DRN-5710287

The complaint

Miss C complains that Bank of Scotland plc ("BoS") won't refund her the money she lost as a result of a scam.

What happened

The parties are familiar with the details of the scam, so I'll simply summarise what happened here.

In brief, Miss C fell victim to a task-based job scam. She says she received a text from a recruitment company about home-based work for a company. An online search showed the company to be legitimate, with mostly positive reviews. So she signed up and went through an onboarding process.

At the scammer's request, Miss C opened an account with a cryptocurrency platform. She had to make payments in cryptocurrency to unlock "tasks", which involved earning commission through simulating purchases. She was given access to a portal on which she could track her commission and unlock tasks. And she was told she'd be able to withdraw commission after completing a given number of tasks.

Eventually, when she was unable to withdraw money, having had to make ever increasing deposits to unlock tasks, Miss C realised she'd fallen victim to a scam.

Miss C made the following payments to the scam from her account with BoS:

	Date	**Transaction**	**Amount**
1	9 October 2023	Debit card to B	£34
2	12 October 2023	Debit card to B	£68
3	14 October 2023	Debit card to B	£108
4	14 October 2023	Debit card to B	£139
5	16 October 2023	Debit card to B	£2,000
	16 October 2023	*Debit card to N*	*£4,000 Declined*
	17 October 2023	*Debit card to R*	*£3,500 Declined*
6	17 October 2023	Faster payment to R	£3,500
7	17 October 2023	Debit card to B	£1,000
8	18 October 2023	Debit card to B	£700
9	18 October 2023	Debit card to B	£1600

	18 October 2023	*Debit card to B*	*£3,000 Declined*
	19 October 2023	*Debit card to B*	*£3,000 Declined*
	20 October 2023	*Debit card to B*	*£3,075 Declined*
	20 October 2023	*Debit card to B*	*£3,075 Declined*
10	20 October 2023	Debit card to B	£1,650
11	21 October 2023	Debit card to B	£12
12	22 October 2023	Debit card to B	£12
13	23 October 2023	Debit card to B	£12
		Total	**£10,835**

Miss C phoned BoS after her attempt to transfer money to R on 17 October 2023 was stopped. BoS asked her some questions about the payment and warned her about the danger of "safe account" scams. The transfer was then allowed. BoS didn't intervene when Miss C made any of the other payments.

One of our investigators considered the complaint, but didn't think it should be upheld. In summary, she thought that BoS had taken proportionate action when it spoke to Miss C before allowing payment 6, and she didn't think there was anything about the pattern or amounts of the payments, that ought to have prompted it to intervene further.

Miss C didn't agree with the investigator's view, so the complaint was passed to me.

My provisional decision

On 2 July 2025 I issued a provisional decision on this complaint to Miss C and to BoS. I explained that having considered all the relevant information about the complaint, I'd reached the same conclusion as the investigator, and on the basis of what I'd seen so far, I wasn't intending to uphold the complaint. But I said my reasoning was different from the investigator's, so I'd like both parties to have an opportunity to provide any further comments or evidence before I issued my final 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.*
>
> *It's not in dispute that Miss C has fallen victim to a cruel scam, and I was sorry to learn of this. It's also common ground that the payments made to the scam were 'authorised'. Miss C knew she was sending money to her own accounts with B and R. So even though she didn't intend the* payments *to end up with a fraudster, the payments were 'authorised' under the Payment Services Regulations. BoS had an obligation to follow the payment instructions it received, and Miss C is presumed liable for her loss in the first instance. But that's not the end of the story.*

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations, regulators' *rules, guidance, standards and codes of practice and, where appropriate, what I consider to have been good industry practice at the time. Taking those things into account, I think that at the time the payments were made, BoS should have been doing the following to help protect its customers from the possibility of financial harm:*

- *monitoring accounts and payments to counter various risks, including fraud and scams;*

- *keeping 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) – especially given the increase in sophisticated fraud and scams in recent years, with which financial institutions are generally more familiar than the average customer;*

- *acting to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring that all aspects of its products, including the contractual terms, enabled it to do so;*

- *in some circumstances, regardless of the payment method used, taking additional steps, or making additional checks, before processing a payment, or, where appropriate, declining to make a payment altogether; and*

- *being mindful of -among other things – common scam scenarios, how fraudulent practices were evolving (including, for example, the common use of multi-stage fraud by scammers, and the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers when deciding whether to intervene.*

All 13 payments were made to accounts in Miss C's own name. So the principles of the Contingent Reimbursement Model don't apply in this case. I've also borne in mind that all except payment 6 were *for the purchase of genuine cryptocurrency. So I acknowledge that Miss C's loss didn't arise directly from the payments she made from her account with BoS. The loss occurred at a later stage. But even so, there might have come a point at which I'd have considered that BoS should have taken a closer look at the payments, given the significant risk of fraud associated with cryptocurrency investments at the time.*

However, I also need to bear in mind that banks process high volumes of transactions every day, and I consider that there's a balance to be struck. Banks have obligations to be alert to fraud and scams *and to act in their customers' best interests, but they can't reasonably be involved in every transaction. And I think it was reasonable of BoS to consider a range of factors when deciding whether to take any additional steps before making the payments. Ultimately, I need to decide whether the payments were concerning enough that it would have been reasonable to expect BoS to have a closer look at the circumstances surrounding them, and whether, where it did so, it did enough.*

The first five payments were spread over a week, and while I recognise that some of them were significant amounts of money for Miss C, they weren't of such a high value that I consider that they should have prompted BoS to be concerned that Miss C was at heightened risk of financial harm.

Payment 6 was different from the other payments, in that it was made by faster payment, and was to an account Miss C held with a digital banking platform, rather than a cryptocurrency platform*. BoS stopped the payment and Miss C phoned its security team to confirm that she wanted to make the transfer.*

I've listened to a recording of the phone call. Miss C told the agent that she was sending the money to her account with R as it was almost Christmas, and she needed to do some online shopping. The agent asked her whether anyone else had access to her account with R, whether anyone had asked her to move money, whether anyone had called claiming to work for a bank or credit card company, and whether anyone had asked her to mislead BoS. She answered no to all those questions. The agent then went on to warn Miss C about "safe account" scams, outlining briefly how they worked, and told her that it might not be able to get her money back. Miss C said she hadn't received any calls like that, and the payment was then released.

I've thought carefully about the circumstances surrounding payment 6. It was made less than an hour after Miss C had unsuccessfully tried to pay the same amount to R by debit card. And the previous evening, she'd tried to pay a similar amount (£4,000) by debit card to a cryptocurrency provider, but *that had also been declined. BoS no longer has a record of why those two debit card payments were declined, but Miss C had more than enough money in her account to make the payments. And I think the most likely explanation is that BoS's systems flagged them as unusual and potentially financially harmful to Miss C.*

There's no record of Miss C having contacted BoS about the declined debit card transactions on 16 and 17 October. But when she phoned about the attempted transfer on 17 October, BoS picked up on the possibility that the transfer was connected to a "safe account" scam. In those cases, someone pretending to be from the victim's bank persuades the victim that the money in their account is in danger, and persuades them to move it to another account to keep it "safe".

Given that the attempted transfer for £3,500 was to an account in her own name, I can see why BoS warned Miss C about safe account scams, as that (a customer transferring money to their own account) is what 'appears' to be happening in that type of scam. But I don't consider that the intervention *went far enough in the context of this particular case.*

By the summer of 2023, a variety of types of scam involving cryptocurrency had become prevalent. In the circumstances*, I think it would have been fair and reasonable to expect BoS to ask Miss C a series of questions to try to establish what, if any, scam risk there was in this case.*

As it was, BoS didn't ask Miss C any open questions about the transfer, or about the payments she'd recently started making to cryptocurrency platforms, including the two significant debit card payments that had been declined within the previous 24 hours – one of them less than an hour before the attempted transfer. I acknowledge that the payment to R had no clear link to cryptocurrency, but against the background of the transactions over the previous week, I consider that BoS should have asked Miss C more detailed and probing questions, with a view to preventing foreseeable harm to her. And I need to decide on the balance of probabilities what it's likely would have happened if it had done so.

However, I can only uphold Miss C's complaint if I think it likely, on balance, that proportionate intervention by BoS would have made a difference, and would have led to her stopping making payments to the scam. I'm sorry to disappoint Miss C, but in the light of all the available evidence, I'm not persuaded that it would. I'll explain why.

In the course of my investigation I contacted R. It provided copies of Miss C's statements for the period around the time she made payment 6. They show that on the day on which Miss C made payment 6, she made two payments of £850 from her account with R to the same person. It looks, from Miss C's WhatsApp chats, as if those were for the purchase of cryptocurrency – what's known as a "peer to peer" purchase.

R paused the first of those payments and redirected Miss C to what it's described as a "targeted scam intervention *flow". It explained to Miss C that its system had flagged the transaction as a potential scam, and that it needed to ask her some questions in order to continue. There was the option to cancel the payment, but Miss C selected "continue to questions". Miss C was taken to a screen which highlighted the importance of answering truthfully, and warned her specifically that if she was being scammed, the scammer might ask her to hide the real reason for making the payment. Miss C confirmed that she understood.*

R then asked Miss C a series of targeted questions. It asked whether anyone was telling her how to answer the questions*, or telling her that the payment was urgent. Miss C said that nobody was doing either of those things. R said that if someone was telling her to ignore the warnings, they were a scammer. And it said she should only continue with the payments if she wasn't being prompted to do so. Miss C chose to continue, and was then asked why she was making the transfer. She selected "As part of an investment" and then specified "Gains from crypto". That answer triggered further questions from R, in response to which Miss C confirmed that:*

i) she hadn't been asked to instal any software;

ii) she'd discovered the investment opportunity through a friend or family member;

iii) she'd invested in cryptocurrency before;

iv) she'd researched the investment company; and

v) the money was being sent to her existing account.

Next, R displayed a warning that Miss C might be falling victim to a crypto investment scam, with additional warnings *about matters such as being wary of social media promotions, and not giving remote access to her computer.*

*Miss C selected "*Continue*" to go ahead with the payment, and was taken to a "Risk agreement" screen. R says Miss C couldn't go ahead with the transfer without writing her name to acknowledge that she understood that "[R] has warned me that this payment is suspicious and I understand the risk of losing my money". Miss C wrote her name and was given the option to either "send payment" or "cancel payment". She chose to send it.*

So Miss C was given a clear and firm warning by R that it thought she was the victim of a scam, but she concealed the true background to the payments, and still went ahead and made them.

Miss C has consistently told us that she wasn't coached by the scammer about what to say in answer to any questions from banks, other than the general explanation that she was making the transfers for shopping*. Miss C's representatives have commented that it's not clear why she'd have needed to transfer money from her BoS account to another account in order to shop. I agree that it's unlikely that the shopping story would have held together if BoS had asked Miss C open and probing questions about the payment and recent activity during the call on 17 October 2023.*

Whether or not she was being coached by the scammer about what answers to give, in the light of the answers she gave to rigorous questioning by R, I think it's unlikely that Miss C's answers to proportionate questioning by BoS would have led it to the truth – that she'd fallen victim to a job scam. In light of the previous account activity, and given her answers to R, I think it's more likely that her answers would have led BoS to provide a tailored cryptocurrency investment scam warning, and that Miss C would have chosen to go ahead with the payment, as she did after R questioned and warned her.

I acknowledge that R's intervention took place online, and that it can be easier to give convincing answers online than it is under pressure in a phone call. But overall, I think Miss C was determined *to make the payments, and I'm not convinced that BoS would have discovered the truth about the purpose of the payments, even if it had done all that I find that it should have done.*

I acknowledge that if BoS had provided Miss C with a targeted job scam warning, it's possible that it would have resonated with her. But without any indication or hint that that was the true reason *for the payments, I don't think BoS could reasonably have been expected to provide such a warning.*

So taking everything into account, while I don't think that BoS went far enough with the questions that it asked Miss C on 17 October 2023, I don't think she'd have stopped making the payments even if it had done. And the remaining payments to the scam weren't of a pattern or size that I think would have warranted further intervention by BoS after that date.

I've thought about whether BoS could have recovered the money using a chargeback. But I don't think a chargeback *would have succeeded in this case. This is because the money was sent to a crypto account in Miss C's own name, and was used to buy genuine cryptocurrency. So she effectively got what she paid for. And I can't see that there'd have been any other way to recover the money.*"

And I said that my provisional decision was that I didn't uphold the complaint.

Further submissions

BoS hasn't responded to my provisional decision, and the time for providing any further comments has expired. Miss C commented that I hadn't referred to her vulnerability. She's explained that she is neurodivergent, and this made it easier for the scammer to build up a relationship with her and take advantage of her. She says she was also suffering mentally at the time, due to the serious poor health of a close family member.

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.

Since receiving Miss C's comments on my provisional decision, the investigator has explained to her that while I take into account all the information provided by both parties, I only refer specifically in my decision to key points that I consider relevant to the outcome. The investigator told Miss C that the complaints management company which previously represented her had raised the issue of her vulnerability again in its response to the investigator's view, and the investigator had explained that BoS hadn't been aware of Miss C's vulnerability until after the scam.

I'd like to add to what the investigator's said to Miss C. I'm aware that I've summarised the complaint in less detail than Miss C has set out, and using my own words. I'd like to reassure Miss C that no discourtesy is intended by this. If there's something I haven't mentioned, it isn't because I've ignored it. Rather, it's because I'm satisfied that I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this, and it's in keeping with our role as an informal dispute resolution service.

BoS's records show that Miss C didn't notify it of her vulnerability until around five months after the scam took place. I acknowledge that Miss C has provided a copy of a letter from BoS apologising for the way it handled a call when she contacted it in March 2024. In that letter it accepts that it could have done more at that stage to support her, in view of her vulnerability. But that was some time after Miss C fell victim to the scam, and it isn't in dispute that by then she'd told BoS about her vulnerability. Neither Miss C nor her former representative has suggested that she had, in fact, told BoS about her vulnerability before she fell victim to the scam.

I'm very sorry to hear of the additional challenges Miss C was facing at the time, and can understand how these may have made her more susceptible to being scammed. But based on the information I have, I can't reasonably find that BoS ought to have taken extra measures, at the time the payments were made in October 2023, to take account of Miss C's vulnerability. This is because I've seen nothing to make me think that it had been notified of it at that stage. So I'm sorry to disappoint Miss C, but this doesn't change my view of the complaint.

As I said in my provisional decision, it isn't in dispute that Miss C fell victim to a cruel scam. I have considerable sympathy for her, and don't underestimate the impact the situation will have had on her. But having thought carefully again about everything that both parties have said, I don't consider that there's any good reason to depart from the findings I set out in my provisional decision.

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 Miss C to accept or reject my decision before 27 August 2025.

Juliet Collins
Ombudsman