DRN-5535895

The complaint

Miss S complains that Bank of Scotland plc trading as Halifax failed to protect her from falling victim to a scam. Miss S also complains that Halifax won't reimburse her losses.

What happened

All parties are aware of the background to Miss S' complaint so I'll summarise things here.

In June 2024 Miss S came across a job advert on social media. Miss S was then contacted by individuals via a messaging service who claimed to offer work completing online reviews. As part of the process, Miss S was given access to an online portal where she completed job tasks. Miss S was initially able to withdraw a small amount of commission. Miss S was also given different job tasks that came with a higher rate of commission but required her to deposit cryptocurrency into online wallets she believed were owned by the business. Miss S was told she would then receive her deposit back plus the commission she'd earned.

On 6 June 2024, Miss S made a payment of £1,500 and another of £3,700 from her Halifax account to her account with an online cryptocurrency exchange I'll refer to as C. Miss S then converted those funds to cryptocurrency and sent them to an online wallet belonging to the scammers. Miss S attempted to make a further payment of £12,000 to her account with C but it was picked up by Halifax's fraud prevention system. Halifax went on to speak with Miss S about the payment she was trying to make.

After discussing the circumstances of Miss S' payments, Halifax's agent explained they thought she was the victim of a scam. The agent advised Miss S not to send any more money to the scammers as the job opportunity wasn't genuine. Halifax declined the payment and sent £12,000 back to Miss S' account.

On 7 June 2024 Miss S sent two further cryptocurrency payments that valued around £7,350 from balances held with C to the scammers.

Miss S contacted Halifax again on 8 June 2024 and raised a claim with its fraud team. Halifax reviewed the two payments it made to C on 6 June 2024, totalling £5,200, but didn't agree to reimburse Miss S for her losses.

Representatives acting on Miss S' behalf went on to raise a complaint and Halifax issued a final response. Halifax said the payments Miss S made were to an account in her name and didn't offer to reimburse the £5,200 she lost. Halifax paid Miss S £60 in recognition of some incorrect information given when she first called to report the scam.

An investigator at this service looked at Miss S' complaint. Given Miss S' account history and what she told us about the scam, the investigator thought Halifax should've intervened when she instructed the second payment, for £3,700, on 6 June 2024. The investigator thought Halifax should've held the payment and asked Miss S some automated questions to help narrow the risk of financial harm and provided some written warnings about fraud. But the investigator wasn't persuaded earlier intervention, either by automated warnings or human contact with Miss S, from Halifax would've prevented her losses. The investigator pointed

out that despite Halifax identifying the payments she'd already made on 6 June 2024 were likely to have gone to scammers and declined the £12,000 payment she tried to make, Miss S still went on to make further substantial payments from C on 7 June 2024. The investigator didn't uphold Miss S' complaint.

Miss S asked to appeal and said Halifax had failed in its duty of care as it hadn't identified or acted upon clear risk indicators that were present. Miss S also said the payment of £3,700 she made ought to have triggered enhanced intervention from Halifax and that clear, direct and serious scam warnings would have stopped her losing funds to the scammers. As Miss S asked to appeal, her complaint 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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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

Taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 2024 that Halifax should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment.
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

So I've gone onto consider, taking into account what Halifax knew about the payments, at what point, if any, it ought to have identified that Miss S might be at an increased risk of fraud.

Looking at Miss S' Halifax account history, I can see she had made and received payments in relation to cryptocurrency in 2022 and 2023. But the payments were generally for lower amounts than the ones Miss S lost to the scam. And there were no recent payments to C or for other cryptocurrency purchases shown on Miss S' bank statements.

In my view, it would've been reasonable for Hallifax to have intervened when Miss S tried to make the second payment on 6 June 2024, for £3,700. The payment was significantly higher than previous payments Miss S made and her account history in general. And, as noted above, Halifax should've been on the lookout for unusual transactions including those made to cryptocurrency exchanges like C, even when being made to an account in the customer's name. I think a reasonable and proportionate approach from Halifax would've been for an agent to have contacted Miss S directly and asked questions about the payment she was trying to make. Halifax could then have provided targeted information and warnings about cryptocurrency and job scams that were relevant to Miss S' situation.

It's not enough for me to reach the conclusion that Halifax should've intervened sooner. I need to consider whether an intervention from Halifax would've made a difference and prevented Miss S' losses. I think it's fair to note that Halifax did intervene when Miss S attempted to make a payment of £12,000 later in the day on 6 June 2024. During the conversation, Miss S provided some details about the payments she'd already made. And the agent Miss S spoke with confirmed their view that she'd fallen victim to scammers. The agent advised Miss S not to send any more money and that a genuine job role wouldn't require her to do that. But the evidence provided by Miss S' representatives shows that despite Halifax confirming her previous payments had likely been sent to scammers, she went on to make two further cryptocurrency transfers to them totalling around £7,350 on 7 June 2024.

I understand Miss S felt the investigator's view of her complaint was speculative as it considered what she would've done differently if an earlier intervention from Halifax had taken place. But we have to consider what's most likely to have occurred if Halifax had taken action earlier. Where the details or circumstances of a complaint are disputed by the parties involved, we'll base our decisions on the balance of probabilities. That is, what I consider most likely to have occurred based on all the available information. As I've said above, I need to consider what difference an earlier intervention would've made to Miss S on 6 June 2024.

In my view, the fact Miss S went on to send further substantial payments to the scammers after Halifax spoke with her and confirmed its view she had fallen victim to scammers indicates that even if it had intervened earlier and provided either an automated warning or direct human intervention, it's more likely than not she would've still proceeded. I think Miss S was very much under the influence of the scammers at this point and was ultimately persuaded the job opportunity was genuine and she'd receive a return on her payments. I can see that Miss S has told us she found the job portal to be professional and online reviews of the business were positive. Miss S has also argued that if Halifax had intervened when she made the payment of £3,700 it's likely that her further losses would've been prevented. But given the later direct warning by Halifax that specifically confirmed the view she was a victim of fraud failed to stop Miss S sending further payments totalling £7,350, my view is it's unlikely that earlier interventions would've made a difference.

I'm very sorry to disappoint Miss S but I haven't been persuaded that earlier intervention from Halifax would've prevented her losses. As a result, I'm unable to uphold Miss S' complaint or tell Halifax to reimburse her payments totalling £5,200.

My final decision

My decision is that I don't uphold Miss S' complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 6 August 2025.

Marco Manente
Ombudsman