DRN-4557567

The complaint

Mr K has complained that Bank of Scotland Plc (trading as "Halifax") didn't protect him from falling victim to a cryptocurrency-related investment scam.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mr K explains that between September and November 2021 he made payments totalling over £100,000 from his Halifax account to a cryptocurrency exchange, which was ultimately related with a scam. He says that Halifax failed to contact him to establish the reasons for the payments, and the scam therefore wasn't uncovered.

Mr K was contacted by an individual ("the scammer") on a popular messaging app after he downloaded a cryptocurrency investment app. The scammer encouraged Mr K to open an account with a cryptocurrency exchange platform, which he did, and he then made several payments from his Halifax account to his cryptocurrency account. Mr K was then persuaded to convert the pounds he'd sent from Halifax into cryptocurrency, and then forward it on to the scammer, under the belief that he was funding an investment. Mr K says he was given access to what appeared to be a sophisticated trading platform, which persuaded him that the payments he was making were being used to fund legitimate investments.

After he'd made several payments to it, Mr K's account at the cryptocurrency exchange platform was closed. Mr K was advised by the scammer to open a different account, with another bank, in order to continue trading. Mr K did this and sent further payments to that account totalling £29,500, of which £29,000 was sent on to the scammer.

The payments Mr K made as part of the scam were as follows:

	Date	Amount (£)	Recipient
1	06/09/2021	1,500	Crypto exchange
2	10/09/2021	1,000	Crypto exchange
3	15/09/2021	5,000	Crypto exchange
4	22/09/2021	10,000	Crypto exchange
5	27/09/2021	9,200	Crypto exchange
6	27/09/2021	4,900	Crypto exchange
7	28/09/2021	5,000	Crypto exchange
8	29/09/2021	5,000	Crypto exchange
9	08/10/2021	8,000	Crypto exchange
10	08/10/2021	9,000	Crypto exchange
11	*15/10/2021*	*10,000**	*Crypto exchange*
12	*15/10/2021*	*9,500**	*Crypto exchange*
13	18/10/2021	100	Other bank account
14	18/10/2021	19,400	Other bank account

15	27/10/2021	10,000	Other bank account

*these payments were returned as Mr K's cryptocurrency account had been closed

Mr K realised he'd been scammed when he was told he needed to make a further deposit into his cryptocurrency investment before he could make a withdrawal.

Mr K made a complaint to Halifax. Halifax didn't uphold the complaint; in its response it said that the payments Mr K made were in line with the general spending on his account, so it didn't have sufficient cause to be suspicious of what was happening. It also said it had showed Mr K an appropriate warning related to scam investments, but Mr K had decided to proceed to make the payments regardless. Mr K remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. He explained that he thought Halifax's had provided warnings to Mr K. He also explained that he didn't think the payments Mr K made were particularly out-of-character when taking into account the way Mr K had used his account in the months preceding the scam.

As Mr K didn't accept the investigator's opinion, the case has been passed to me to make 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.

I'm sorry to disappoint Mr K but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr K authorised these payments from leaving his account. It's accepted by all parties that Mr K gave the instructions to Halifax and Halifax made the payments in line with those instructions, and in line with the terms and conditions of Mr K's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I've firstly considered the activity on Mr K's account in the months preceding the scam payments, to establish whether Halifax should've been concerned about a change to the way Mr K was using his account.

I can see that in March 2021 Mr K made a payment of £6,314.10, and in August 2021 he made three payments of £25,000 each, and one of £10,000.

The payments Mr K made as part of the scam to the cryptocurrency exchange ranged in size from £1,000 to £10,000. So I think it's fair to say that they weren't entirely out-of-character when considered alongside the payments Mr K had made previously. They were also made to the same payee, and spaced out over almost two months, which isn't typical of what's seen in scams.

Halifax says it asked Mr K for the reason for the payment when he initially created the payee, and it showed him a warning before making the first payment which it says was

directly relevant to the reason Mr K gave. Halifax has provided a copy of this warning which says:

“Make sure this investment is real. Deals that look too good can be scams. Do lots of research - good deals don't find you. See what your friends and family think. Use the FCA to check an advisor or company. People who invest without checking are typically scammed £14,052. Fraudsters can send or advertise tempting offers to make money. Only invest with a company who are allowed to offer products and services. The FCA site can help you check. Find out how to stay safe from scams on our Fraud Hub."

It then gave Mr K the option to continue with the payment, or to cancel it, and Mr K continued to make the payment.

Following this warning, when Mr K made payments three to five, and then seven to ten, Halifax showed Mr K a different warning, and he again had to choose whether to proceed with the payments or cancel them each time. This warning read:

"Be sure that you know who you're sending money to. Please check the account details with a trusted source. Fraudsters invent persuasive reasons to get you to make a payment. See all the latest scams fraudsters use on our fraud hub page. Failure to take precautions before you make your payment could mean we are not able to get your money back in the event of fraud. What do you want to do?"

On all occasions Mr K chose to proceed and Halifax processed the payments in line with Mr K’s instructions.

Having considered these warnings, I’m satisfied that they were proportionate to the circumstances of the payments. The wording was clear and unambiguous and gave Mr K specific guidance on how to protect himself from scams, and Mr K chose to proceed with the payments. Whilst I do note that Halifax didn’t show a warning for payments two and six, I don’t think that made a difference in this case. On the basis that Mr K had chosen to proceed each time he was given a warning, and had to actively choose to proceed, I don’t think Halifax showing a warning for the other payments would’ve made a difference, and I don’t see any reason to suggest that Mr K would’ve taken more notice or acted differently on those occasions.

It’s worth bearing in mind that in some cases it might not be proportionate for a business to intervene by just showing on-screen warnings, where there’s a payment pattern such as this one. But given Mr K’s overall account history, in this case, I think the on-screen warnings were proportionate. I also note that Mr K also received a payment from this payee around a week after he first made a payment to it – so I think it was fair for Halifax to assume Mr K trusted the payee, and not to intervene any more than it did.

The payments Mr K made to his own account at the other bank were for £100, £19,400, and £10,000. I can’t see that Halifax asked Mr K for the reason he was making those payments, nor did it show him any warnings before they were processed.

However when taking into account the previous activity that I’ve mentioned both before the cryptocurrency payments, and the cryptocurrency payments themselves, the scam had, to some extent, normalised transactions of this size. Whilst there’s no doubt that the transactions Mr K made were large, and had an even larger cumulative value, when considering them in the broader context of Mr K’s account activity I can’t say they stood out as particularly unusual or suspicious, especially as they were going to an account in Mr K’s own name.

This, plus the fact that the payments were spread out over several days, means I don't think it was negligent for Halifax to follow Mr K's instructions and process the payments he asked it to, without intervening further beforehand.

In reviewing the allegations against Halifax it was fair for me to consider whether – if at all – Mr K could've done anything to prevent his losses. I'd like to start by reassuring Mr K that I've carefully reviewed everything he's provided, including the extensive chat history he had with the scammer, and there's no doubt he's the victim here.

But despite the scammer's professional and knowledgeable communications, I haven't been made aware that Mr K did any further checks on the investment he was allegedly making. It's also not apparent that he was dealing with – or told he was dealing with – an individual qualified to give investment advice. In addition, it's unusual to have to make further payments or investments in order to withdraw the proceeds of an investment, so I think this should've been something that Mr K questioned before making the additional payments that he was told to make. With this in mind, I also think it's fair to say that Mr K could've done more to protect himself from this financial harm.

I do recognise that Mr K has drawn likeness between his complaint and one of the case studies on the Financial Ombudsman Service's website, so he believes Halifax should be held responsible for his losses. But I'm afraid that complaints often have many individual features that differentiate them, and whilst some scam cases may appear similar on the surface, the individual factors will nearly always differ, and that's the case here.

Mr K has also mentioned the Payment Systems Regulator's new rules in relation to Authorised Push Payment scams, introduced in October 2024. These rules only apply to scam-related payments made on or after 7 October 2024, so they don't apply to Mr K's complaint.

Finally, I've seen Mr K's comment that due to Halifax's recent profits it should prioritise refunding customers who've been victims of scams. But I'm afraid Halifax's financial position doesn't affect my judgement on what's fair, so that doesn't change my thinking in this case.

Recovery of the funds

I've seen that Halifax contacted the receiving banks in an attempt to recover the funds Mr K sent as part of the scam.

But as the funds had been made available to Mr K and he'd used them to purchase cryptocurrency, Halifax wasn't able to recover anything to return to Mr K, as he'd effectively spent the money he sent. So there's nothing more Halifax could or should've done here.

I'm very sorry that Mr K has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Halifax responsible for that.

My final decision

I don't uphold Mr K's complaint against Bank of Scotland Plc, trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 17 December 2024.

Sam Wade

Ombudsman