DRN-5167696

The complaint

Mr C has complained that Bank of Scotland plc (trading as "Halifax") failed to protect him from falling victim to an impersonation scam and hasn't refunded the money he lost.

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 C has used a professional representative to refer his complaint to this service. For the purposes of my decision, I'll refer directly to Mr C, but I'd like to reassure Mr C and his representative that I've considered everything both parties have said.

Mr C has explained that in November 2023, his home was affected by severe weather, leading to water flooding into his property. As he was concerned about the potential cost of repairs, he applied for a loan online with a company that I'll refer to as "Z". But after a professional assessed the damage, Mr C was told that no major repairs were needed. To avoid paying interest, he decided to return the loan to Z early.

When Mr C searched online for information about repaying the loan, he visited Z's website and found a section where he could speak to someone about the process. He's explained that around the same time he received an email and then a phone call from an individual ("the scammer") claiming to work for a company called GDPR. Mr C says this individual told him that GDPR was a holding company for Z, based in Canada.

The scammer convinced Mr C that any returned funds had to go through their head office in Canada and that the transfer had to be done in cryptocurrency. He was told this would be an instant transfer, whereas a traditional bank transfer would take several days and incur a fee. The scammer guided Mr C through the process using remote access software.

Mr C received emails from the scammer that included FCA and FSCS logos, which he says made them appear legitimate. This, as well as the fact the scammer spoke in a professional and knowledgeable manner further reassured Mr C that he was dealing with a genuine financial institution on behalf of Z.

The scam firstly involved Mr C making eleven payments, over the course of around a week, from his Halifax account to two legitimate cryptocurrency platforms as bank transfers and using his debit card. Once the funds reached the cryptocurrency platforms Mr C was instructed to convert them into cryptocurrency, and to then forward the cryptocurrency to wallets directed by the scammer, under the guise of repaying his loan.

The payments Mr C made in relation to the scam were as follows:

	Date	Amount	Description
1	21 November 2023	£10.10	Bank transfer

2	21 November 2023	£505	Bank transfer
3	22 November 2023	£2,020	Bank transfer
4	22 November 2023	£986.37	Bank transfer
5	24 November 2023	£1,800	Bank transfer
6	27 November 2023	£600	Bank transfer
7	27 November 2023	£959.50	Debit card payment
8	27 November 2023	£1,515	Debit card payment
9	27 November 2023	£1,909.38	Debit card payment
10	29 November 2023	£131.30	Debit card payment
11	29 November 2023	£404	Debit card payment
	Total	**£10,840.65**	

Mr C describes the experience as feeling like he was dealing with a professional organisation. He says he only realised it was a scam when the scammer became aggressive and threatening after he refused to send further money. At that point, he reported the matter to Z and asked for it to be escalated to Halifax. Z informed him that it was investigating the situation.

Mr C made a complaint to Halifax on the basis that the transactions seen throughout the scam were completely out of character for him. He says he had never sent money via cryptocurrency before, and his account was mainly used for bill payments and standing orders. He further explained that during the period a significant amount of money was moved between accounts and then transferred out, which was a very unusual pattern of activity for him and had the hallmarks of a scam. He also said that as an 81-year-old customer, he was clearly vulnerable and confused about the situation. Mr C said that Halifax should have identified the payments as suspicious and acted to prevent the scam from taking place.

Halifax upheld Mr C's complaint and refunded half of what he lost in the scam from payment three onwards, plus interest. It explained it had repaid half of Mr C's losses from that point as opposed to the full value to take into account the negligence it said Mr C had showed by making the payments to the scammer without a reasonable basis to believe he was dealing with a legitimate organisation. Halifax also paid Mr C £50 compensation as an apology for not getting things right when it should have.

Mr C didn't agree with the way Halifax had dealt with things so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained she thought that the refund Halifax had offered was fair. She explained there was nothing to suggest the first two payments Mr C made were particularly high risk, or for cryptocurrency. She also said the first two payments were in line with the normal activity on Mr C's account – so she thought it was reasonable Halifax stepped in at payment three, and when it did, it was right to speak to Mr C by phone.

Finally, the investigator found that it was reasonable for Halifax to hold Mr C jointly responsible for his losses, as he wasn't entirely honest with it when he spoke to it about the payments. She noted he'd been using his cryptocurrency accounts for some time, and she didn't agree that his age made him vulnerable, nor did she believe that when he told Halifax he was buying Christmas presents instead of purchasing cryptocurrency, that's what he genuinely believed he was doing.

As Mr C 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 C 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 C authorised these payments from leaving his account. It's accepted by all parties that Mr C 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 C'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.

Should Halifax have intervened before Mr C made the payments?

In thinking about whether Halifax ought to have intervened before Mr C made the payments, and at which point, I've started by considering his account activity in the six months prior to the scam taking place. As a starting point, this would've given Halifax an idea of what Mr C's normal account usage looked like, so that it could decide what was out-of-character and take appropriate action.

In May 2023 Mr C made a payment of £530 to a cryptocurrency platform, and one for £800 to another financial institution. In July 2023 he made a payment of £850 to the same company, as well as one for £900 to another person. And in August and October 2023 he made three payments to two different cryptocurrency platforms with values of £350, £250 and £100 respectively.

With this in mind, I don't agree with Mr C's complaint point that the transactions in this scam were the first cryptocurrency-related payments he'd made.

Keeping in mind the value of the payment, plus the fact that it was being made to an identifiable cryptocurrency platform, alongside the aggravating factor of Mr C's age which could've made him more susceptible to cryptocurrency scams, it was proportionate for Halifax to use a human intervention, as opposed to giving him an on-screen or automated scam warning.

How did Halifax intervene?

Halifax blocked payment three and told Mr C it needed to speak to him by phone before the payment would be released. Mr C phoned Halifax, where he had a brief conversation with the fraud team, who referred him to a Halifax branch. This process involved two phone calls and I've listened to both calls, and provided a summary of them below.

The first call began with Halifax carrying out security verification. The representative then explained that a scam check had been triggered due to concerns about the payment Mr C was making and advised him that he needed to visit a branch to complete some further

checks. Halifax clarified that the visit didn't need to be immediate, but Mr C responded that he was working on something and wanted the payment cleared as quickly as possible.

Halifax then proceeded to explain the process, detailing what Mr C needed to take to the branch and what he should say when he arrived. However, no further discussion took place about the potential scam risks or the reasons behind Halifax's concerns. The call ended without any additional probing or warnings about the nature of the payments Mr C was trying to make.
The next day Mr C visited the branch and spoke to one of the members of staff. It appears the member of staff was required to call Halifax's fraud team whilst Mr C was present, so the second call I've listened to took place between two Halifax members of staff.

During the call, Halifax asked Mr C where a recent credit of £10,000 had come from. He confirmed it was from Z, explaining that he had taken out the loan due to concerns about storm damage to his property. He went on to explain that as he no longer needed the money, he wanted to repay it. Halifax questioned where he was sending the funds, noting that the payment details didn't appear to be linked to Z, but instead to a cryptocurrency platform. When asked where he had got the payment details from, Mr C avoided answering directly and instead stated that he hadn't yet attempted to send the money back. Halifax accepted this response without probing further.

The conversation then moved to cryptocurrency, with Halifax asking whether Mr C had access to his cryptocurrency account. Mr C confirmed that he did but stated that he wanted to exit from it. The Halifax representative repeatedly responded "that's fine" without further questioning. They then instructed their branch colleague to warn Mr C that using cryptocurrency was an investment and carried a risk of losing money. This message was passed on to Mr C, who accepted it without further discussion.

The member of the fraud team then confirmed they'd removed the blocks on the payment and Mr C could now proceed, although they explained they'd removed the link between his Halifax account and his cryptocurrency account, and if he wanted to make further payments to it he'd need to re-establish the link.

Did Halifax do enough?

Having listened to the calls above I agree with Halifax's conclusion that although Halifax did intervene before the third payment was made, and had the opportunity to uncover the scam, it didn't do enough in order to do so.

Throughout the second call there were long periods of silence, and Halifax didn't press Mr C for further details about the payment or the confusion between repaying the loan and purchasing cryptocurrency. The questioning was limited, and there was little effort to explore why the funds were being sent or to challenge Mr C's vague or avoidant responses.

Despite clear indicators of potential fraud, Halifax didn't thoroughly investigate or provide a strong warning that might have prevented Mr C from proceeding with the payment.

So the starting point is that Halifax is responsible for Mr C's losses from payment three onwards.

Is Mr C responsible for any of his losses?

I've considered the part Mr C played in allowing the scam to take place. While Halifax has a duty to protect him from fraud, he also has a responsibility to take reasonable steps to keep himself safe. Scams can be highly sophisticated, and it's clear that Mr C was manipulated by

fraudsters using convincing tactics. However, there were several points where he could have taken steps to protect himself, which Halifax has reasonably considered in reducing his refund by 50%.

Although Mr C says he searched for the company online and it sounded legitimate, I haven't been able to find the company in question located in Canada. So I'm not persuaded that Mr C did in fact carry out any independent checks to verify the legitimacy of the company that contacted him, despite there being no clear link to Z. I think it's more likely that he accepted the scammer's claims at face value, including the unusual instruction to repay the loan using cryptocurrency, based on what he's described as the legitimate-looking emails and recognisable logo.

In addition, although the emails from the company referred to recovering lost cryptocurrency funds rather than repaying his loan with Z, I haven't seen that Mr C questioned why this was the case. Additionally, I'm not aware that Mr C challenged why he couldn't simply repay the loan directly from Halifax to Z, as would normally be expected, nor that he questioned why he was repaying the loan as several payments as opposed to the one lump sum that it was received in.

Crucially, when Halifax did intervene on multiple occasions, both in branch and over the phone, Mr C misled it by giving inaccurate information about the purpose of the payments.

Whilst Halifax has a duty to detect and prevent fraud, Mr C also had a responsibility to act cautiously and responsibly, and to respond to Halifax's interventions truthfully. By failing to question these inconsistencies, seek clarification, or be honest when Halifax queried the payments, Mr C made it more difficult for Halifax to intervene effectively.

I've kept in mind Mr C and his representative's comments that the reason the scammer's explanations seemed plausible is because Mr C is elderly and doesn't have investment experience. But neither the loan repayment, nor the scammer's emails in relation to recovering cryptocurrency, relate to investments. So I'm not persuaded that Mr C's lack of investment experience affected his ability to detect the unusual nature of the scammer's proposal to recover cryptocurrency, as opposed to repaying the loan, which is what Mr C had set out to do.

I also note Mr C's representative's point that *"Had the bank asked some simple questions they would have uncovered the following Red Flags:*

- *They were paying a loan back with crypto*
- *They were sending multiple payments to crypto exchange platforms*
- *The company in talks with him (GDPR) has no connection to Z the where the loan came from*
- *The email sent by the fraudsters was not from Z"*

I've considered these points in my decision, but I don't agree that Halifax's interventions ought to have uncovered the scam, owing to the fact that Halifax did intervene multiple times, and Mr C wasn't honest in the way he responded to Halifax's questioning.

I've also seen Mr C's representative's point that Mr C didn't fully understand the process of converting funds into cryptocurrency, or the distinction between that and repaying his loan, so this shouldn't be considered wilful deceit, but a lack of understanding. Whilst I've taken this into account, I must also bear in mind that Mr C did deceive the bank by telling it he was buying Christmas presents, and that he was making the payment as he was "working on

something" – both statements that, regardless of Mr C's understanding of cryptocurrency, were untrue.

As a result of these points I've concluded that it's reasonable for Halifax to have determined that Mr C's actions contributed to his loss, and to have reduced his refund accordingly, which in this case is by half.

Finally, I've also considered whether Halifax ought to have intervened again after payment three, as more payments were made. Halifax did intervene a number of times throughout the scam and whilst I haven't gone into detail, I've also listened to the relevant intervention calls. During those calls, despite multiple opportunities to disclose the true reasons behind the payments, Mr C avoids telling Halifax the true details of the situation. He tells Halifax he is making payments to purchase Christmas presents. He's also probed on whether he was converting his money into cryptocurrency more than once, which he denies, but as he had been using cryptocurrency platforms for around two years I'm satisfied that Mr C knew this wasn't true, but he answered in this way to minimise suspicion on Halifax's part.

I'm also satisfied that even if Halifax had intervened even more times, or asked different or more probing questions, I'm not convinced this would've changed the outcome for Mr C. Given his evident determination to make the payments without Halifax uncovering the true reason behind them, I'm persuaded this would've continued no matter what Halifax had done to intervene.

Recovery of the funds

Halifax didn't attempt to recover any of the payments Mr C sent. It said this is because he sent the funds to an account in his own name, before transferring them on to the scammer.

As the accounts Mr C made the payments to were in his own name, under his control, I think this was a reasonable course of action for Halifax to take. If it had attempted recovery, it would've been recovering the funds from Mr C, although he'd used the funds to purchase cryptocurrency.

Any remaining funds he hadn't converted into cryptocurrency would've still been under his control at the cryptocurrency platforms, so he'd have been free to return them to his Halifax account or to use them how he chose to.

I'm very sorry that Mr C 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 require Halifax to do anything else to put things right, as I think the refund it paid to Mr C is fair.

My final decision

I don't uphold Mr C's complaint against Bank of Scotland plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 29 April 2025.

Sam Wade
Ombudsman