DRN-5127648

Complaint

Ms M is unhappy that Bank of Scotland plc (trading as Halifax) didn't refund her after she told it she'd fallen victim to a scam.

Background

In 2023, Ms M received unsolicited contact on a social messaging app. The person who contacted her said they could offer her a job opportunity. The client was a cinema company and Ms M would be paid commission for writing reviews of films. The premise was that these reviews would boost the films' exposure. Unfortunately, although Ms M didn't realise it at the time, she hadn't been offered a legitimate job opportunity. The person who had contacted her was a fraudster.

She was told that, in order to earn commission, she needed to fund her account and that the company needed to be paid in cryptocurrency. She transferred funds from her Halifax account to an e-wallet with a third-party cryptocurrency exchange. Those deposits were then converted to cryptocurrency and transferred into the control of the fraudsters.

She made multiple payments using the debit card connected to her Halifax account. When she said that she wanted to withdraw her earnings, she was told that she needed to pay further fees. When she still wasn't able to withdraw funds, she realised that she must have fallen victim to a scam.

She informed Halifax. It looked into things, but it didn't agree to refund her. Ms M wasn't happy with that and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. Ms M disagreed with the Investigator's view and so the complaint has been passed to me to consider and come to a final decision.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

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. Ms M did authorise these payments and so she is considered liable for them at first instance.

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 protect their customer. That might be as simple as providing a written warning as part of the payment process or it might extend to making contact with the customer to establish the circumstances surrounding the payment.

I can see that there were several interventions by the bank in connection with Ms M's

payments, but these weren't successful. I've listened to recordings of the telephone calls she had with the bank. Unfortunately, the information she shared with the bank wasn't accurate. For example, on 18 August, she spoke to employees of the bank who gave general warnings about crypto scams and explained some of the background risks. Ms M said that she was acting of her own volition and that she had been investing in cryptocurrency for some time.

She was in contact with the scammer throughout. Shortly before contacting Halifax, she was advised by the scammer to tell the bank she was making a normal cryptocurrency investment and not to say anything else. Ms M followed these instructions. I appreciate this may have been because she genuinely believed the scammer's platform was legitimate and that she would receive her profits in return. Unfortunately, it meant Halifax couldn't realistically identify the scam type and so its ability to provide her with an appropriately tailored warning was undermined.

Ms M's representative has made some criticisms of the quality of Halifax's interventions. Those points are generally well made. While I wouldn't expect an employee of the bank to subject Ms M to a forensic level of scrutiny, I agree that, at times, they were too willing to take her answers at face value and ought to have probed a little more than they did.

Unfortunately, I'm not persuaded that it would've made any difference – she was being guided by the fraudsters in how to respond to the bank's questions. She was also evidently frustrated in some of the later calls at the barriers that had been placed in her way to prevent her moving the money as she wanted. I think it's more likely than not that she would've continued to follow the fraudster's advice when responding to queries from the bank.

Overall, I'm satisfied that Halifax took reasonable and proportionate steps to protect Ms M from financial harm here. She received warnings based on the information that she volunteered, she was asked relevant questions, and was given time to reconsider. Despite this, she appears to have been determined to make the payments – and she misled the bank in order to ensure that they were made.

For the sake of completeness, I've also considered whether the bank should've done more to help her recover her funds. They'd already been moved on from the receiving account by Ms M, so it wouldn't have been able to contact the cryptocurrency firm's bank to request that funds be sent back. I'm also satisfied that a chargeback wouldn't have had any reasonable prospect of success given that her contract with the payee was to receive funds into an e-wallet and that contract was performed.

I don't say any of this to downplay the fact that she's fallen victim to a cruel and cynical scam. I have a great deal of sympathy for her and the position she's found herself in. Nonetheless, my role here is to look at the actions and inactions of the bank and, while I accept that there were some shortcomings with the intervention calls, I'm not persuaded that they were the cause of her losses here.

Final decision

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 Ms M to accept or reject my decision before 22 April 2025.

James Kimmitt
Ombudsman