement of a third party who tells a victim what to do or to lie to their bank/EMI.

As I've said above, the scammer was clear that Mrs P wasn't investing, and I'm not persuaded Mrs P would have been able to provide a plausible explanation for why she was buying cryptocurrency. I've not seen any discussions in any of the chats Mrs P has provided which discuss how to explain cryptocurrency trading. I think Mrs P would have struggled to explain why she had bought so much cryptocurrency.

Also, by the time Mrs P made transaction 22, she was concerned about the amount of money she'd been asked to provide and how she would find it. It's clear she was stressed, and she said she wasn't able to focus at work. Shortly after, Mrs P says in the chat with the scammer that she was trying to persuade her sister to join the scheme but was now re-evaluating the whole thing. I think that Mrs P would ultimately have told Revolut what she was really doing and Revolut would have recognised that she was likely falling victim to a scam.

Overall, I think that appropriate intervention by Revolut would have given the perspective Mrs P needed and reinforced her own developing concerns. As a result, I consider she would more likely than not have concluded that the scheme was not genuine and decided not to go ahead with any further payments.

Ultimately, as Revolut didn't question the payment Mrs P made, it can provide no compelling evidence that she would have misled it about the purpose of it or the surrounding circumstances if it had effectively intervened when I think it should have.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut wasn't the original source of the funds for the money Mrs P lost to the scam. Mrs P had moved the money from another bank (which didn't intervene) to her Revolut account, before sending the funds on to a cryptocurrency wallet.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs P might have been at risk of financial harm from fraud when she made payment 22, 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 further losses Mrs P suffered.

The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mrs P's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs P'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 Mrs P has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mrs P could instead, or in addition, have sought to complain against those firms. But Mrs P has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

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

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mrs P's loss from payment 22 (subject to a deduction for Mrs P's own contribution which I will consider below).

I'm also aware that the Payment Service Regulator's ("PSR") mandatory reimbursement scheme does not require Revolut to reimburse Mrs P.

The PSR's mandatory reimbursement scheme is not relevant to my decision about what is fair and reasonable in this complaint. But I do not consider the fact that the PSR has not made it compulsory for payment service providers to reimburse consumers who transfer money to an account in their own name as part of a multi-stage fraud, means that Revolut should not compensate Mrs P in circumstances when it failed to act fairly and reasonably, as I have found was the case here.

I do not consider it to be relevant that the circumstances here do not fall under the specific definition of an APP scam set out in the CRM Code and DISP rules. Those definitions define the scope of the CRM Code and eligibility of payers to complain about a payee's PSP respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made payment two without asking Mrs P questions to understand the reason for the payment or providing any warnings. So, I'm satisfied Revolut should fairly and reasonably have made further enquiries before processing any further payments. If it had, it is more likely than not that the scam would have been exposed and Mrs P would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mrs P's loss.

Should Mrs P bear any responsibility for her loss?

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.

I recognise that there were relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent earnings and tasks. I note that Mrs P was also part of an instant messaging group with other people who shared positive stories. I can imagine this would have given some validation to the scheme.

But on balance, I think a 50% deduction (from payment 22) is fair and reasonable in all the circumstances of this case. The nature of the job was unusual, and I think this ought to have led Mrs P to ask questions, complete some additional research and to look at reviews. Mrs P was told that she would earn a significant amount of money for work that does not appear to be particularly time-consuming or arduous. And buying and transferring cryptocurrency to be paid is very unusual.

I note that when Mrs P started to believe she might be the victim of a scam she said she should have checked for online reviews and references and asked the scammer for A's business address. So, it's clear Mrs P didn't complete any research before agreeing to send money. And, as I said above, there was a scam warning on the site of the company A was impersonating.

I also consider that at the point at which I have said Revolut needed to do more Mrs P had concerns about the amount of money she was being asked to pay. By this point I think Mrs P should have realised that the dynamic of being asked to pay money before she could get her commission would go on indefinitely.

Overall, I consider it fair to reduce the amount Revolut pays Mrs P to reflect the role she played in what happened."

Responses to my provisional decision

Mrs P let me know that she accepts my provisional decision.

Revolut responded and said it had nothing further to add to the comments already made.

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.

As neither party has raised any new evidence or arguments for me to consider my final decision is the same as my provisional decision. I have set out my full reasoning above.

In summary, I consider that Revolut ought to have satisfied itself that Mrs P chose the payment to a safe account payment reason in error. It should also have recognised a heightened risk and provided a warning tailored to cryptocurrency investment scams when she made transaction 12. But I don't think these actions would have made a difference and resulted in the payments not being made.

When Mrs P made transaction 22, I consider Revolut should have recognised a significant risk of financial harm and asked Mrs P questions about it. Given the concerns Mrs P had at the time and the difficulty she would have had in explaining why she was buying so much cryptocurrency, I consider the scam would have been uncovered at this point and Mrs P's further loss prevented.

I think it is fair to split liability from transaction 22 onwards between Mrs P and Revolut. I say this for a number of reasons including the unusual nature of the job, the fact Mrs P didn't complete any research, and because she had concerns but continued to make payments.

My final decision

I uphold this complaint and require Revolut Ltd to:

- Reimburse 50% of all payments from (and including) payment 22; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of each transaction to the date of settlement.

If Revolut Ltd is legally required to deduct tax from the interest it should send Mrs P a tax deduction certificate so she can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs P to accept or reject my decision before 5 February 2025.

Jay Hadfield
Ombudsman