DRN-4593620

The complaint

Ms P has complained that Bank of Scotland Plc (trading as "Halifax") failed to protect her from falling victim to a 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.

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

Ms P explains that around August 2023 she was contacted by an individual ("the scammer") on a popular messaging application offering her an employment opportunity. She says that although she wasn't actively looking for a job at that time, she'd initially been recruited into her existing role by the agency that the scammer was allegedly working for. Ms P expressed an interest in the role and she says the scammer explained that the job involved completing online reviews of products in order to boost their search results and sales. Ms P was told she'd need to deposit funds into a "work platform" in order to simulate buying the items before reviewing them, and she'd then complete batches of 20-30 tasks and then she could withdraw her earnings as well as her initial outlay.

Ms P says the company's website, and the systems used to show her work tasks and earnings, were extremely professional and had all the characteristics she'd expect from a legitimate company. She also says she searched online and found various websites with positive reviews about the employment opportunity, and she was added to a group chat with other alleged employees.

In order to fund her work account to simulate purchasing the products to be reviewed, Ms P was required to send funds to her own wallet at a cryptocurrency exchange. She then converted the pounds into cryptocurrency and forwarded it on to the scammer's cryptocurrency wallet, under the impression it was being sent to her work account.

The payments Ms P made as part of the scam were as follows:

Date	Amount
15/07/2023	£2,000
16/07/2023	£3,500
17/07/2023	£4,400
Total	**£9,900**

Ms P says she realised she'd been scammed when she stopped receiving responses from the "customer service" department of her alleged employer, as well as the scammer who'd she'd been messaging since being recruited.

Ms P made a complaint to Halifax in which she said that its systems failed to pick up on out-of-character transactions that were indicative of her falling victim to a scam. She also said the scam would've been prevented if Halifax had appropriately intervened. Halifax didn't uphold the complaint as it said Ms P should've done more checks in relation to the employment opportunity before making the payments. It also said Ms P had sent the funds to another account in her own name before forwarding them on to the scammer from that account. Ms P remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained she thought that Halifax had done enough to intervene and warn Ms P about the risks associated with cryptocurrency scams. She also noted that Ms P wasn't honest in answering Halifax's questions, so she said she couldn't hold Halifax responsible for not doing more than it did, based on the information it had available.

As Ms P 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 Ms P but having considered everything I'm afraid I'm not upholding her 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 Ms P authorised these payments from leaving her account. It's accepted by all parties that Ms P gave the instructions to Halifax and Halifax made the payments in line with those instructions, and in line with the terms and conditions of Ms P'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 reviewed Ms P's account activity before these payments took place and although she made a payment of £2,000 in August 2022, and another payment of £1,608 in July 2023, I don't think it's reasonable to say that these payments were in line with what Halifax should've expected to see. I say this because the first payment was almost a year before the first scam-related payment, and the second was for a lower value than of those related with the scam. So I've gone on to think about what, if anything, Halifax did to make sure as far as reasonably possible that Ms P wasn't as risk of financial harm.

I can see from Halifax's records that Ms P initially attempted to make a payment of £6,349 to the cryptocurrency exchange, but the payment was blocked by Halifax's fraud detection systems and Ms P was asked to contact the bank to verify the payment.

I've reviewed transcripts of the calls and whilst I'm not going to include them fully here, I'm satisfied that Halifax did as much as it could to ensure Ms P was aware of what she was doing, and of the scams that exist.

During the call Halifax asks Ms P about the reason for the payment and she says she's investing in cryptocurrency, which she has done before. Halifax tells her on numerous

occasions that lots of people are being scammed using cryptocurrency, and it can be very difficult to recover any money lost in this way, to which Ms P responds “I understand, I understand”. She also confirms that nobody has contacted her and asked her to move money to a cryptocurrency account, and she’s given information about publicly available warnings about the risks associated with cryptocurrency. Ms P’s advised that the payment would remain blocked for 24 hours, and that she should call back after completing her own independent research, if she still wished to make the payment.

Ms P also attempted to make two payments, for £1,000 and £3,000, to her own account with another bank. These payments were blocked by Halifax so Ms P called Halifax and was again given scam warnings, and during that call she told it she didn’t intend to make the payment that had initially been blocked. She assured Nationwide that the £1,000 and £3,000 payments weren’t related with cryptocurrency so the blocks were removed, and the payments were made.

During this call Halifax asked several robust questions to understand the circumstances behind what was happening, and it told Ms P it was concerned that she was being scammed. After some conversation Ms P was very clear that she wouldn’t be sending money to the cryptocurrency exchange and she’s told by Halifax “If you're telling me now, you're not going to send money to this, I can cancel it and remove your blocks but I will tell you now, this call is recorded and if you choose to send money again and you're scammed, we wouldn't even look at this for you and the money will be gone”. Ms P confirms she can’t afford to lose £6,000 and says she’s not going to make the payment to the cryptocurrency company. During the same call Halifax asks Ms P why she’d only just started using her Halifax account to make these payments. She says she’d previously been making them from an account held elsewhere, but that that account had been closed without warning. She explains she’d researched and found that Halifax was one of the banks that allows cryptocurrency-related transactions to be made. Halifax further warns Ms P about the risks associated with cryptocurrency-related scams, which Ms P acknowledges, and the call ends.

In a another call later on the same day, due to the blocks not having been fully removed from Ms P’s account, Halifax confirms with Ms P whether she’d been told why the payments were initially blocked – to which she responds “Yeah yeah yeah, I am fully aware of the risks, I have taken the advice, all calls are recorded and I am fully aware of the risk and that's why I’m not going ahead with this”. The blocks are then removed and the call ends.

Following this call, Ms P made the first of the three transactions to the cryptocurrency exchange. On the two following days she then made the next two payments.

Halifax says the payments were made to the cryptocurrency platform using Open Banking. Open Banking is a system that allows consumers to securely share their financial data with authorised third-party providers, such as budgeting apps and other payment services. The idea is to give people more control over their financial information and allow them to use it to access better deals, new products, or services that can help manage their money.

With Open Banking, banks are required to provide access to this data (with the customer’s permission) through secure technology called APIs (Application Programming Interfaces). Halifax says that as Ms P made the payments from her Halifax account via Open Banking it didn’t provide any warnings,

The fact that Open Banking features in this payment journey doesn’t mean Halifax didn’t need to be aware of signs of financial harm to Ms P. Although using Open Banking means the payments were initiated by the cryptocurrency exchange where Ms P held her cryptocurrency account, the payments were sent from Ms P’s Halifax account, so Halifax

was still responsible for having effective systems and controls in place to monitor and identify potential risks as part of that payment journey.

But I've also considered whether it would've made a difference if Halifax *had* intervened further – and I don't think it would.

I say this because it's evident having reviewed calls between Ms P and Halifax that she was determined to make the payments, and she wasn't entirely honest with Halifax when answering the questions about them. Ms P assured Halifax she hadn't been asked to make the payments by a third party, and she also gave the impression she wouldn't make the cryptocurrency-related payments that she then went on to make. Halifax also gave Ms P a multiple scam-related warnings and a lot of relevant information, during all of the separate calls, but she still chose to make the payments. So even if Halifax had gone further or intervened in some other way before these payments were made, I think it's unlikely Ms P would've acted differently, and I therefore don't think Ms P's losses would've been prevented.

It's important to remember that whilst businesses have a duty to detect and identify unusual account activity, they are also reliant on customers being honest in response to the questions they're asked and receptive to the advice and information they're given. That's not the case here, so whilst I accept that Ms P is the victim here, I can't hold Halifax responsible for the loss on that basis alone.

Recovery of the funds

I haven't seen that Halifax attempted to recover the funds Ms P sent as part of the scam.

But as the funds had been made available to Ms P and she'd used them to purchase cryptocurrency, Halifax wouldn't have been able to recover anything in any case, as she'd effectively spent the money she sent. So I don't think Halifax ought to have done more, nor that this affected the outcome for Ms P.

I'm very sorry that Ms P 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 Ms P's complaint against Bank of Scotland Plc, trading as Halifax.

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

Sam Wade
Ombudsman