DRN-5211432

The complaint

Mrs T complains that Bank of Scotland plc, trading as Halifax, won't refund money she lost when she was a victim of an investment scam.

Mrs T is represented by a firm I'll refer to as 'M'.

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 Mrs T was introduced to an investment opportunity – with a firm I'll refer to as 'IC' – by a friend. Mrs T was added to instant messenger app group chat with other investors. And, as part of the scam, Mrs T purchase crypto from a legitimate crypto provider before forwarding it on to IC. The relevant transactions are:

Date	**Transaction type**	**Amount**
10 November 2023	Faster payment	£1,000
20 November 2023	Faster payment	£3,226
20 November 2023	Faster payment	£502
20 November 2023	Faster payment	£3,223
21 November 2023	Faster payment	£2,823
22 November 2023	Faster payment	£301
	Total	£11,075

Mrs T received credits from the crypto provider of £400 and £3,223 on 21 November 2023. And so, her loss to the scam is £7,452.

Mrs T realised she'd been scammed when investors in the group chat started reporting that they couldn't withdraw their funds. M complained, on Mrs T's behalf, to Halifax on 24 January 2024. In short, they said:

- The Financial Conduct Authority (FCA) published a warning about IC on 5 December 2023. It's widely accepted to have been a scam.
- Under the Contingent Reimbursement Model (CRM) code, a payment service

provider is expected to offer protection to their customers from Authorised Push Payment (APP) scams.

- The bank is required to reimburse for loss incurred through an APP scam unless their customer is found to have been grossly negligent or has ignored effective warnings issue by their bank.

- They consider any warnings Mrs T may have received from Halifax weren't effective.

- As Mrs T was inexperienced, she should've been considered vulnerable. So, Halifax should've put additional measures in place to protect her.

- Halifax should refund Mrs T in full, pay 8% simple interest and £1,000 compensation.

Halifax didn't uphold Mrs T's complaint. They said the payments weren't covered under the CRM code as they were sent to an account in Mrs T's own name – and not directly to the fraudster. They also explained that they spoke to Mrs T about the first payment – discussing scams, crypto risks and that she could possibly lose all her money. Mrs T was happy to go ahead with the payment, which meant they had no reason to stop subsequent payments.

Mrs T's complaint was referred to the Financial Ombudsman. Our Investigator didn't think Halifax had to do anything further, as she didn't think Halifax could've reasonably prevented Mrs T's loss. She explained the payments weren't unusual for Mrs T based on her prior account usage. But Halifax did speak to Mrs T in relation to the first payment before processing it. From this discussion, they had no reason to suspect anything untoward and Mrs T confirmed she understood the risks and wished to continue with the payment. Our Investigator also didn't think Halifax could've reasonably recovered Mrs T's funds, or that compensation was warranted.

M disagreed. In short, they said:

- The payments to the crypto provider, as a new payee, should've flagged as irregular. And so, they should've been questioned at the time. Had this happened, Halifax would've been aware of Mrs T's status and vulnerability – having recently lost her father. The bank should've then put additional measures in place to protect her.

- The enquiries made in the call by Halifax were insufficient. The bank should've sought clarity on the purpose of the transaction with further questions asked.

- This would've led to Mrs T disclosing it was for an investment with IC, which Halifax should've identified as a fraudulent scheme (with a website link provided to the Financial Ombudsman showing it was scam).

- The payments were made in quick succession and involved substantial amounts – which was inconsistent with Mrs T's usual account activity. Halifax should've put all this information together and put in more measures to protect Mrs T.

The matter 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 Mrs T has been the victim of a scam, and I don't underestimate the impact this has had on her – as I appreciate it is a significant amount of money she has lost. I therefore want to reassure Mrs T that I've given careful consideration to her complaint and all the points put forward by M on her behalf. If, however, I don't mention a particular point, it's not because I haven't considered it, but I've focussed instead on what I believe to be important to the outcome of this complaint. And here, I must consider whether Halifax is responsible for the loss Mrs T has suffered. I know this won't be the outcome Mrs T is hoping for but, for similar reasons as our Investigator, I don't think they are. I therefore don't think Halifax has acted unfairly by not refunding the payments. I'll explain why.

I've thought about the CRM code which can offer a potential means of obtaining a refund following scams like this one. Here however, the payments aren't covered by it. This is because the payments were made to a crypto wallet in Mrs T's own name, with a legitimate crypto provider. I've therefore considered whether it would otherwise be fair and reasonable to hold Halifax responsible for Mrs T's loss.

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

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Halifax 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, Halifax did speak with Mrs T before processing the first payment. I've therefore considered whether Halifax did enough to protect Mrs T from the scam when carrying out their additional checks. And if they didn't, whether this caused her loss.

I've listened carefully to the call between Mrs T and Halifax. Having done so, I think they asked appropriate questions, tailored to the risks associated with crypto, to establish whether Mrs T was potentially falling victim to a scam. This is because, from their conversation, Halifax were able to establish that Mrs T's payment, which she confirmed was for investment purposes, was going to an account (wallet) in her own name had that nobody else had access to her log in details. Mrs T also confirmed that she had done a little bit of crypto before. And Halifax specifically asked:

> *"Are there any third parties that you've met online, or anyone you don't personally know, who helps you, or advises you, or mentors you with your trading?"*

Mrs T replied *"No, no one"*. This, unfortunately, meant Halifax were unaware that Mrs T was investing with IC. Because of this, Halifax would've felt reassured that Mrs T was investing in crypto legitimately in her own right – with the funds secure in her own crypto wallet. Later in the call, Halifax also explained that the FCA had highlighted the volatility of crypto several times and that investors should be prepared to loss of their money. Mrs T confirmed she understood this risk and wanted to proceed with the payment.

Halifax could, arguably, have asked further questions about the surrounding circumstances of the payment – such as how she'd come to decide to invest in crypto or what checks she had undertaken. But even if they had, I'm not convinced this would've led to the scam being

uncovered by Halifax. This is because Mrs T was introduced to IC, who she didn't mention in the call, via a friend. So, even if Mrs T had disclosed the recommendation to invest had originated from her friend, this likely would've reassured Halifax she wasn't falling victim to a scam - as it hadn't come through social media or unsolicited contact (which are common features of crypto scams). The FCA warning about IC also hadn't been published at the time of the payment(s). And from what I've seen, there seemed to be limited information in the public domain suggesting IC could be a scam (I note that the website link M has provided no longer works). But because of this, I don't think Halifax, through proportionate enquiry to the risk presented by the payment, could've uncovered Mrs T was being scammed – particularly in the absence of knowing about IC.

The subsequent payments Mrs T made rose in value and were also made in a relatively short period of time. It would've been reasonable to have expected Halifax to have carried out further checks before processing some of these too. But if they had, I'm not persuaded it would've made a difference. I think questioning aimed at the risks associated with crypto investments would've most likely resulted similarly – with Halifax reassured that Mrs T, who had some prior crypto experience, was investing independently and with a legitimate provider.

I'm aware M has suggested Halifax ought to have identified Mrs T as being vulnerable and put in place additional measures to protect her. While I appreciate Mrs T would've understandably been impacted by her father's death, I don't think Halifax could've reasonably identified – from their interaction with Mrs T – that she was *potentially* more vulnerable to falling victim to a scam due to her personal circumstances. Nor have I seen anything to show Mrs T informed Halifax as such. Because of this, I don't think Halifax needed to do anything more in this respect (or that they treated Mrs T unfairly as a result).

I've considered whether, on being alerted to the scam, Halifax could reasonably have done anything more to recover Mrs T's losses, but I don't think they could. This is because Mrs T had already transferred the funds out of her crypto wallet to IC. And so, there weren't any funds to recover from the payee – that being the crypto provider. But even if there were funds remaining, Mrs T would've had access to them.

I have a great deal of sympathy for Mrs T and the loss she's suffered. But it would only be fair for me to direct Halifax to refund her loss if I thought they were responsible – and I'm not persuaded that this was the case. For the above reasons, 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 to accept or reject my decision before 16 July 2025.

Daniel O'Dell
Ombudsman