DRN-4454388

The complaint

Mr G complains Revolut Ltd won't refund the money he lost as a result of a job scam.

Mr G has used a professional representative to bring this complaint to our service and they have made submissions on his behalf. For consistency, I'll refer to Mr G throughout.

What happened

After sharing his CV online, Mr G received a text message in or around May 2023 about a job opportunity, from who he thought was a recruitment agency (that I'll call C). Unbeknown to Mr G, he was speaking to a fraudster.

The fraudster told Mr G about a remote working opportunity with an advertising company (that I'll call ADM). Mr G then was contacted on a social media messenger service by a representative of ADM. They explained the job involved advertising products to boost sales for merchants. Mr G had to boost at least 40 to hit his target and earn commission from the sales. He'd also be able to buy additional data to boost his earnings. Mr G says he looked into ADM online and found their website to be impressive and detailed. What he didn't know at the time was the fraudster had cloned the branding and logo of a genuine company.

The fraudster instructed Mr G on how to open an account via the ADM website. The evidence shows Mr G was in regular contact with his 'mentor', and he had access to an online portal. The account he opened was pre-funded by ADM which Mr G used to boost his first set of 40 tasks. Over 24 hours, Mr G saw his commission continuously increase on the account. Once he'd utilised the balance, he was told he needed to add more funds to start the second set. Mr G was reluctant to put more of his own funds into the platform, saying 'I knew this won't make money'. The fraudster persuaded him that he wasn't paying any fees for the job and that by depositing funds, he'd clear the negative balance, complete the tasks and get his money back. As he said he wasn't willing to put his own money into it, the fraudster offered to deposit 100 USDT for him as a loan, which Mr G accepted. Again, his balance went into negative, but this time he made a payment of £102 from another bank account. This was a peer to peer cryptocurrency payment.

Mr G was able to make two withdrawals on 19 June 2023 for £15.05 and £287.65. So, he proceeded to make 3 payments between 19 June 2023 and 20 June 2023. The payments were used to purchase cryptocurrency from individual sellers on a cryptocurrency exchange (that I'll call B), which Mr G received. And this was sent to a digital wallet ID provided by the fraudster.

Mr G was unable to make a withdrawal from his account until he completed further tasks and purchased more data. Therefore, he made five further payments between 21 June 2023 and 22 June 2023 to access his returns. The items on the site grew increasingly more expensive and each time he tried to access his funds he was asked for more money. After the fraudster asked for £19,000 to access his funds, Mr G refused. The fraudster encouraged Mr G to take out loans, but Mr G wasn't prepared to do this, and couldn't afford the £19,000. He realised he'd been scammed as the fraudster continued to make various excuses as to why he couldn't withdraw his funds from the account without paying more.

All in all, Mr G was tricked into making 8 transactions from his Revolut account, totalling £6,616 to 6 different payees. These were all peer to peer cryptocurrency payments. These transactions can be seen in the table below:

No#	Date & Time	Transaction	Amount
	19/6/2023 14:45	*Credit from B*	*+£15.05*
	19/6/2023 14:47	*Credit from C*	*+£287.65*
1	19/6/2023 16:32	Payee 1	£100
2	20/6/2023 11:58	Payee 2	£30
3	20/6/2023 12:44	Payee 3	£515
4	21/6/2023 11:21	Payee 4	£300
5	21/6/2023 12:25	Payee 5	£1,900
6	21/6/202314:57	Payee 5	£1,671
7	21/6/2023 16:38	Payee 5	£2,000
8	22/6/2023 17:34	Payee 6	£100
	1/8/2023	*Recovered funds*	*+£300*
		Total loss	**£6,013.30**

**I note in the investigator's view, a £700 payment debited on 22 June 2023 was included in the table of disputed payments. Mr G has since clarified this was a payment to a friend and was included in error. I've therefore discounted this payment from his claim and any redress.*

Mr G reported the scam to Revolut on 26 June 2023. On 1 August 2023, Revolut recovered £300 from one of the accounts Mr G sent his funds to (payment 4). No funds remained in the other accounts he paid.

Revolut says it gave Mr G a warning (which I'll come on to talk about later in the decision) when he set up each of the 6 payees. Mr G selected 'Goods and services' as the payment purpose for payment 3 and in response to this, Revolut presented a scam warning. For payments 4-7, he chose 'Transfer to a 'safe account'' as the payment purpose and again, he was shown a scam warning. Mr G was given the option to get advice from an agent, or cancel the payment, but he chose to proceed. Revolut said Mr G spent 18 seconds between generating the warning and proceeding with the payment, suggesting he didn't pay attention to the warnings, nor did he complete any further due diligence. Revolut says this presents a strong element of contributory negligence. It also noted it emailed Mr G on 19 May 2023, with information about investment scams.

Revolut denied all liability. It said it was not at fault for processing the payments Mr G authorised. And it set out in its terms and conditions that it's not liable for financial losses of a third party deal.

Unhappy with this outcome, Mr G referred his complaint to our service.

Revolut maintained its defence, adding the following points:

- Mr G was participating in an activity which isn't a normal or legitimate type of employment, and the job might be considered a scam itself.
- He received a job opportunity through social media messenger, which isn't common.

- He sent fraudsters a considerable amount of money, in advance, without being able to withdraw higher amounts. For an employee it would be reasonable to expect to receive money from their employer and not the other way around.
- The fraudster told Mr G he'd make £1,000 a week to provide evaluation over some products. And he was told another employee made £1,000 from just 45 minutes' worth of work. This was too good to be true and should have been considered a red flag.
- The payments were neither high value nor did they follow a fraud pattern. So, it didn't intervene by contacting Mr G directly.

Our Investigator upheld Mr G's complaint in part. They thought Revolut ought to have prevented Mr G's loss from payment 4 by making some basic enquiries. They also thought Mr G should accept partial liability by way of contributory negligence. They recommended a refund of 50% of Mr G's loss from payment 4, less the sum recovered, with 8% simple interest on this amount from the date of debit to settlement.

Mr G accepted this outcome, but Revolut did not. It made a number of arguments in its defence, which I've summarised below:

- Mr G selected 'Transfer to a 'safe account'' when he was sending money to third party accounts which he had no control over.
- The final payments went to a legitimate cryptocurrency platform and there were no solid grounds for Revolut to suspect those transactions were being made under fraudulent scenarios.
- Revolut is bound by contract, applicable regulations, and the common law to execute valid payment instructions. The duty is strict and is subject to only very limited exceptions (for example if the customer has asked Revolut to act unlawfully).
- The Payment Services Regulations 2017 (PSR 2017) impose obligations on the PSP to execute authorised payments promptly. And in accordance with the personal terms, Revolut agrees to execute transfers in accordance with the customer's instructions. There was no uncertainty as to the validity of Mr G's instructions and any delay by Revolut to execute these instructions would have amounted to a breach of its duty to Mr G.
- FOS have overstated Revolut's duty to its customers, and errors in law, by stating that Revolut should have "taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud".
- Revolut recognises its obligations to put in place adequate procedures to counter the risk that it may be used to further financial crime (and has such systems and controls in place). But that duty does not go as far as to require Revolut to ask detailed questions of Mr G about the context and purpose of the transactions, particularly in the face of authorised customer instructions, and in circumstances where the transactions were being made to an account in his own name at a legitimate cryptocurrency exchange.
- It has no legal duty to prevent and detect all fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25.
- Our service appears to be treating Revolut as if it were a signatory to the Contingent Reimbursement Model (CRM) Code. But Revolut is not a signatory to the Code and

therefore its rules do not apply. The Payment Service Regulator's ("PSR") mandatory reimbursement scheme rules are not yet in force and so should not be applied either.

- Revolut has adequate systems and controls in place to detect unusual or suspicious transactions, but Revolut did not have any reason to believe that Mr G might be at risk of financial harm.
- 7 general warnings were provided to ask if Mr G was sure about who the payees were. Adding to this, 6 tailored warnings were shown to him as well, having a total of 13 warnings that could raise some suspicious thoughts on Mr G's behalf. Mr G chose to continue with the transactions, and therefore it is clear that even if Revolut intervened directly and ask more questions, Mr G would still have told Revolut that he would like to proceed with the disputed transactions.

As no agreement could be reached, this case was passed to me for a decision to be issued.

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.

In doing so, 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 Mr G 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*".

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

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in June 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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;[2]
- 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, 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)[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".*

---

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

[2] 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_/

[3] 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.

- 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[4], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

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
- 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.

Should Revolut have recognised that Mr G was at risk of financial harm from fraud?

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

I've reviewed Mr G's account statements since the account was opened on 8 February 2022. These show me that the account wasn't used frequently by Mr G, especially in the months leading up to the scam. The transactions he did make were mostly card payments, with some transfers in and out of the account, and some ATM withdrawals.

The first three disputed transactions were low in value, made on different days and went to different beneficiaries. There was no clear link between these payments, so I'm not persuaded a pattern began to emerge. Revolut sought to establish the reason for payment 3 and Mr G said it was for 'Goods and services'. So Revolut gave an online warning about purchase scams. I wouldn't have expected Revolut to have taken further action up to this point.

However, like our Investigator, I'm persuaded Revolut ought to have identified Mr G was at risk of financial harm from fraud when he made payment 4. Mr G chose a payment purpose which was indicative of fraudulent activity – that being 'Transfer to a 'safe account''. There are very few, if any, legitimate scenarios when a consumer might be moving money to a 'safe account'. And this payment purpose intends to identify customers falling victim to a safe account scam. So, Revolut ought to have taken steps to establish that Mr G had chosen this in error and wasn't at risk of a safe account scam.

What did Revolut do to warn Mr G?

Revolut says it showed Mr G the following warning when he set up each of the 6 payees:

> *"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."*

For the reasons I've explained, Revolut acted proportionately in response to payments 1-3. It provided some general advice about knowing and trusting the payee. And when Mr G selected 'Goods and services' for payment 3, it presented a warning about purchase scams. Overall, I'm satisfied that these warnings were proportionate to the risk associated with payments 1-3.

Revolut also says it sent Mr G some information about investment scams via email, although I note Mr G's claim concerns a 'job scam'. In any event, such advice was not given at the time Mr G made the payments and so could not fairly or reasonably be considered as a timely or impactful warning.

When Mr G selected 'Transfer to a 'safe account'' for payment 4, Revolut showed Mr G some warning screens which warned him against fraudsters pretending to be from Revolut or other financial institutions, telling customers to move money to a 'safe account' due to a problem with your account. He was also warned against number spoofing and was told how to verify a call from Revolut. Mr G was given the option to read some scam guidance, get advice, cancel the payment or proceed with it. He chose to proceed.

I appreciate that Revolut gave Mr G some advice about safe account scams, because this was the scam risk identified through the payment purpose given by Mr G. However, for the reasons I've explained, Revolut ought to have done more than just show Mr G some information about this type of scam, given the payment purpose he selected indicated that Mr G was more likely than not at risk of being defrauded.

What kind of warning should Revolut have provided?

Whilst I appreciate Revolut took some steps to warn Mr G against proceeding with the payment, the warning required no real engagement or interaction from Mr G. Given the information Revolut had at the time suggested Mr G was at risk of a safe account scam, it ought to have taken steps to establish the circumstances surrounding the payment before allowing it to debit Mr G's account. I think it should have done this by, for example, directing Mr G to its in-app chat to discuss the payment further.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr G suffered from payment 4?

I've thought carefully about whether Mr G would have revealed the true reason for the payments, had Revolut made further enquiries about payment 4. It's true that Mr G didn't select the most accurate payment purposes when asked to do so by Revolut. Mr G says the fraudster told him what payment purposes to select, and he didn't think this was suspicious. But Mr G also says the fraudster didn't specifically tell him to hide the reason from Revolut. Having considered the list of payment purposes Revolut presented Mr G, a more appropriate option would have been 'Cryptocurrency', given these were peer to peer cryptocurrency payments. But I am mindful that the true purpose for the payment was for a job opportunity and there was no payment purpose specific to 'job scams' in place at the time.

Revolut has said that as Mr G only spent 18 seconds on the warning message this suggests he didn't pay attention to it or complete further due diligence before proceeding. Mr G says he recalls seeing Revolut's warnings, but as these were generic, he proceeded with the payments. I've carefully considered whether Mr G would have paid attention had Revolut made further enquiries about the payment he was making. I'm mindful that an in-app chat intervention is a far less common occurrence than an online warning. And this would require a greater amount of engagement from Mr G, in order to be able to proceed with the payment. So I'm satisfied he would have engaged with further enquiries from Revolut.

I'd expect Revolut to have asked Mr G further questions to ensure he wasn't falling victim to a safe account scam, as indicated by the payment purpose he selected. So it ought to have asked further questions of Mr G to establish the context around the payment he was making. The evidence I've seen shows Mr G was aware that he was buying cryptocurrency when making these payments. For example, it's clear in the correspondence between him and the fraudster that he was being instructed to buy cryptocurrency, and he was also operating his own account with B – a well-known cryptocurrency exchange. So, I accept Mr G might have told Revolut he was purchasing cryptocurrency. However, I don't think this ought to have satisfied Revolut that Mr G wasn't at risk of financial harm.

Had Revolut asked Mr G further questions around why he was purchasing cryptocurrency, I think Mr G's answers would have been an immediate red flag to Revolut. He was buying the cryptocurrency so that he could complete tasks for a job opportunity, and he was being guided by his 'mentor'. Had further questions been asked about the job opportunity, this would have highlighted that;

- he'd been contacted out of the blue via a social media messenger service
- he was being told to use his own money to gain employment
- he'd been instructed to open an account with a cryptocurrency exchange to facilitate 'tasks'
- he was making a payment in order to access his 'returns'

Given these circumstances, I'm satisfied that Revolut ought to have identified that the job opportunity Mr G was involved in was highly unusual and implausible, and it should have been concerned that he was at risk of being scammed.

I'm mindful that in the messages between Mr G and the fraudster, I can see he did have continuous doubts about what he was being asked to do. As previously mentioned, he was reluctant to put his own money into the platform. And in other messages he can be seen saying *'I hope I won't loose [sic] my money'* which suggests to me he didn't fully trust in the process. Given the clear doubts Mr G had about the scam up to this point, I do believe that a warning from Revolut that he was likely falling victim to a scam, would have resonated with him. And had Mr G been warned that if he proceeded, it would be highly likely he'd lose his funds, I don't believe he would have proceeded to make further payments. Afterall, he engaged with the job opportunity to improve his financial standing, not to make it worse. So I'm persuaded Revolut could have prevented further loss from and including payment 4.

Is it fair and reasonable for Revolut to be held responsible for Mr G's loss?

I've taken into account that Mr G received cryptocurrency in receipt of the payments made to the beneficiaries, and sent this on to a fraudster, rather than paying the fraudster directly from Revolut.

But as I've set out above, I think that Revolut still should have recognised that Mr G might have been at risk of financial harm from fraud when he made payment 4, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mr G suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred out of Revolut, does not alter that fact and I think Revolut can fairly be held responsible for Mr G'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 Mr G 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 Mr G could instead, or in addition, have sought to complain against those firms. But Mr G has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut. I'm also not persuaded it would be fair to reduce Mr G'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 Mr G's loss from payment 4 (subject to a deduction for Mr G's own contribution which I will consider below).

Revolut has also argued that we are applying the provisions of the CRM Code to complaints against it, despite it not being a signatory and in circumstances where the CRM Code would not, in any case, apply. I do not seek to treat Revolut as if it were a signatory to the CRM Code. I've explained in some detail the basis on which I think, fairly and reasonably, Revolut ought to have identified that Mr G may have been at risk of financial harm from fraud and the steps it should have taken before allowing the final payment to leave Mr G's account.

I also acknowledge the PSR's proposed mandatory reimbursement scheme for authorised push payments would not require Revolut to reimburse Mr G in relation to these payments.

However, the PSR's proposals are not yet in force and are not relevant to my decision about what is fair and reasonable in this complaint, and in any event will not apply to peer 2 peer cryptocurrency purchases.

Should Mr G bear any responsibility for his losses?

Mr G has accepted our Investigator's findings that he should share responsibility for his loss. I am in agreement with this point, and largely for the same reasons as our Investigator.

Mr G had clear doubts throughout his messages with the fraudster, as I've previously mentioned. Mr G says he was contacted by another member of the 'group chat' he was in, and they assured him they had received withdrawals. But given the clear concerns Mr G had, and the implausible nature of the job opportunity, I don't think Mr G acted reasonably in taking the word of someone he didn't know, nor had any reason to trust.

And I think he ought to have had serious concerns when he was being continuously asked to make more payments, of increasing size, without being able to access the 'commission' he'd made. Whilst I do appreciate there were some more persuasive elements of the scam, such as online training and access to a platform to complete tasks, I find that the causes for concern far outweigh these. And whilst it seems ADM cloned a legitimate marketing agency, I think it was highly unusual for him to have been contacted about this job by text message, with no interview process, no paperwork, and a salary paid in cryptocurrency. This all ought to have prompted a more cautious approach from Mr G. Overall, I think it's fair that Mr G accept partial responsibility for his loss.

I've also considered Revolut's argument that the job Mr G was agreeing to complete could be seen as a scam itself. I'm mindful that this was positioned to Mr G as a marketing role, as is incredibly common with this type of scam. I'm satisfied that he is an unwitting victim of a scam here, and I have no reason to believe Mr G thought he was doing something untoward in accepting this 'job offer'.

Recovery of funds

I'm not persuaded that there was any reasonable prospect of Revolut being able to successfully recover Mr G's funds once he reported the scam. I say this because Mr G used the funds sent from his Revolut account to individual sellers on B's platform, to purchase cryptocurrency, which he received and sent on to the fraudster. So Revolut was unable to recover this.

Putting things right

For the reasons I've explained, I've reached the same conclusions as our Investigator that Revolut can fairly and reasonably be held liable for 50% of Mr G's loss from and including payment 4, less the £300* it recovered. Therefore, Revolut should refund £2,835.50.
My calculations are below:

£300 + £1,900 + £1,671 + £2,000 + £100 = £5,971
£5,971 - £300 (recovered funds) = £5,671*
£5,671 x 50% = £2,835.50

I am aware that Mr G did fund the disputed payments through funds borrowed from friends. Some of these payments credited his Revolut account, and some credited his accounts with other banks. Mr G has also paid the majority of these funds back. However, I am satisfied that Mr G has suffered a loss and so I think it's fair for Revolut to pay 8% simple interest per year, on the amount I will be asking it to refund, less any tax lawfully deductible.

My final decision

For the reasons I've explained, my final decision is that I partially uphold this complaint about Revolut Ltd. It should now put things right by:

- Refunding £2,835.50
- Paying 8% simple interest per year on the refund, from the date the payments debited Mr G's account, until the date the refund is paid (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 11 October 2024.

Meghan Gilligan
Ombudsman