DRN-4430686

The complaint

Ms W complains that Bank of Scotland Plc didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In February 2023, Ms W was approached by someone on social media who I'll refer to as "the scammer". They started communicating via WhatsApp and after a couple of weeks the scammer started to tell Ms W about her work, explaining that she had a contract to manage data on an investment platform I'll refer to as "M". She said she could help Ms W make money by investing in cryptocurrency and after hearing about how the investment would work, Ms W decided to make a small investment.

The scammer told her to open accounts with M and a cryptocurrency exchange company I'll refer to as "F". She advised her to purchase cryptocurrency through F and then load it onto an online wallet, and between 9 March 2023 and 12 April 2023, Ms W made nine transfers to F totalling £134,500 from her Bank of Scotland account.

During the scam period Ms W received two credits totalling £317.76, but when she asked to make a larger withdrawal she was told she'd have to pay 20% of her profits to release the funds, at which point she realised she'd been scammed.

Ms W contacted Bank of Scotland but it refused to refund any of the money she'd lost. It said it had intervened throughout the payment journey, but Ms W wasn't entirely honest and had continued to invest even though it had provided warnings and scam education.

It said Ms W had made payments to her own cryptocurrency account and then moved the funds to the scammers, so it was unable to raise a scam claim. And the payments weren't covered under the Contingent Reimbursement Model ("CRM") code because she was paying an account in her own name.

It also said she didn't complete any due diligence, which was unreasonable given the amounts she was investing and the fact there were scam warnings about M, which she'd have discovered if she'd done any research.

Our investigator didn't think the complaint should be upheld. She explained that Bank of Scotland had blocked payments and spoken to Ms W on 9 March 2023, 16 March 2023, 23 March 2023, 28 March 2023, 30 March 2023, 5 April 2023 and 12 April 2023. During these interventions, she gave incorrect answers to the questions she was asked and went ahead with the payments despite several tailored warnings, which included examples of scams and descriptions of common tactics used by scammers. She was also required to visit her local branch with photo ID where she was asked further questions before the payment was

processed. Overall our investigator was satisfied that Bank of Scotland had intervened appropriately and that there was nothing further it could have done to prevent Ms W's loss.

Ms W has asked for her complaint to be reviewed by an Ombudsman arguing that Bank of Scotland should have investigated further before processing the payments. She's said she was coerced into making the payments and that she wouldn't have gone ahead with the payments if she'd known it was a scam. She accepts that Bank of Scotland did intervene but she's argued that she was open about the fact she was investing in cryptocurrency and that it didn't do enough to prevent her loss as it wasn't enough to simply ask her questions.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Ms W has been the victim of a cruel scam. I know she feels strongly about this complaint and this will come as a disappointment to her, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Ms W says she's fallen victim to, in all but a limited number of circumstances. Bank of Scotland has said the CRM code didn't apply in this case because Ms W was paying an account in her own name, and I'm satisfied that's fair.

I'm also satisfied Ms W 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Ms W is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Ms W didn't intend her money to go to scammers, she did authorise the disputed payments. Bank of Scotland is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Bank of Scotland could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Bank of Scotland ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough to warn Ms W when she tried to make the payments.

Because Ms W made nine payments to the scam and Bank of Scotland intervened in seven of them, including the first payment, I don't think it missed any opportunities to intervene. So I need to consider whether it did enough on the occasions it did intervene.

It blocked the first payment of £2,000 on 9 March 2023 and in the subsequent call Ms W told the call handler she wasn't approached on social media, she was being helped by her sister and she was the only person with access to her cryptocurrency account. She was given a general scam warning and the payment was released.

The second payment of £14,000 was also flagged and during that call Ms W said again that she was being helped by her sister and that she invested in property and she could see her investment growing on the trading platform. The call handler warned her that scam victims often say they are being advised by siblings having been contacted on social media by people promising good returns using what look like legitimate trading companies. She was asked if she'd checked the Financial conduct Authority ("FCA") register and whether she'd been told to lie to the bank. She was also warned that scammers often ask people to move money out of cryptocurrency accounts.

The fourth payment of £8,000 on 23 March 2023 was flagged for further checks. In the subsequent call, Mrs W was asked whether she'd done any research and whether she'd received the previous transfers into the account. She was also given a scam warning and told to attend a branch with ID for the payment to be processed. On 28 March 2023, Ms W maintained she hadn't been contacted out of the blue and it was her own decision to invest.

On 30 March 2023, Bank of Scotland blocked a further payment of £15,000. During this call, Ms W maintained that she was making the investment herself, she'd done her own research and there was no third-party involved. She was warned against lying to the bank and she insisted she was happy to proceed with the payment. In a further call on 5 April 2023, Ms W was warned that fraudsters tell victims to lie to the bank, promise unrealistic returns and encourage them to open accounts with trading platforms. They also asked whether she'd been coerced or whether she'd been told to download remote access software, which she confirmed she hadn't.

The eight payment was for £40,000 and was competed in branch on 11 April 2023. Based on what took place during the earlier calls, I think its unlikely Ms W would have disclosed any more information about the scam, so even if she was asked probing questions about the payment while she was in the branch, Bank of Scotland wouldn't have been in a position to perform a more robust intervention. The final payment for £15,500 was also made in the branch, when the branch staff contacted the fraud team, confirming Ms W knew about the risks associated with cryptocurrency and that she wanted to go ahead with the payment.

I accept some of the interventions were more detailed than others both in respect of the questions Ms W was asked and the advice she was given. And I think she should have been asked more questions when she attended the branch to make the final payment. But based on her responses to the questions she was asked during the previous calls I don't think it would have made a difference to the outcome. This is because I'm satisfied that across the various interactions, Ms W was asked probing questions which were relevant to the nature and value of the payments and Bank of Scotland provided relevant and robust warnings about the risks involved with cryptocurrency based on the information it had. She was also told about the FCA's guidance on cryptocurrency investments and directed to other scam education on its website. And she was warned about the consequences of not telling the truth and given relevant examples of common tactics used by scammers.

Ms W told Bank of Scotland that she had investments in shares and property, she had researched the investment and knew about scams involving social media platforms. She didn't disclose that she was taking advice from someone who'd approached her on social media who had advised her to make an onwards payment from F, so it didn't have enough information to say for sure that she was being scammed. This wasn't a case where Bank of Scotland, contrary to Ms W's instructions, should have refused to put the payments through and in the circumstances, I'm satisfied it did all it reasonably could to draw her attention to the risks.

Ms W has said Bank of Scotland should have done more than simply ask questions but it's not unreasonable to expect her to provide honest answers, having been warned that

fraudsters sometimes tell their victims to lie to their banks. I accept that banks should be aware that consumers are often coached by scammers to lie, but I'm satisfied that Ms W was warned about the risks notwithstanding the fact she hid the existence of the third party.

Ms W has said she wouldn't have gone ahead with the payments if she'd known it was a scam, but it's clear she was so convinced that the investment was genuine that she was prepared to repeatedly ignore all the advice that Bank of Scotland gave her at every reasonable opportunity and I don't think there was anything else it could reasonably have done to change the outcome. Because of this, I can't fairly ask it to do anything further to resolve this complaint.

Overall, I'm satisfied Bank of Scotland took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Ms W has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Bank of Scotland is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr O paid an account in his own name and moved the funds onwards from there.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms W to accept or reject my decision before 7 February 2024.

Carolyn Bonnell
Ombudsman