DRN-5708693

The complaint

Mr K complains that Bank of Scotland plc (Halifax) won't refund money he lost when he was a victim of a scam.

What happened

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

In February 2024, Mr K received a telephone call from a person, that we now know to be a scammer, which introduced themselves as being a representative of a genuine cryptocurrency provider, which I will refer to as 'X'. The scammer said he was calling Mr K to help him recover bitcoin assets he had previously invested.

Mr K said he felt the call was genuine as he did have bitcoin assets in a dormant account with X, which he was unable to access as he had forgotten his login details. The scammer then told Mr K he would receive contact from another firm, which I will refer to as 'F', who will help him get his bitcoin investment released. An advisor from F then convinced Mr K to open an account with another financial provider, that I will refer to as 'W', which would be used to receive the funds once the bitcoin was released. Mr K then said the scammer told him he would need to make a series of payments to release the bitcoin.

I understand Mr K made the following payments from his Halifax account as part of the scam. Two payments went directly to a crypto exchange provider, with the rest going to accounts Mr K held with other providers – 'W', 'B' and 'R' – before being forwarded on:

Payment	Date	Type	Payee	Amount
1	29 February 2024	Faster payment	'W'	£5
2	29 February 2024	Faster payment	'B'	£5
3	1 March 2024	Faster payment	'B'	£15,400
4	7 March 2024	Faster payment	'B'	£9,314.96
5	14 March 2024	Faster payment	'B'	£4,299.84
6	24 April 2024	Faster payment	'B'	£1,631.96
7	29 April 2024	Faster payment	Crypto exchange provider	£2,200
8	29 April 2024	Faster payment	Crypto exchange provider	£1,750
9	30 April 2024	Faster payment	'R'	£1,450
10	1 May 2024	Faster payment	'R'	£1,555
11	16 May 2024	Faster payment	'B'	£60

Around late April / early May 2024, Mr K said he realised he had been a victim of a scam and reported the incident to Action Fraud and his banking providers. Mr K has confirmed he has received a refund from B. And as I've addressed in a separate complaint, W have also agreed to issue Mr K with a partial refund.

Mr K raised a complaint with Halifax, which they didn't uphold. In summary, they said:

- The payments to B weren't unusual or out of character for Mr K and so they had no reason to intervene.
- They did stop the payments to the crypto exchange provider and R. They spoke to Mr K to question the payments and provided him with education on tactics scammers use to get customers to send money. They also asked if anybody was helping him or asking him to make the payments, which Mr K denied. This made it difficult to protect him from the scam he was falling victim to.
- If Mr K had explained what the payments were for and how he had been contacted by a third party about a dormant account, they would have been able to explain that he was likely falling victim to a scam.
- Halifax did accept they could have provided better customer service on a call they had with Mr K as they left him on hold for nearly 30 minutes when he called to discuss one of the transactions. So, they paid him £100 as an apology for this.

Our Investigator looked into the complaint but didn't think it should be upheld. In short, she said:

- Halifax should have recognised Payment 3 carried a heightened risk of financial harm from fraud due to the high value and they should have discussed the payment with Mr K. However, even if Halifax had intervened on Payment 3, she wasn't persuaded this would have prevented the loss.
- This was because Mr K had spoken with B, before and during the scam, whereby he was given clear scam warnings specifically relevant to his situation. And also, due to Mr K informing B he was making the payments for investing in stocks and shares.
- Halifax also intervened on 29 April 2024 and spoke to Mr K on two occasions to ask him questions about the payments and provide him with warnings. However, as he provided incorrect information, they were unable to provide warnings relevant to the scam he was falling victim to, so she didn't think Halifax could have done anything else to prevent the scam and wouldn't be asking them to provide any refund.
- The Investigator agreed the £100 compensation Halifax paid for the poor customer service they provided was fair.

Mr K didn't agree, so the complaint has been passed to me for a decision.

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.

Firstly, I've thought about the Contingent Reimbursement Model (CRM) code which can offer a potential means of obtaining a refund following Authorised Push Payment (APP) scams. However, the CRM code doesn't cover payments sent to accounts held in a person's own name, so Mr K's payments are not covered under it. I've therefore considered whether it would otherwise be fair and reasonable for Halifax to refund Mr K.

It's not in dispute that Mr K authorised the payments, and Halifax does have a duty to act on his instructions. But in some circumstances, it should take a closer look at the circumstances of the payments – for example, if it ought to be alert to a fraud risk, because the transaction is unusual, or looks out of character or suspicious. And if so, it should intervene, for example, by contacting the customer directly, before releasing the payments. I'd expect any intervention to be proportionate to the circumstances of the payment.

But I've also kept in mind that banks such as Halifax process high volumes of transactions each day. There is a balance for it to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate.

That said, there's no question Mr K has fallen victim to a cruel and cynical scam. Unfortunately, that alone doesn't mean Halifax has to refund him. Although we now know with the benefit of hindsight that this was a scam, the question I have to consider is, when should Halifax have recognised this, given the information that was available to it at the time.

So, the starting point here is whether the instructions given by Mr K to Halifax were unusual enough - in relation to his typical account activity – to have expected Halifax to have identified Mr K was at risk of financial harm from fraud.

Having done so, I don't think the first two payments were unusual enough for Halifax to have sufficient reason to think he could be at risk of financial harm from fraud due to their low value. However, by Payment 3, I would've expected them to have had concerns Mr K could be at a risk of financial harm from fraud. I therefore would've expected Halifax to have carried out additional checks before processing it. But even if Halifax had reached out to establish the surrounding circumstances of the payment Mr K was making, I'm not persuaded they would've uncovered the scam. I'll explain why.

I've considered Mr K's interactions with both Halifax and B before and during the scam. This includes a conversation the day before the scam begun with B. And in this call, which lasted around 25 minutes, B explained that, as Mr K had recently fallen victim to a scam, he would very likely be targeted again and by the same scammers So, B was keen to explain what kind of tactics the scammers would use. And they mentioned the scammers would call him pretending to be from recovery companies, that specialise in helping customers recover lost crypto. The advisor went onto explain the whole process the scammers generally tend to use, which was very similar to the scam Mr K fell victim to.

A second call with B took place on 26 February 2024, a few days before Mr K made Payment 1 from his Halifax account. Mr K called B and said a payment he was trying to make from his B account to W had been blocked. The advisor explained this was due to its high value. Mr K informed B *"he was making payments in stocks and shares which are regulated, so he doesn't want to keep calling the banks to verify payments".* B went onto explain the checks were only being done to protect him from fraud.

Halifax have also provided us with four calls they had with Mr K between 29 April 2024 and 1 May 2024, when he attempted to make payments 7 and 8 to the crypto exchange provider and Payment 9 and 10 to R. Halifax asked Mr K various questions before the payments were released, including the following:

Halifax: *"Have you opened the wallet yourself? Or has anyone else helped you open it?"*

Mr K: *"No, no, it's my wallet and I have passwords for it and everything else".*

Halifax: *"And no-one's helped you open it, no other third parties and no one else has access to it?"*

Mr K: *"No, no".*

Halifax: *"What's happening with some of these is, the fraudster is claiming to be from the likes of these places and they'll take remote access to your computer and set up a digital wallet, you move the money into it and they pinch it".*

Halifax: *"Have you received any calls from anyone pretending to be from another company? "Did someone contact you about this opportunity?"*

Mr K: *"No".*

Halifax: *"Why are you making the payment?"*

Mr K: *"sending money to my own crypto account and* [I]*wasn't being instructed to make the payments by anyone else".*

Across the calls Mr K was provided with various crypto investment scam warnings, as well as scam warnings about other types of scams that are common, such as impersonation scams, job scams etc.

For the reasons mentioned above, while I think Halifax ought to have taken additional steps before processing Payment 3, I'm not persuaded that even if Halifax had done this it would've deterred Mr K from making the payment or those that followed. I think the conversations Mr K had with B and Halifax demonstrate that he wasn't willing to disclose the true circumstances of why he was making the payments – specifically that a third-party recovery firm was directing him to make payments to release crypto held in a dormant account. I appreciate Mr K may have been under the scammer's spell, but I don't think I can reasonably hold Halifax responsible for that. And due to Mr K not providing accurate information, they were prevented from uncovering the scam and providing relevant warnings to his situation.

Nevertheless, even if Halifax had provided a scam warning tailored to crypto recovery scams, I'm not persuaded this would've made a difference. This is because Mr K received such a warning the day prior to the scam occurring from B. So, it should've been at the forefront of his mind and resonated enough with him to have realised the contact he received from X and F wasn't genuine.

Because of this, I don't think Halifax is responsible for the loss Mr K suffered.

I've also thought about whether Halifax could've done anything to recover Mr K's loss when the scam was reported. But Halifax could've only sought to recover them from accounts in Mr K's name. And given Mr K 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 Mr K's own accounts. I therefore don't think Halifax could've recovered Mr K's funds.

Regarding the £100 compensation Halifax has paid, I agree the amount is fair and reasonable to recognise the inconvenience Mr K experienced for being put on hold for nearly 30 mins. So, I'm not increasing this further.

Although, I am sympathetic to Mr K's situation as I realise, he's suffered a significant financial loss, it would only be fair for me to direct Halifax to refund him if I thought the bank was responsible for his loss – and I'm not persuaded that this was the case. For the above reasons, I don't think Halifax could've reasonably prevented Mr K's loss.

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 Mr K to accept or reject my decision before 28 August 2025.

Israr Ahmed
Ombudsman