DRN-5104416

The complaint

Mrs A and Mr A complain that Bank of Scotland plc trading as Halifax (Halifax) won't refund money they lost in an investment scam.

What happened

What Mrs A and Mr A say:

Although Mrs A and Mr A have a joint account (from where the payments were made), the contact with Halifax was with Mr A – so for simplicity I refer to Mr A as the complainant here.

Mr A says he was added to a 'Telegram' chat group, and people on it were saying they'd made good returns by investing with 'firm X'. They shared screenshots of their earnings. He managed to speak to a representative of firm X who was professional and knowledgeable. Mr A looked at firm X's website and it appeared professional and high quality. He was told he could make returns of 200-300 %. He says he was unfamiliar with crypto currency investment.

Mr A made four payments to a crypto exchange account in his name and then to firm X:

	Date	Payment	Amount
1	3 November 2022	Faster payment – crypto wallet	£470
2	3 November 2022	Faster payment – crypto wallet	£4,650
3	10 November 2022	Faster payment – crypto wallet	£3,900
4	11 November 2022	Faster payment – crypto wallet	£4,025
	Total		**£13,045**

But when he tried to withdraw funds, he was told he had to pay a fee – which he did. But a further fee was then asked for, and he realised he had been the victim of a scam.

Mr A says Halifax should've done more to protect him. He says:

- He wasn't aware of the need to check the Financial Conduct Authority (FCA) website.
- Firm X wasn't registered in the UK.
- The crypto exchange account was set up the same day and under the guidance of

someone else.

- He didn't understand how such investments worked or the scam risk involved when investing online.

He recalls there were some conversations with the bank, but all the bank did was to establish that it was he who authorised the payments. He says the questioning wasn't thorough enough. Had they done more, the scam would've been uncovered. He says Halifax should refund the money he's lost plus interest at 8% per annum.

What Halifax said:

Halifax didn't refund any money. The bank said they'd spoke to Mr A on three of the payments but he wasn't truthful about the nature of them, so they were allowed to go through.

And in June 2020, he was the victim of an earlier investment scam and was given education at that stage about how to avoid future investment scams. However, he didn't follow that guidance.

Our investigation so far:

Mr A instructed a third-party claims firm to bring his complaint to us. Our investigator didn't uphold it and said:

- Halifax spoke to Mr A regarding three of the payments. During the calls, Mr A had the chance to tell Halifax about what had happened but wasn't open with the bank.

- Therefore he thought the bank did enough checks and were entitled to put the payments through.

Mr A didn't agree, he said the questioning wasn't open and probing enough. He felt there were enough indications in the calls to show he was involved in a scam and the bank should've picked up on that. In response, our investigator didn't change his view, and so Mr A asked that an ombudsman look at his complaint. So, it has come to me.

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 to hear that Mr A has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr A didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make 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.

I need to decide whether Halifax acted fairly and reasonably in its dealings with Mr A when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary– and in this case, the payments were made to Mr A's own account with the crypto exchange.

The important matter here is whether these were payments that Halifax might reasonably have considered unusual, and therefore whether they should've held or stopped the payments and contacted Mr A.

I note that we've not been provided with the Telegram chats that caused Mr A to be introduced to firm X, nor have we seen any emails or online chats between Mr A and the scammers. I've therefore based my decision of the information we've received.

I looked at Mrs A and Mr A's account history with Halifax. And it's fair to say they made regular and large payments out of the account – I could see for example:

November 2022 (prior to scam): £19,500 (crypto related).

October 2022: £2,174.

September 2022: £1,464.

August 2022: £2,500.

June 2022: £8,000, £1,500, £1,137, £1,000.

May 2022: £5,000.

So – I wouldn't have been surprised if Halifax hadn't stopped any of the payments in question – as they weren't completely out of character.

But in this case, the payments were detected by the bank's fraud protection systems and Halifax contacted Mr A – and asked him more questions.

Halifax was the expert in such matters and we would have expected them to ask open questions such as:

- Why are you making the payment?

- Who to?
- For what purpose?
- How did you hear about the investment?
- How were you contacted about it?
- Where did the money come from that you're investing?
- Where is the money going to from your crypto wallet?
- What do you know about crypto investing?
- Have you made crypto investments before?

So, I reviewed the calls in the light of what we'd expect Halifax to have done when they spoke to Mr A.

The calls are important in the context of this complaint – as Mr A's advisors have argued. I set out some of the conversations here:

Call - 5 November 2022 - £4,650:

Halifax couldn't provide this call for us to listen to but did provide a transcript of it.

Halifax's call handler: *have you used (named crypto exchange) before for crypto?* Mr A: yes.

Halifax's call handler: (*have the other payments) successfully shown in your wallet?* Mr A: yes.

Halifax's call handler: (*always) make sure you can see your money going your account.* Mr A: definitely.

Halifax's call handler: *confirm to me…you haven't received any phone calls, texts, emails from anybody asking you to complete these crypto transactions (and) you've (done it) yourself*. Mr A: no (confirmed).

Halifax's call handler: *we are seeing people responding to the ads like advertisement on the likes of Instagram or social media…. .You haven't responded to any ads?* Mr A: no

Call - 10 November 2022 - £3,900:

Halifax's call handler: *What is the payment for?* Mr A: forex trading.

Halifax's call handler: *What are you trading? Currencies?* Mr A: yes.

Halifax's call handler: *But this appears to be for crypto*? Mr A: yes, it is for forex trading.

(there's some confusion here as the call handler tries to establish whether it is for crypto or pure currency trading – there is a confusion over the name of the crypto exchange)

Halifax's call handler: *Is it for crypto currency or for currency trading?:* Mr A: for different currencies…a 'global exchange'. Mr A gives the name of firm X.

Halifax's call handler: *That's a crypto platform.* Mr A: yes it's (names another currency exchange).

Halifax's call handler: *Has anyone asked you to set this up, contacted you via social media?* Mr A: no.

Halifax's call handler: *Is it crypto?* Mr A: no.

Halifax's call handler: *What is firm X?* Mr A: it trades with currencies, including crypto currencies.

Halifax's call handler: *Have you checked the FCA register?* Mr A: yes, been investing for quite a while now. The money is there (i.e. in the account of either firm X or the crypto exchange).

Halifax's call handler: *Have you made any withdrawals?* Mr A: yes.

Halifax's call handler: (We) *want to make sure it isn't a scam…* Mr A: yes ok.

Halifax's call handler: *I see you've sent money to crypto before – why use firm X now instead?* Mr A: a friend I know introduced me to it, Someone I trust.

Halifax's call handler: *Someone you met online?* Mr A: no, someone I know in person. He's done it and I'm comfortable with it.

Halifax's call handler: *Firm X comes up (in a search) as 'online trading scams'…who decides where the money goes - what trades?* Mr A: me, I decide. I control the money.

Halifax's call handler: *Anyone telling you what trades*? Mr A: no.

Halifax's call handler: *Anyone help you set up an account?* Mr A: no.

Halifax's call handler*: Some things about this sounds like a common scam. If it is a scam, we won't be able to help you and the money will be lost.*

Halifax's call handler: *Was the money you sent last week received ok*? Mr A: yes

The payment was then released.

Call -11 November 2022- £4,025:

Mr A said he wasn't happy at the payment being stopped for a third time in a few days. He said he was told by the previous call handler it wouldn't happen again. In the light of the fact that Mr A had been asked questions before, Halifax's call handler only asked brief questions.

Halifax's call handler: *whose account is this going to?* Mr A: my account.

Halifax's call handler: *Why payment to this account*? Mr A: no, it's to my account.

Halifax's call handler: *Have you done your checks?* Mr A; yes I've been through this three times.

Halifax's call handler: *Before I release this payment if it turns out to be a scam, you won't be able to get your money back and the chances are you'll lose your cash ok*? Mr A: yes I'm happy.

Call - 30 June 2020:

I also listened the call between Halifax and Mr A which took place on 30 June 2020. Mr A had lost £8,000 (two payments of £4,000) in an investment scam. As part of the conversation, Halifax's call handler advised him in future to:

- Check the FCA website for the investment firm and the registration of a firm's investment advisors.
- Check Companies House for the investment firm.
- Check it out with a known and trusted financial advisor.

Mr A said he would write down this guidance as it 'was important'.

Mr A's advisors (in bringing this complaint to us) argue that there were signs in the calls that suggested Mr A was being scammed and therefore the payments should've not been made.

They said:

- Halifax's call handler at one stage stated that firm X came up as a 'scam' online.
- It comes across that Mr A wasn't aware of what he was investing in – confusion between crypto currency and actual traditional currencies.
- Mr A indicated there were other people involved such as a third party.
- Mr A stated he'd been made redundant and was therefore susceptible to a scam.

I considered these points – and as Mr A's advisors will be aware, my role is to make balanced decision based on the evidence I've seen.

And I think Halifax went far enough – they asked a lot of open questions; especially about what Mr A was investing in – whether it was in crypto or traditional currencies. Mr A was evasive about that for some time on the second call.

Mr A also stated that he had been introduced to firm X by a trusted and known friend – this was an important piece of information for Halifax to consider. He also said there wasn't an online introduction (which wasn't the case of course). And Mr A stated he made all the investment decisions when moving money from the crypto exchange – which may not have been the case, but nevertheless, he told Halifax he was in control.

He also told Halifax he hadn't been instructed to open the crypto exchange account – but in Mr A's evidence to us, he stated he had been told to do so. And he stated to Halifax that he'd completed the necessary checks with the FCA website.

So, on the balance of evidence here I think there was enough in the calls for Halifax to feel comfortable that Mr A knew what he was doing, and none of the reasonable questions they asked brought forward enough to suggest he was being scammed.

I also noted that Mr A (through his advisors) said he had no experience of crypto trading. But I can see from his statements that:

- between November 2020 and May 2021, Mr A made 16 crypto related payments totalling more than £42,000 and received crypto income of about £17,000 during the same period.
- he made three further crypto payments for £5,000 in January 2022 to February 2022.
- and he made one crypto payment for £19,500 just prior the scam taking place in November 2022.

So, I don't think it's reasonable to say he was inexperienced.

Therefore, I don't think it is reasonable to ask Halifax to refund any of the money Mr A has lost.

Recovery: We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Halifax took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

And here, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover.

I'm sorry Mrs A and Mr A have had to contact us in these circumstances. I accept they've been the victim of a cruel scam, but I can't reasonably hold Halifax responsible for their loss.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A and Mr A to accept or reject my decision before 20 May 2025.

Martin Lord
Ombudsman