

The complaint

Mr and Mrs E complain that Bank of Scotland plc, trading as Halifax ('Halifax'), hasn't refunded all the money they lost after Mr E fell victim to a scam.

Although funds were sent from a joint account, it was only Mr E who made the scam payments. So, for ease, I'll refer only to Mr E throughout the remainder of my decision.

What happened

The circumstances of the complaint are well known to both parties, so I don't intend to repeat these in detail here. However, I'll provide a brief summary of what's happened.

In March 2023, Mr E was contacted by a third party ('the scammer') about an employment opportunity. The premise of the job was that Mr E would need to complete online tasks reviewing holidays. In return, he would be paid commission for completing sets of tasks.

Each time Mr E completed a set of tasks, he was required to make refundable deposits, in order to unlock new tasks and to receive his commission. Whilst initially Mr E received his deposits back with the commission he earned, he started being asked to make larger payments, whilst he was prevented from withdrawing any further funds. The payments continued until Mr E ran out of money. It was at this time that Mr E realised he'd been the victim of a scam and reported the situation to Halifax.

From his Halifax account, Mr E made, or attempted to make, 22 payments relating to the scam. Some of the payments were sent from Halifax to the scammer via Mr E's own accounts with other regulated firms. Other payments were sent from Halifax to the scammer via Mr E's own digital wallets with cryptocurrency exchange platforms. The remaining scam payments were sent from Halifax directly to third parties.

Halifax agreed to reimburse the payments that were sent to third parties. However, it declined to reimburse the payments that Mr E sent to his own accounts or digital wallets. Unhappy that Halifax wouldn't refund all the payments he'd sent, Mr E referred his complaint to our service.

Our Investigator didn't uphold Mr E's complaint. They thought that Halifax had missed an opportunity to question Mr E about a large payment to a cryptocurrency exchange platform. However, our Investigator wasn't of the opinion that proportionate intervention from Halifax would've prevented Mr E from going ahead with that payment, or the subsequent payments.

They further explained that Mr E had expressed doubts to the scammer on multiple occasions and had always been persuaded to continue making the scam payments. Our Investigator also didn't think Mr E would've been honest with Halifax if questioned about the payments and so Halifax wouldn't have been able to uncover the scam and prevented the loss.

Mr E didn't agree. He thought that proportionate intervention from Halifax would've reinforced his concerns about what he was doing and given him enough doubt to stop making payments.

As an agreement couldn't be reached, the complaint has been referred 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.

In 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 have been good industry practice at the time.

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

It's not in dispute here that Mr E made the scam payments himself and authorised Halifax to send the funds. So, under the Payment Services Regulations, the starting position here is that Mr E is responsible for the payments (and the subsequent loss) despite the payments being made as the result of a scam.

However, that isn't the end of the story. Good industry practice required that Halifax be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

Between 16 March 2023 and 19 March 2023, Mr E made:

- three debit card payments (for £20, £50 and £100) to a cryptocurrency exchange platform – which I'll refer to as 'C';
- two faster payments (for £10 and £50) to C (which were rejected and returned by C);
- a faster payment (for £700) to his own account with another bank – which I'll refer to as 'S'; and
- two faster payments (for £850 and £3,000) to his own account with an electronic money ('e-money') provider – which I'll refer to as 'W'.

I don't think there was anything particularly unusual or suspicious about these payments and I wouldn't have expected Halifax to have intervened when these payments were made. As a result, I'm not of the opinion that Halifax reasonably ought to have identified a fraud risk in the circumstances. So, I'm not recommending Halifax needs to refund any of those payments.

Mr E then went on and also made a £6,900 faster payment to W on 19 March 2023. The value of this payment was out of character for Mr E. It was the second payment to W within the space of 35 minutes and significantly larger than the first. It also took the total sent to W (a newly created payee), within a 24-hour period to almost £11,000.

Whilst Mr E still had a considerable balance in his account, I think there were warning signs that Mr E could've been at risk of financial harm from fraud and as a result, I think Halifax ought to have intervened and spoken to Mr E about what he was doing. So, I've thought about whether human intervention would've likely resulted in the scam being identified.

I can't say for certain what would've happened if Halifax had intervened (because it didn't question the scam payment). So, I must consider whether the available evidence shows that it was more likely than not that Mr E would've acted differently.

Throughout the scam, Mr E was in constant contact with the scammer. He was being heavily coached on what he was doing, such as being told which accounts or digital wallets to open, how to deposit funds and move these on. He also received advice on what to say when his accounts or digital wallets were restricted by the providers. If Halifax had blocked the £6,900 payment to W on 19 March 2023 and asked Mr E to call, I think on balance Mr E would, more likely than not, have told the scammer and followed their advice on how to get the payment approved.

I say this because when W restricted Mr E's e-money account, he spoke to W about when his funds would be returned. At no point in that call did Mr E disclose what he was making the payments for. Mr E also spoke to Halifax on two occasions. Again, Mr E didn't disclose the true purpose of the payments and misled Halifax about the reason he was buying cryptocurrency. Finally, Mr E wasn't truthful with S when it asked him questions about one of the scam payments.

This demonstrates that Mr E was prepared to lie to Halifax (and other financial institutions) about what he was doing and that he intentionally misled them to hide the true purpose of the payments he was making.

The scam lasted for approximately seven weeks. During this time, Mr E expressed his concerns about what he was being asked to do – and he did this on multiple occasions. However, the scammer was always able to persuade Mr E to continue following their instructions.

On 29 April 2023, Mr E said to the scammer:

"I am speaking with the bank currently and they have told me that this is definitely a scam and I have lost all the money I have put in."

The scammer said Mr E just needed to make one final payment and he would be able to withdraw his funds. Mr E said:

"They (the bank he was speaking to) tell me that is what everyone is told."

Despite this, Mr E made a further scam payment, moving funds from Halifax to S, before sending the funds from S to a third party. Mr E wasn't provided with a plausible or convincing explanation for why he should ignore the advice he'd received that he was being scammed. He simply followed the scammer's instructions.

Taking all this into consideration, I'm not as persuaded as I'd need to be that Halifax would've uncovered the scam if it had questioned the £6,900 payment to W on 19 March 2023. And I'm also not persuaded that Halifax would've been able to prevent Mr E from making the payment.

Between 12 April 2023 and 17 April 2023, Mr E made four payments to his digital wallet held with C, totalling £20,800. He also made a £5,300 payment to C which was rejected and returned to him. Given the amounts and frequency of the payments going to a cryptocurrency exchange platform, I'd have expected Halifax to question the payments, but Halifax also failed to identify this suspicious activity.

Halifax did question some later payments to a different cryptocurrency exchange platform and spoke to Mr E on two occasions. The scammer told Mr E:

"No matter what questions your bank asks you, you will need to tell your bank that you are buying cryptocurrency."

Mr E proceeded to tell Halifax that he was buying cryptocurrency to purchase assets in Gambia (where he was living at the time) from companies that used cryptocurrency as it was preferable to using fiat currency due to better exchange rates. He also said he was buying cryptocurrency to make a profit to help with his rising living costs.

It seems likely therefore, that if Halifax had questioned the payments Mr E was making to C that he wouldn't have been honest and would've likely responded in a similar way. I don't find his reasons for buying cryptocurrency to have been particularly convincing and I'd have expected Halifax to have been concerned that Mr E might be falling victim to a cryptocurrency investment scam.

In those circumstances I'd have expected Halifax to have provided education and warnings around cryptocurrency investment scams. But I don't think Halifax would've been able to uncover Mr E was falling victim to a job-task scam and therefore any cryptocurrency investment scam advice is unlikely to have resonated with him at the time those payments were made.

On 23 April 2023, Mr E made two faster payments, of £5,000 each, to a new payee. Again, I don't think Halifax identified that this was unusual behaviour for Mr E, and it should've intervened to question him about the payments. But, as I've explained above, I don't think Mr E would've been honest with his answers if questioned and this would've prevented Halifax from identifying he was falling victim to a job-task scam. In any event, Halifax has refunded these two payments in full.

Between 22 April 2023 and 27 April 2023, Mr E made four payments to two cryptocurrency exchange platforms. As I've discussed above, two of these payments were blocked and Halifax spoke to Mr E. I don't think the intervention was good enough, but for the reasons explained above, I don't think Halifax would've been able to prevent Mr E from making those payments.

On 28 April 2023, Mr E made a £3,000 faster payment to another new payee. In the circumstances, I'd have expected Halifax to have asked the purpose of the payment and provided a written scam warning based on Mr E's answer. I've seen no evidence that Halifax did provide a warning, but Halifax has already refunded this payment in full.

On 29 April 2023, Mr E moved £3,500 from his account with Halifax to his account with S. From there, Mr E sent the funds to the payee he paid from Halifax on 28 April 2023. S has already refunded 50% of that payment. I've thought about whether Halifax should be held responsible for the remaining 50% and I'm not persuaded that Halifax should reimburse any of the funds that were sent to the third party via S.

Prior to the movement of funds from Halifax to S, Mr E has explained that he was told by a bank that he had fallen victim to a scam. However, Mr E ignored that advice and continued to make a final payment to the scammer. Mr E hadn't been able to withdraw any funds for approximately seven weeks, despite repeatedly being told he would be able to after one more payment and sending thousands of pounds to the scammer.

In the circumstances, I think Mr E was contributorily negligent and so, even if I thought Halifax was at fault for allowing funds to be moved to S, I think Mr E should fairly be held equally responsible for the loss and therefore he isn't entitled to any further reimbursement beyond the 50% already refunded by S.

Throughout the scam, Mr E was sceptical about whether he was dealing with a legitimate business. Despite his concerns, he continued to make payments as requested by the scammer and I don't think he took much convincing or persuading to follow their instructions.

In my opinion, Halifax didn't meet its expectations given the concerning account activity. However, I don't think the loss could've been prevented even if Halifax had intervened where necessary and asked proportionate questions, as I'm not persuaded Mr E would've been honest with his answers or that he would've followed appropriate scam education. As a result, I don't think Halifax can fairly be held responsible for refunding Mr E's remaining loss.

I've thought about Halifax's actions once it was aware of the scam. It refunded the three faster payments Mr E made to third parties. The remaining scam payments were sent to Mr E's own accounts or digital wallets with other providers. As such, there was nothing Halifax could've done to recover those funds, as they were either still in Mr E's control, or had already been sent to the scammer.

Some of the scam payments were cryptocurrency purchases made using Mr E's debit card. So, Halifax could've attempted a chargeback to recover those payments from the merchants.

However, as there's been no suggestion made that Mr E didn't receive the cryptocurrency he purchased, I think a chargeback would've likely been defended by the merchants. So, as a chargeback would've had no reasonable prospect of success, I don't find that Halifax did anything wrong by not attempting this in the circumstances.

My final decision

I appreciate Mr and Mrs E have lost a significant amount of money to a cruel scam, orchestrated by someone Mr E thought he could trust. Whilst I have every sympathy for Mr and Mrs E, for the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E and Mrs E to accept or reject my decision before 28 March 2025.

Liam Davies
Ombudsman