DRN-5092834

The complaint

Ms P complains that The Royal Bank of Scotland Plc (RBS) won't refund money she lost when she was the victim of a scam.

Ms P is represented by a firm I'll refer to as 'R'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In 2023 Ms P fell victim to a task-based job scam. She was contacted on an instant messenger application by an unknown person that claimed to work for a recruitment firm – who asked Ms P if they could share her details with an employer to receive detailed information on the job opportunity. Ms P agreed.

Ms P was then contacted by a firm – which we now know to be a scam – that I'll refer to as 'B'. B explained to Ms P that the job entailed increasing the exposure and visibility of products. And to do this, Ms P was required to complete tasks on B's platform that would generate positive ratings for the products. Ms P was told she would need to complete sets of 40 tasks and that it would take 45 to 60 minutes per day. For this, she would receive a commission of *"at least £80-100 or more"* plus a weekly salary of £700 (which would increase after the first week when she became a permanent employee).

As part of the job though, there were 'bonus missions' randomly generated that provided three times the commission. This required funds to be deposited to bring Ms P's account out of a negative balance. Ms P was assured these funds would be returned once the tasks were completed – along with her commission earnings. Ms P received a link to B's platform for her to set up an account. B then provided instructions to Ms P on how she could complete the sets – which included funding the account to complete the 'bonus missions' by purchasing crypto. Ms P went on to make the following payments from her RBS account to one of her other banking providers (that I'll refer to as 'L'), whereby the funds were sent to the scam via a legitimate crypto provider:

Date	**Type**	**Amount**
19 February 2023	Faster payment	£20
23 February 2023	Faster payment	£5,000
23 February 2023	Faster payment	£5,000
28 February 2023	Faster payment	£15,000
	Total	**£25,020**

To fund the scam, Ms P took out three loans – two of which, totalling £25,000 and taken out with other firms, were paid in to her RBS account to fund the above payments. The third loan, for £15,000, was taken out with L.

Ms P realised she'd been scammed when she was unable to withdraw her funds.

R complained on Ms P's behalf to RBS on 22 March 2024 saying the payments were made as part of a scam. In short, they said:

- The account activity was out of character and had RBS intervened in line with industry standards, the scam would've been exposed thereby preventing any further financial loss.
- Ms P should be refunded under the Contingent Reimbursement Model (CRM) code.
- It is understandable why Ms P felt this job opportunity was real and believable – as she reviewed B's website which appeared professional, she didn't find anything negative from an internet search, and she was also able to start with small payments and make withdrawals. Furthermore, Ms P was added to an instant messenger group with other freelancers sharing success and received professional onboarding.
- The scammers were in constant contact with Ms P, and she was unfamiliar with working from home and this type of work offered. And the contact first came from a 'recruiter'.
- RBS should be on the lookout for this type of scam to prevent their customers from foreseeable harm.
- If RBS had intervened by asking open probing questions, the scam would've been exposed, and the spell of the scammer would've been broken.
- RBS should refund Ms P and pay 8% simple interest.

RBS didn't uphold the complaint. In short, they said:

- The funds were sent directly to one of Ms P's own accounts elsewhere. As such, no loss occurred as a result of RBS following Ms P's payment instructions.
- The payments weren't covered by the CRM code.
- Every transaction receives a risk score that is made up of various factors. Here, the activity didn't receive a high enough score to trigger a restriction.
- Ms P should raise her concerns with the other firm (L).
- Ms P didn't do enough due diligence before parting with the funds.

The complaint was referred to the Financial Ombudsman. Our Investigator didn't think RBS were responsible for Ms P's losses. She thought RBS should've spoken with Ms P before processing the third and fourth payments. But taking into consideration Ms P's interactions with her other payment service providers (PSPs) – L and an EMI provider (that I'll refer to as 'E') – she didn't think this would've made a difference. This was because our Investigator didn't think Ms P answered their questions accurately. And even when L restricted a crypto payment and directed Ms P to branch for additional fraud prevention checks, she

circumvented the payment restriction by forwarding funds to E. Furthermore, our Investigator noted that Ms P had been told by B to lie about the purpose of the loans she applied for and to not reveal details about them to her bank(s).

R disagreed and, in short, they said:

- RBS should've intervened and spoken with Ms P before processing the first £5,000 payment.

- The interventions undertaken by L were insufficient and inappropriate given the risk of fraud as:

    - The questioning was generic and close-ended. At no point did Ms P state she was investing but this was assumed by L. And Ms P answered their questions honestly and to the best of her ability.

    - Questions were phrased poorly – merging multiple questions that are likely to result in different answers in the same sentence and often make the questions overly specific.

    - L's agents focused on the security of Ms P's crypto wallet, whether there was a third-party investment broker involved, if she'd been forced to make the payments and if she had to pay any withdrawal fees. These however didn't apply to her circumstances.

    - It's evident in the last call (of four) between Ms P and L, when she was referred to branch, that she had very little understanding of crypto. And she told them that she wasn't investing and had no plans to invest – which was true, as she believed she was making the payments for a job/task.

    - If Ms P had even been presented with a tailored warning relevant to crypto investment scams, this would've potentially uncovered the scam as there are similarities – such as being approached through social media and being pressured to make payments to capitalise on opportunities presented. Instead, Ms P was given a generic crypto warning explaining that the Financial Conduct Authority (FCA) has warned of its risk and that people should be prepared to lose money as a result.

- In respect of the intervention(s) undertaken by E:

    - The payment purposes she gave for transactions – 'something else' and 'investment' – were appropriate answers.

    - 'something else' as a payment purpose should also be subject to an even higher level of scrutiny. Yet E only gave a generic online warning which was wholly unsuitable.

    - Ms P wasn't provided an effective warning to allow her to understand the fraud risk.

- The payments were made in 2023 when job/task scams were very prevalent, and banks should've been aware of such scams – and provided tailored warnings and/or questioning regarding them specifically.

- They didn't think our Investigator's conclusion that Ms P *"made it hard for both*

businesses to understand the true circumstances surrounding the payments and provide a truly tailored warning" was fair. Ms P answered all questions to the best of her ability given the poor nature of L's questioning, which revolved purely around her being a victim of an investment scam despite her never stating she was investing.

- No coaching took place at the time of the first two calls with L (on 23 February and 1 March 2023), meaning that all further questions would've been answered honestly with the scam being uncovered.

- Had RBS intervened:

    - Ms P wouldn't have said she was making the payments for investment purposes.

    - Even if she did, RBS should've quickly realised based on Ms P's answers to further questioning that this wasn't a simple investment. And a proper intervention would've involved some adaption in response, not just an agent reading from a script.

    - Despite poor questioning from L, it still led to her account being blocked. And so, it's reasonable to conclude that RBS would've been equally suspicious and prevented payments from being made – with a better intervention uncovering the scam.

    - As Ms P hadn't been coached to lie at the time of the RBS payments, she would've answered questions honestly – which would've involved disclosing the payments being made for an employment opportunity and further questioning uncovering the hallmarks a job/task scam.

    - Ms P wouldn't have made the payments had she been presented with a proper warning or education about this type of scam.

The complaint has been passed to me to decide.

What I've decided – and why

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

I'm sorry Ms P has lost a significant amount of money and I don't underestimate the impact this has had on her. But while I know this won't be the outcome she is hoping for, I don't think RBS has acted unfairly by not refunding her loss for similar reasons to our Investigator. I'll explain why.

Before I do, I want to reassure Ms P that I've considered everything R has submitted on her behalf. And so, while I've summarised this complaint in far less detail than what has been provided, I want to stress that no discourtesy is intended by this. If there is a submission I've not addressed; it isn't because I have ignored the point. It's simply because my findings focus on what I consider to be the central issue in this complaint – that being whether RBS is responsible for the loss Ms P suffered to the scam.

As RBS has pointed out, these payments aren't covered by the CRM code – which can offer a potential means of obtaining a refund following APP scams. This is because it doesn't cover payments made to an account held in a person's own name. I've therefore considered whether it would otherwise be fair and reasonable for RBS to reimburse Ms P.

In broad terms, the starting position in law is that a bank is expected to process payments that their customer authorises them to make. Here, it isn't disputed that Ms P knowingly made the payments from her RBS account and so, I'm satisfied she authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of her account, RBS are expected to process Ms P's payments, and she is presumed liable for the loss in the first instance.

However, taking into account regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for RBS to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

Here, before making the £20 payment, RBS has confirmed that Ms P would've been required to provide the reason for it as it was being made to a new payee (albeit to an account in her own name with L). In turn, a warning would've been provided to Ms P tailored to the associated risks with the reason selected. RBS can't confirm which reason was selected or what warning was provided to Ms P. But given it was of a very low value, I think this additional check – and the warning provided based on the payment reason selected - was proportionate to the risk presented by the payment at the time.

While R disagrees, I wouldn't reasonably have expected RBS to have carried out any additional checks before processing the first £5,000 payment. This is because, while it was of a greater value than Ms P typically spent on her account, it was being paid to an account held in Ms P's own name. And so, although RBS should be mindful of multi-stage fraud, I think RBS would've been reassured by this and I don't think the payment was so unusual or suspicious whereby I would've expected RBS to have been concerned Ms P was at a significant risk of financial harm. Particularly as it's common for customers to make occasional transactions of a higher value, and there is a balance for RBS to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate.

But I think the second £5,000 presented a greater risk, and so it would've been reasonable for RBS to have carried out additional checks before processing it. This is because it was the second £5,000 payment made to same payee on the same day. And although the payee was Ms P, this amount of spending was out of character for her based on prior account usage. I also consider the need to send two separate payments, rather than a single £10,000 payment, was unusual. And, as I've said, RBS should've been aware of the potential risk of multi-stage fraud. I therefore think it would've been reasonable and proportionate to the risk presented by the payment(s), for RBS to have contacted Ms P to discuss the payment before processing it.

I similarly consider that it would've been reasonable for RBS to have contacted Ms P before processing the £15,000 payment too – as it was a considerable increase on her prior account activity. Considering this, I've thought about whether, had RBS contacted Ms P to establish the surrounding circumstances of the payments, the scam would've been uncovered, and her loss prevented.

It's impossible to know with certainty how Ms P would have responded had RBS questioned her about the payments. I've therefore considered the overall circumstances of what happened - including what I know about Ms P's interactions with B, L and E – to reach a conclusion on what I think would most likely have happened.

At which point, I should clarify that I'm only considering the actions of RBS in respect of their responsibility to protect Ms P from financial harm from fraud as part of this decision. The actions of the other PSPs, which were involved as part of this multi-stage fraud, are being

dealt with separately. Nevertheless, Ms P's interactions with other third parties gives me a better understanding of what I think, on balance, would've most likely happened had RBS carried out further checks before processing the payments.

I've noted that R has provided substantive arguments regarding the quality of the interventions undertaken by the other PSPs involved – particularly by L. I've heavily summarised this, but I can assure R that I've considered everything they've said.

As R has pointed out, there isn't any evidence of coaching from B at the time of these payments – although I can't rule it out entirely – as the instant messenger chat conversations show it predominantly began from 2 March 2023. That said, I've considered Ms P spoke with L regarding a £5,000 payment she was attempting to make to the crypto provider on 23 February 2023 (funded from her RBS account). And in this call, Ms P confirmed to L she was making the payment for crypto purposes and that she'd successfully made payments to her wallet before. L then goes on to ask Ms P various questions, explaining to her this is because *"they are seeing a lot of scams with regards to crypto and it's just to make sure everything is ok at your end, and nobody is trying to get a hold of your money"*. L's questioning led to Ms P confirming:

- Nobody else had access to her wallet information, and she could withdraw from it.
- She hadn't received any calls offering great investment opportunities with crypto, to get high returns, nor have they asked her to move this money on a phone call.
- She hadn't responded to any ads on the internet or social media websites offering these good deals, and that she'd done her own independent validation.
- The money had come from one of her other personal accounts.

L also provided Ms P with a warning about crypto and the risks involved, with reference given to the FCA's published crypto warning – to which Ms P confirmed she was aware of the risks.

I understand R has said L didn't ask open and probing questions when undertaking their fraud checks. Instead, L focussed their questioning on some of the most common features of crypto investment scams – such as regarding unsolicited phone calls offering investment opportunities, responding to ads online or on social media, and access to the crypto wallet (including the ability to make withdrawals).

I accept a consumer shouldn't reasonably be expected to disclose information to a business beyond what they're asked, nor should they necessarily know what information a business requires. But I'm mindful that this part of the questioning, despite its context being in relation to investment scams, was somewhat relevant to Ms P's situation.

This is because Ms P had received unsolicited contact from a third-party, albeit via an instant messaging service, offering an opportunity to earn money. And although this was a job and not an investment, Ms P was still being directed to send funds to crypto as part of it. And so, I think this part of L's questioning ought reasonably to have resonated with her. It therefore wouldn't have been unreasonable to have expected Ms P to have disclosed that there was a third-party involved (B) and that they had directed her to send funds to the crypto provider. And even if Ms P hadn't specifically said this was as part of a job opportunity, as she wasn't asked nor would she reasonably have known to tell L, it would've given L pertinent information when ascertaining Ms P's risk of financial harm from fraud. In turn, it would've allowed L to have probed Ms P further about the payment and improved their ability to uncover the scam. Unfortunately, Ms P didn't share this information – and it's unclear to me

why she didn't.

I've also considered that, prior to the section of the chat conversation showing coaching from B, Ms P told them that she'd *"spent 20 minutes on the phone convincing my bank to allow the transfer".* And that, as part of the scam journey, Ms P had conversations with L about payments she was attempting to make – which included her being told there was a higher-than-normal risk of it being fraudulent, that fraudsters can provide convincing stories which can be very believable, and they often tell them not to speak with their bank. Furthermore, in the last call that took place in L's branch, Ms P withheld the true purpose of the payment she was attempting to make. With her at first saying she wasn't investing but putting the funds into her wallet to decide at a later date how to use it, before going on to explain that she would be using it *'indirectly'* for home improvements/debt consolidation (which was the reason she gave for the £15,000 loan application). And when questioned about who recommended the crypto provider, Ms P says she'd asked her friends – which wasn't true.

I accept that by the point of this last call between Ms P and L there is clear evidence of coaching from B for Ms P to mislead her bank(s). But I consider Ms P's willingness to follow B's instructions demonstrates her trust in B – and that she was heavily *'under their spell'*. This is further supported by the fact that, despite L's interventions that included scam warnings (albeit not specific to jobs scams), Ms P circumvented the payment restrictions L put in place by sending funds to her own account with E. And I think Ms P would've been aware the payments were being held due to fraud concerns.

Further to this, I've also considered that, despite an absence of evidence to show Ms P was coached prior to making the payments from her RBS account, there is evidence to show she was willing to provide misleading information. This is evident in her loan applications whereby, for example, she told L that it was for home improvements/debt consolidation. And despite the context of the first three conversations with L being around the risks of investing in crypto (an assumption on L's part), Ms P didn't seek to correct L or clarify the true payment reason – that being as part of a job opportunity. And when Ms P was eventually asked an open-ending question as to the purpose of one of the payments she was making, she only initially disclosed that it was to deposit funds to her wallet.

Because of this, I can't reasonably conclude that Ms P would've been forthcoming about the true reason for making the payments from her account if questioned by RBS. While I think RBS might have established it was for crypto purposes, given the payment references included the name of the crypto provider, it would've similarly been understandable for RBS to focus any questioning on the risk of crypto investment scams (as L did). This is because, although job scams involving crypto at the time had been on the rise, they weren't as prevalent as they are now. And the vast majority of crypto scams at the time of the disputed payments were in relation to investment scams.

It follows that, while I think RBS should've done more before processing the payments, I'm not persuaded Ms P would've told them that she was making them as part of a job opportunity or that a third party was involved – as she didn't with L. And I consider it more likely than not that Ms P would've very likely remained of the belief she was making the payments for legitimate purposes - particularly as she'd received several returns by this point. And any crypto scam warnings, based on what Ms P was willing to disclose, would've likely addressed the key risks and features of the most common crypto scams – crypto investment scams. Unfortunately, these wouldn't have been relevant to Ms P's situation and so, I don't think they would've resonated to the extent whereby she wouldn't have gone ahead with the payment(s). But even if Ms P did have any concerns, given the clear trust she had in B that I've alluded to, I think she would've likely referred such concerns to B and, accordingly, she would've been reassured of their legitimacy. In turn, I think Ms P would've followed their instructions to ensure she could continue making payments as part of the job

opportunity (as she did).

I've thought about whether RBS could've done anything to recover Ms P's loss when the scam was reported. But RBS could've only sought to recover them from L. And given Ms P had already used the funds as part of the scam, no funds would've remained. And even if they did, they would've been in Ms P's own account with L. I therefore don't think RBS could've recovered Ms P's loss.

I'm sympathetic to Ms P's situation as I realise she's suffered a significant financial loss. But it would only be fair for me to direct RBS to refund her if I thought the bank was responsible for her loss – and I'm not persuaded that this was the case. For the above reasons, I think RBS has acted fairly and so I'm not going to tell them to do anything further.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms P to accept or reject my decision before 29 May 2025.

Daniel O'Dell
Ombudsman