DRN-4677450

The complaint

Mr E complains that Bank of Scotland plc trading as Halifax didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'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.

Mr E was the victim of an investment scam. He came into contact with someone who I'll refer to as "the scammer" who claimed to work for an investment company I'll refer to as "E". The scammer told Mr E he could make money from investing in cryptocurrency. He instructed him to send money to an account with an electronic money institute ("EMI") I'll refer to as "R" and then to buy cryptocurrency from a cryptocurrency exchange company I'll refer to as "B". From there it would be loaded onto an online wallet.

Between 25 October 2022 and 6 February 2023, Mr E made six payments totalling £23,550. The initial payment of £250 was made using a debit card connected to Mr E's Halifax account, followed by five transfers, two of which were made in branch on 23 November 2022 and 9 December 2022.

Mr E had access to a trading platform where he could see his profits grow. But he realised he'd been the victim of a scam when he was asked to make further payments to withdraw his profits. He complained to Halifax but it refused to refund any of the money he'd lost. It said it couldn't recover the debit card payment because it was properly authorised. It said the Contingent Reimbursement Model ("CRM") code didn't apply to the transfers as they were to an account in his own name and control. It also said Mr E had failed to check E was regulated by the Financial Conduct Authority ("FCA"), he wasn't given any paperwork and the returns were too good to be true.

It said it stopped the first payment for a security check and during the subsequent call it provided advice based on the fact Mr E told it the payment was for holiday funds. It further explained Mr E had made two payments in branch when it followed its high value checklist which asks questions around scams and provided adequate scam education. There was also a further call when Mr E said he'd opened the account with R and was using it for holiday funds.

Mr E wasn't satisfied and so he complained to this service. Halifax maintained that Mr E had moved funds to an account he held with R, therefore it was unable to raise a claim under the CRM code.

It said the faster payment on 1 November 2022 was stopped and Mr E said the money was going to R to pay for a holiday and he was given scam education. It said the payment was robustly reviewed and confirmed as genuine.

It said its branch staff were unable to recall the specific details of the payments Mr E made in branch on 23 November 2022 but as the payment was over £5,000, full checks and fraud leaflet and procedures would have been followed and further questions would have been asked. It said there was no evidence of what took place when Mr E made the second payment in branch on 9 December 2022 but all the evidence pointed to the correct branch procedures, scam questioning, education and leaflet having been followed.

It said the payments were spread over three months which didn't fit the pattern of an investment scam. It maintained Mr E didn't carry out any due diligence and failed to take any reasonable steps to protect himself. The returns were too good to be true and he didn't have a reasonable basis for believing the investment was genuine.

Our investigator didn't think the complaint should be upheld. She explained that during the call on 1 November 2022, Mr E said he was depositing money into his own account as he was possibly going on holiday. He also confirmed he hadn't been told to lie. She noted Mr E wasn't truthful about the reason for the payment, so even if Halifax had asked further probing questions either then, when he attended the branch or before any of the later payments, she was satisfied he wouldn't have disclosed that he intended to buy cryptocurrency, so it wouldn't have been on notice that he was being scammed.

Our investigator also explained that Mr E was out of time to raise a chargeback request and the CRM code wouldn't apply to the faster payments because he was paying an account in his own name. And there was no realistic prospect of a successful recovery.

Mr E has asked for his complaint to be reviewed by an Ombudsman arguing that when he attended the branch, the staff didn't know what R was or that it is often used in scams.

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 Mr E has been the victim of a cruel scam. I know he feels strongly about this complaint and this will come as a disappointment to him, so I'll explain why.

I've thought about whether Halifax could have done more to recover the debit card payment when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. HSBC) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr E).

However, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mr E's case, the claim was referred to Halifax after this time, so this wasn't an option.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr E says he's fallen victim to, in all but a limited number of circumstances. Halifax has said the

CRM code didn't apply in this case because Mr E paid an account in his own name, and I'm satisfied that's fair.

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

There's no dispute that this was a scam, but although Mr E didn't intend his money to go to scammers, she did authorise the disputed payments. Halifax 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 HSBC could have done more to prevent the scam from occurring altogether. HSBC 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 ought to have done more to warn Mr E when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect HSBC to intervene with a view to protecting Mr E from financial harm due to fraud.

Based on the fact it was low value, I wouldn't expect the first payment to have flagged as suspicious on HSBC's systems. The second payment was only £2,000 and so I wouldn't necessarily expect that to have been flagged either, but as there was an intervention, I've gone on to consider whether HSBC did enough. During the call, Mr E was asked what the payment was for and he said he wanted to move it to R because he was possibly going on holiday. The call handler asked him if he'd had any scam messages or texts and whether he'd been contacted by anyone telling him to lie or move his money for any reason. Mr E was also warned that he wouldn't get the money back once it had left his account and asked to confirm it was a genuine payment being made his own instruction and not because someone had convinced him to do it.

I'm satisfied that Mr E was asked relevant and probing questions and that because he wasn't open about the purpose of the payment, the call handler didn't have enough information to identify that he was possibly being scammed or to provide a more tailored warning. I'm also satisfied that based on the information Halifax did have, Mr E was given relevant scam advice and there was nothing further the call handler could have done to uncover the scam or prevent his loss on that occasion.

I've thought about what happened when Mr E's attended the branch on 23 November 2022 and 9 December 2022. Halifax has been unable to produce evidence of exactly what was discussed before the payments were approved, but it has explained that full checks and procedures would have been followed and he was given a fraud leaflet. As Mr E was sending £8,000 and £5,000 to R, I would expect him to have been asked some probing questions about the purpose of the payment but, based on what he said during the call on 1 November 2022 and the fact there is evidence he'd been coached to lie, I think it's likely he'd had said he was moving funds to R to pay for a holiday. Consequently, there would have been nothing Halifax could reasonably have done to stop him from going ahead with the payments.

Mr E has suggested the branch staff didn't know anything about R and so it was unable to warn him that it is often used by scammers. Its right that scammers often tell victims to use

EMIs to transfer funds but it's also used for legitimate transactions. And as I've explained, I'm satisfied there was no reason for it to suspect the payments were being made to a scam.

I've considered whether Halifax missed any other opportunities to intervene and based on the fact Mr E was paying an account in his own name, the payments weren't increasing in value and they weren't made in quick succession, I don't think it did. And even if it had intervened, based on what took place during the call, I think the outcome would have been the same.

Compensation

Mr E isn't entitled to any compensation.

Recovery

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

Overall, I'm satisfied Halifax 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 Mr E has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Halifax is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 9 April 2024.

Carolyn Bonnell
Ombudsman