DRN-5811012

The complaint

Mr A complains that Bank of Scotland plc trading as Halifax are refusing to refund him the amount he lost as the result of a scam.

Mr A is represented by a firm I will call "W".

What happened

In June 2024, Mr A came across an advert online promoting an investment opportunity. After completing a form, Mr A was contacted by a representative of a company, who I will refer to as the scammer. Mr A carried out some research and following that, decided to invest.

On 20 September 2024, Mr A sent several payments from his credit card to a cryptocurrency platform account held in his own name, totalling over £3,000. Initially Mr A saw a profit being made, and it was only when he wanted to withdraw funds that he experienced issues, with the scammer telling him he needed to pay various different fees. It was then he realised he had been scammed.

W complained to Halifax on behalf of Mr A, who said that as the payments were authorised and made to the cryptocurrency platform before being sent on, there was no fraud linked to them. Halifax said they provided scam education to Mr A and he continued to authorise the payments. Because of this, they weren't willing to reimburse any of the funds lost.

Mr A remained unhappy and so W referred his complaint to our service. Our Investigator looked into the complaint, along with two others connected to it, and ultimately found that while Halifax could have done more to try and stop the scam from progressing by speaking with Mr A directly, he didn't think any further intervention would have worked. He explained that as the payments were made by credit card, the money had been borrowed from Halifax.

As Mr A has also borrowed from other lenders as well as family members, our Investigator was of the view that even if Halifax had prevented the payments from being made, Mr A would have borrowed funds from elsewhere. As Mr A was so heavily under the spell of the scammer, our Investigator didn't feel any further intervention would have been successful in uncovering the scam. He noted that when Mr A wasn't able to send money with one provider, he tried another, meaning it was more likely that, had any further intervention taken place, he would have continued to mislead the firms involved, or would have found another way to make the payments.

W disagreed and so the case has been passed to me for a final 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.

I'm very aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied 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 simply reflects the informal nature of our service as a free alternative to the courts.

When deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Where the evidence is incomplete or missing, I am required to make my findings based on the balance of probabilities. In other words, what I consider is most likely to have happened given the information available to me.

As a starting point in this case, Mr A doesn't dispute that the payments were made in line with his instruction to Halifax to make them.

In broad terms, the starting position at law is that a firm such as Halifax is expected to process payments and withdrawals that a customer authorises them to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

That means in the first instance Mr A is presumed liable for the payments. Halifax would not ordinarily have any responsibility for a loss incurred through the payments – provided they carried out the instructions correctly. And here, there is nothing that leads me to believe they didn't do so.

I'm really sorry that Mr A has lost such a large sum of money, but this doesn't automatically entitle him to a refund. It would only be fair for me to tell Halifax to reimburse Mr A if I thought they reasonably ought to have prevented the payments, or they unreasonably hindered recovery of the funds.

Prevention

Businesses have various and long-standing obligations to be on alert for fraud and scams and to act in their customers' best interests. So, a first consideration in determining Halifax's obligations here would normally be: should they ought reasonably to have held any suspicions or concerns in relation to the payments, and if so, what might have been expected from a proportionate intervention.

In this case, I'm satisfied Mr A authorised the relevant payments, and as explained above, Halifax would generally be expected to process payments a customer authorises them to make.

That said, as a matter of good industry practice, they should have taken proactive steps to identify and help prevent transactions – particularly sufficiently unusual, uncharacteristic or suspicious transactions – that could involve fraud or be the result of a scam. However, there are many payments made by customers each day and it's not realistic or reasonable to expect a business to stop and check every payment instruction. There's a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

In this case, having considered the circumstances of the payments Mr A made, I agree that Halifax should have intervened, given there were so many made to the same account in quick succession on the same day. Halifax would have known the payments were going to a cryptocurrency platform and therefore would have been on alert knowing that type of payment carried a higher risk than others.

But for me to find it reasonable that Halifax should refund the payments requires more than me finding that they should have intervened/probed further. This is because legitimate payments can also be large, and made to cryptocurrency platforms, which doesn't always mean the money is being lost to fraud or a scam.

For me to ask Halifax to refund the payments, I would need to be satisfied that not only did they fail to intervene sufficiently, but had they intervened in a way that we would expect, the loss would have been avoided.

So, as I have touched on above, I have thought about whether appropriate intervention or questioning would likely have made a difference. Ultimately, I don't think any intervention by Halifax would have made a difference or prevented the payments from being made here. I will explain why.

The investment wasn't one that Halifax were recommending or endorsing. Their role was to make the payments that Mr A asked them to make, as he had already made the decision to invest, based on what he had been told and the research he had carried out before making the payments. And while there are now concerns about who he invested with, I must consider what Halifax could have established, had they spoken to Mr A about his payments at the time they were made. Ultimately, I don't think I can fairly say that they would have been able to give Mr A any information that would have led him to doubt what he was doing.

Given the amounts he was sending, and the quick succession, I believe Halifax should have discussed things with Mr A in more detail during a phone conversation. During a call they could have asked him open and probing questions about the payments, especially why they were all being made in smaller amounts to the same account in such quick succession. This could have stopped Mr A from making any further payments, as it may have been hard to explain why he was making so many so quickly. However, he was heavily influenced by the scammer and so it is also highly likely that he could have provided a cover story in order to reassure Halifax and get the payments through.

But for the sake of completeness, even if Halifax had probed further and stopped Mr A from making any further payments, I don't think they could have uncovered the scam and prevented any overall loss. I also don't think Mr A would have taken on board any warnings Halifax may have provided. I'll explain why.

Mr A looks to have been heavily influenced by the scammer. I have read through the conversations that took place and can see that Mr A placed a high level of trust in the scammer and followed their instruction. Mr A followed the scammer's guidance on how to make the payments, he gave the scammer full access to his system via a remote access application, and made sure he always waited for the scammer's guidance before doing anything. I therefore find it most likely that even if Halifax had intervened, Mr A would have been coached on how to proceed with the payments, and even if they had stopped the payments he was making, I believe it is most likely he would have found another way to make them.

I say this because Mr A took out loans to fund the scam and also borrowed money from family members. He also has complaints set up with other providers, who he used to make payments to the same scammer. These providers also intervened, and Mr A provided misleading answers to the questions he was being asked.

A firm I will call "M" spoke with Mr A on 19 September after they blocked his card, where he was told that cryptocurrency payments weren't usually allowed on credit cards, to which he said he didn't mind. He was sent scam education by SMS, and was advised to visit M's website, but was happy to go ahead with the payment. After his card was unblocked, Mr A was told to wait 15 minutes before making further payments, but to avoid making cryptocurrency payments. Mr A acknowledged this but went on to make multiple payments to his cryptocurrency platform.

A firm I will refer to as "V" spoke to Mr A multiple times, where he misled them with the answers he gave to their questions. During a call, when asked about a payment he was making, Mr A said that nobody was coaching him, that he was paying for building work to be

carried out, that the company was legitimate and that he knew them personally, and didn't find them on social media.

On 25 September during another call with V, Mr A said he was paying one of his own accounts, not an investment one, that the firm was legitimate, and that he hadn't downloaded any apps or software. On 16 October, Mr A said he was making a payment as he was looking to buy a property abroad, and on 29 October, he said he was making a payment to purchase educational software. In a call made on 30 October, Mr A once again said he was making a payment as he was looking to buy a property abroad.

While making payments through a provider I will call "R," Mr A was asked whether anyone was telling him what to say or assisting him with payments. He said no, and that he was completing the transactions by himself. He also could have told R that he was moving funds to an investment account, but instead chose a different reason, and he also said he hadn't been asked to download any software. When asked if he'd also recently opened any other online accounts, including investment account and platforms, he said he hadn't.

During a live chat with R, Mr A also said he wasn't planning on sending the funds anywhere else once they reached his cryptocurrency platform. Mr A's account with R was later restricted and then closed on 27 September. Following this, Mr A proceeded to make payments via other providers.

Mr A also made payments with a provider who I will call "S." When S intervened on one payment, Mr A said he was making a payment for an invoice towards a company which was helping build services for a business project, and the payment was for a business relationship. Mr A was asked to provide an invoice, which he was able to do. Because of this, S allowed the payment to go through. When Mr A attempted another payment a few days later on 28 October, S deactivated his account as they considered it high risk, and an email was sent letting Mr A know the closure was because he was at high risk of being scammed.

So having considered everything in detail, while I believe Halifax should have done more, I don't believe any intervention would have made a difference, given the level of control the scammer held over Mr A, and the lengths he went to in order to get the payments through with Halifax, but multiple other providers as well.

Recovery

I've also looked at whether Halifax took the correct steps once Mr A contacted them to dispute the payments.

The only method of recovery Halifax had for the payments made by card was to request a chargeback. However, Mr A didn't make the payments to the scammer directly, he paid a cryptocurrency platform. The service provided by that platform would have been to convert or facilitate conversion of Mr A's payments into cryptocurrency. The fact that the cryptocurrency was later transferred to the scammer doesn't give rise to a valid chargeback claim against the merchant Mr A paid. Ultimately, the cryptocurrency platform provided the requested service to Mr A.

Having carefully considered everything overall, I don't find that Halifax could have reasonably prevented the loss Mr A incurred. In saying this, I don't underestimate the impact on Mr A as he has lost such a significant amount of money which has left him in a vulnerable position. I am really sorry he fell victim to such a cruel scam – he is not at fault here, the scammer is.

However, it is simply the case that I don't consider I can fairly and reasonably hold Halifax liable for his 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 A to accept or reject my decision before 23 March 2026.

Danielle Padden
Ombudsman