DRN-5638424

The complaint

Mrs S complains Bank of Scotland plc trading as Halifax won't refund the money she lost when she fell victim to a scam.

What happened

Around September 2020, Mrs S says she came across an advert for a cryptocurrency opportunity, seemingly promoted by a well-known public figure. She responded to the advert and was then contacted by an individual claiming to be an account manager acting for a company, "B". Unfortunately, this was a scam.

The scammer directed Mrs S to set up a cryptocurrency wallet with a genuine exchange, "C" using remote access software to help her with this. She then sent funds from Halifax to her C account. From there, I understand she purchased cryptocurrency and sent it on to the scammer, or possibly granted access for the scammer to move the funds – thinking this money was being genuinely invested for her, by the alleged account manager, on B's trading platform.

Mrs S says contact with B subsequently ceased. She initially thought it was a failed investment, but later found information about B which suggested it was a scam.

In early 2024 she reported the scam to Halifax – and subsequently complained, via a professional representative, about its decision not to refund her. She said it failed to intervene and provide an effective warning. Halifax maintained its position, so Mrs S referred the matter to our service.

Our investigator didn't uphold the complaint. She initially concluded Halifax didn't have cause to intervene with the payments. She later said it arguably could have intervened when Mrs S sent a £5,000 payment to C in September 2020 – but wasn't persuaded this would have uncovered the scam, noting a warning issued by the regulator about B wasn't published until after this payment was made.

Mrs S appealed the investigator's outcome. In summary, her representative said Halifax should have intervened when she sent the £5,000 payment – and this would have succeeded in uncovering the scam. It says the bank is the expert, not consumers, so it should warn them of potential harm.

I issued a provisional decision clarifying the scope of what I was considering – and addressing why I was minded to agree with the investigator's outcome.

On the scope of the complaint, I explained:

> *The investigator's outcome referred to four scam payments made in September and October 2024. However, I can see from Halifax's response to Mrs S's complaint that it considered five more scam payments, made between November 2020 and February 2021.*

In looking at Mrs S's complaint form, I also consider it clear these later payments formed part of her referral to our service – as she explained, "Please note that the total loss differs from the one stated in the original formal letter of complaint sent by my solicitor because the bank brought to our attention that there were additional scam payments".

I'm therefore satisfied these later payments form part of Mrs S's complaint and referral to our service – and so fall within our service's jurisdiction to consider. I therefore want to clarify that, when looking into this complaint, I've taken into account all nine scam payments. Both parties now have the opportunity to let me know if they think I'm wrong about the scope of this complaint before I make a final decision.

I then proceeded to explain why I wasn't minded to uphold the complaint:

It's agreed Mrs S authorised these payments. That means the starting position is that she's liable for the transactions. In line with the Payment Services Regulations 2017, firms are expected to process authorised payment instructions without undue delay.

However, there are some situations where I would reasonably expect a firm to make further enquiries about a payment before deciding whether to process it – such as in circumstances where there are grounds to suspect it presented a fraud risk. An indication of risk could be where the characteristics of the payment(s) looked unusual compared to how the account was normally used.

If a firm failed to respond proportionately to such a risk, and doing so would have prevented the consumer from incurring a fraudulent loss, it may be fair to hold the firm liable. I've considered whether it would be fair to hold Halifax liable for any of Mrs S's loss in the circumstances of this complaint.

All the scam payments were sent to C, a genuine cryptocurrency merchant. The first scam payment (in September 2020) was for £2, followed by £5,000 later that day. Following this, around £500 further was sent. This was spread out over seven payments between October 2020 and January 2021; no more than £100 was sent in one go.

Mrs S also received three credits back from C. She has confirmed the first credit (around £550 in October 2020) was a withdrawal from B's platform. I don't have further details about the later credits (around £120 in November 2020 and £150 in December 2020).

While I don't think most of the scam payments looked particularly concerning, the second scam payment (for £5,000) did look out of character compared to Mrs S's normal spending. It was significantly higher than any prior recent payments and was being sent to a payee Mrs S had only paid once before earlier that same day.

In response to the risk profile of this payment, I think it would have been proportionate for Halifax to have spoken to Mrs S at this point, to find out more about what she was doing. This would have provided an opportunity to gauge whether her responses suggested she was at risk from fraud – and to warn her if so.

I can't know for sure how Mrs S would have responded to appropriate questioning (and warnings) at the time. Given how long ago this scam occurred, records about what happened are limited. Weighing up what I do have available to me, I'm not persuaded what I've seen demonstrates it's more likely than not that Halifax's failure to intervene caused or contributed to Mrs S's fraudulent loss.

I have very little information about this scam. Mrs S says herself she can't recall the exact details of what happened. And her original testimony in her complaint to Halifax was that the scammers ceased contact after a payment in late October 2020. While she then confirmed the later payments to C (which continued until January 2021) were also part of the scam, I haven't been provided with further information about how the scam transpired after this point – or why she initially said contact stopped prior to this.

While difficult to read, I have seen what appears to be a screenshot showing Mrs S's C account has a £0 balance. But I can't see how the C account was being used during the time of the scam. This is relevant to my point above about what happened with the scam from October 2020 onwards. Particularly as credits were received back during this time, which I don't have details for.

It also appears not all the funds were being moved on immediately from C to the scam. Mrs S says, in late October 2020, B asked her for £500. She then sent £100 to C – but says she had enough funds left in her C account to make up the rest. Again, this feeds into my uncertainty around how the funds were being used/moved on.

I also don't have any records of Mrs S's contact with the scammers, to help fill in the gaps in my understanding and Mrs S's recollections of what happened. I appreciate this is all due to the time that has passed since the scam. And to be clear, I don't doubt Mrs S has genuinely fallen victim to a scam. But the lack of evidence, and the contradictions and uncertainty around how the scam transpired does, in my view, make it harder to draw an inference in Mrs S's favour that intervention would have prevented the scam from unfolding.

Additionally, the limited information I do have also gives me reason to doubt whether proportionate intervention would have uncovered the scam. Mrs S believed the account manager to be an experienced stockbroker based abroad. She says she trusted them "implicitly" – mentioning they built up rapport and weren't offering returns which seemed too good to be true. She also had access to B's trading platform (allegedly) showing the trading. And while the UK financial regulator did go on to issue a warning about B, this wasn't published at the point at which I think Halifax should have intervened (September 2020).

All of this gives me pause over whether Halifax would have been able to persuade Mrs S not to proceed. From what I have seen, it's clear Mrs S had built up substantial trust with B. And I'm not sure the main hallmarks that this was a scam would have been clear to Halifax, or Mrs S, at the time.

Furthermore, the fact I don't have any records of Mrs S's contact with the scammers makes it harder for me to draw an inference in her favour in this respect. I'm aware that, in scams like this, it's common for scammers to trick consumers into giving cover stories, to hide the fact they intend to send funds on from the genuine merchant they are paying directly. It's therefore unclear to me if proportionate questioning would have made the nature of the scam risk clear to Halifax – relevant to its ability to assess, and warn Mrs S, of the scam risk.

I appreciate Halifax could still have warned Mrs S about the broad features of cryptocurrency scams. Such as how scammers often target people via cold calls or social media adverts, and trick them into transferring funds on to fake trading platforms. But given what I have outlined above, I simply don't have enough insight into how this scam operated to be persuaded, on balance, that such a warning would have resonated with Mrs S.

Unfortunately, we know scams like this can be very convincing – using sophisticated and professional fake websites and platforms, and employing social engineering tactics to persuade victims to place a lot of trust in the scammers, even over their banks.

I'm also conscious Mrs S was seemingly able to withdraw funds on three separate occasions. I appreciate this occurred after the payment Halifax should have intervened on. But the fact this happened several times suggests that, if Mrs S had attempted to withdraw some funds to test B's legitimacy following an intervention by Halifax, she probably would have been able to do so.

Overall, I'm not persuaded it's more likely than not that Halifax should have been able to prevent Mrs S's fraudulent losses at the time of the payments. And as the funds were sent on to an account she held, Halifax wouldn't have been able to recover the funds either (which it seems were lost or moved on before the scam was reported to Halifax).

Mrs S has expressed concern about her treatment when reporting the scam to Halifax. It seems a lot of this relates to them asking her for records of her C account. I can understand why this was difficult and stressful for Mrs S, but I don't consider it an unreasonable request; it was relevant to establish her loss, and to understand how the scam unfolded.

I'm not persuaded Halifax's handling of the claim caused Mrs S avoidable upset at a level which warrants compensation. In saying that, I do appreciate the process was difficult and upsetting for Mrs [S]. But I think that was largely due to the sensitivities of the scam, rather than errors by Halifax in how it handled things.

I invited both parties to provide any further comments or evidence before I made my final decision. Halifax has confirmed receipt of my provisional decision, but hasn't added anything further.

Mrs S's representative has confirmed she would like a final decision. It disagrees with my conclusion that intervention would have prevented the scam. It says robust intervention was warranted and a timely, informed warning covering the risks of cryptocurrency scams, particularly one involving remote access software, could have worked. This would have provided Mrs S with context to question her trust in the scammers.

What I've decided – and why

As I've received no response to my comments about the scope of this complaint, I consider this matter to be accepted. I've therefore proceeded to consider all nine scam payments within this case.

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

Having done so, I've decided not to uphold it. This is largely for the reasons given in my provisional decision, which are set out above and also form part of my final decision. I'll focus here on responding to the points raised in response to my provisional findings.

Mrs S's representative argues robust intervention was warranted. I agree. However, as set out in my provisional decision, I'm not persuaded such an intervention would have worked.

I highlighted in my provisional decision that I didn't have records of how the funds were

being moved on to the scam via C; Mrs S's contact with the scammers; or any recollections from her about the later scam payments (and credits) that weren't initially reported. The response to the provisional decision doesn't address this. So, I don't have much further insight to help explain why, in the specific circumstances of this scam, intervention on the £5,000 payment would have worked.

I appreciate the representative says mentioning the use of remote access software could have worked, as this is something which Mrs S has mentioned was used during the scam. However, it's unclear to me that Mrs S would have disclosed the use of remote access software if Halifax had asked about this.

It's common for scammers to coach victims and persuade them not to divulge full details of what they are doing if questioned by their bank. In the absence of any records of Mrs S's contact with the scammers, and given the trust she has told us they built up, it seems more likely to me she was (or would have been) coached on what to say.

Furthermore, I'm not persuaded a warning about remote access would have been enough to break the spell of the scam. While its use is associated with cryptocurrency scams, there are also legitimate uses for remote access software. And this is something which the scammer may have been able to "explain away", even if Mrs S had concern about this following a warning from Halifax, given the trust they had built up. Again, as I don't have records of her contact with the scammers, I don't think it's been demonstrated, on balance, that this would have succeeded.

I also think some of the more obvious hallmarks B were a scam likely wouldn't have been so clear at the time of the £5,000 payment. The regulator's warning wasn't issued about B until later on. And while Halifax would have been aware of the common features and risks of cryptocurrency scams in late 2020, I'm conscious awareness and knowledge of these scams has evolved a lot since then.

I can't look at this complaint with the benefit of hindsight; I must think about what it's fair to expect from Halifax at the time. Overall, even if Halifax had intervened at that time – and that intervention had specifically asked/warned about the use of remote access software – I'm not persuaded it's more likely this would have prevented the scam from unfolding.

I appreciate this will be disappointing for Mrs S, who has clearly lost out at the hands of the scammers. However, having carefully considered all the circumstances, I'm not persuaded it would be fair to direct Halifax to refund her loss.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 21 July 2025.

Rachel Loughlin
Ombudsman