DRN-5209296

The complaint

Mr I 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.

At the beginning of October 2023, Mr I received a text message from someone I'll refer to as "the scammer" who claimed to be looking for someone else. This led to further conversations whereby the scammer told Mr I she was a trader and that she could help him to invest in cryptocurrency.

The scammer sent Mr I a link to a platform I'll refer to as "B", which seemed professional and genuine. He saw B had three-star reviews and so he paid £100 to open a trading account. Unfortunately, B was a clone of a genuine cryptocurrency exchange.

The scammer told Mr I to open account with an EMI I'll refer to as "R" and two cryptocurrency exchanges. The scammer told him to first purchase cryptocurrency through the cryptocurrency exchanges and then load it onto an online wallet. Between 13 November 2023 and 27 November 2023, he made five debit card payments and three faster payments from his Halifax account to two cryptocurrency exchange companies totalling £24,798, having made six payments totalling £7,825 from "W" up until 3 November 2023, when the account was deactivated.

He was able to make a small initial withdrawal. But when he tried to make a larger withdrawal towards the end of November 2023, he was told his account had been compromised and that he'd need to deposit further funds and pay taxes. At this point he made some enquiries (including asking the scammer to meet him in person and checking B's IP address) and discovered B was a scam.

Mr I complained to Halifax with the assistance of a representative who said he had no reason to doubt the scammer wasn't genuine. They said it had failed to ask him questions or effectively warn him about the risks associated with the payments, and had it done so he'd have checked the investment was legitimate and wouldn't have made any further payments. The representative said the payments were unusual because Mr I was paying a new payee, he hadn't made any payments higher than £1,600 in the three months before, and there were large credits into the account immediately before the payments. They said Mr I made two high value payments to a cryptocurrency exchange on 13 November 2023 and Halifax should have asked probing questions and warned him about cryptocurrency investment scams.

But Halifax refused to refund any of the money Mr I had lost. It said he should have made sure B was authorised by the Financial Conduct Authority ("FCA"), taken independent

financial advice, and tried to meet the scammer in person or at least had a video call with her before making any investments on her instruction.

It said it intervened on 27 November 2023 and during the call, Mr I said there was no one helping him to trade, so it told him about the risks involved with cryptocurrency and the payment was released.

It said it couldn't recover the funds because Mr I had paid a cryptocurrency account in his own name, and the debit card payments weren't eligible for chargeback because the correct service was provided. It also said the Contingent Reimbursement Model ("CRM") Code didn't apply to payments to accounts in the consumer's own name.

Mr I wasn't satisfied and so he complained to this service. He said he didn't receive any effective warnings and was simply asked if he was sure he wanted to make the payments, which he was because he believed the scam was genuine.

Responding to the complaint, Halifax said it didn't intervene when he made the debit card payments because there were properly authorised, and Mr I sent regular faster payments including ones for similar amounts to those paid to the scam.

It said when Mr I set up the new beneficiary for the faster payment on 27 November 2023, he selected the payment option as 'something else'. He was dishonest during the subsequent call, and the Contingent Reimbursement Model ("CRM") Code didn't apply to debit card or me-to-me payments. It also said he do enough due diligence having been contacted by an unknown person who he hadn't met in person.

Our investigator didn't think the complaint should be upheld. He thought Halifax should have intervened when Mr I made the second payment because it was a significantly large payment to a known cryptocurrency platform, but he explained that a written warning tailored to cryptocurrency scams would have been sufficient, and he didn't think this would have stopped the scam.

He thought Halifax should have intervened again when Mr I made payment three and that it should have contacted him because of the total value of the payments he'd made that day. But he noted that Mr I believed he was romantically involved with the scammer and went ahead with the sixth payment despite a proportionate intervention from Halifax, so he didn't think an earlier intervention would have made a difference.

Mr I has asked for his complaint to be reviewed by an Ombudsman. His representative accepts he provided misleading information, but they've argued that an earlier intervention would have been more effective because he might have been more truthful at the start of the scam. They have also argued that Halifax's intervention wasn't proportionate because the warning didn't adequately address the specific risks and characteristics of cryptocurrency investment scams, or the tactics commonly used by scammers, such as building personal relationships and providing seemingly legitimate investment opportunities.

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 I 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.

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 I says he's fallen victim to, in all but a limited number of circumstances. But the Code doesn't apply to the payments because Mr I was paying account in his own name.

I'm satisfied Mr I '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, Mr I is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr I didn't intend his money to go to scammers, he 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 Halifax 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 genuine cryptocurrency exchanges. However, Halifax 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 Mr I when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Halifax to intervene with a view to protecting Mr I from financial harm due to fraud.

Halifax intervened when Mir I made the sixth payment and so I've considered whether it intervened at the right time and whether the intervention was proportionate to the risk presented by the payment.

The first payment was only £300 and so even though Mr I was sending funds to a high-risk cryptocurrency merchant, there would have been no reason for Halifax to intervene. But I agree with our investigator that it should have intervened when he made the second payment because it was £5,000 to a high-risk cryptocurrency merchant, which was unusual for the account. I've thought about what a proportionate response would have been, and, in the circumstances, I think Halifax should have given Mr I a better automated warning which would involve questions about the purpose of the payment, and a written warning which was tailored to cryptocurrency investment scams.

But he went ahead with the payment on 27 November 2023 after questions and warnings from Halifax, and he was clearly determined to go ahead because he started to make payments from Halifax when he was no longer able to make payments from W. And he thought the scammer was genuine and had seen positive reviews about B. So, I don't think a written warning would have stopped him from going ahead with the payments.

Our investigator felt that Halifax ought to have contacted Mr I and asked probing questions when he tried to make the third payment. I think it's debateable whether it ought to have intervened again on 13 November 2023, or whether payment five would have been more appropriate, as this was the highest individual payment to the same beneficiary, and the total of the five payments to the same high-risk beneficiary within three days had risen to £18,298. But either way, I don't think it would have made a difference to the outcome.

This is because, due to the amount of money Mr I was sending to a high-risk cryptocurrency merchant, I think a proportionate response would have been for Halifax to contact Mr I to

question him about the payments. But, during the call that took place before payment six was processed, Mr I said he was investing alone and making his own choices, he hadn't been approached, there were no third parties involved, and he'd been trading for a while. He accepts these answers were misleading, and his representative has argued that Halifax should have asked more probing questions. But I'm satisfied he was asked sufficiently probing questions, and that his responses prevented the call handler from detecting the scam. I also note that he was warned that scammers might say they are brokers and get people to buy cryptocurrency using a legitimate platform and then give an address to send it to, and the money is lost at that point.

I've considered whether the intervention was proportionate to the risk presented by the payment, and I'm satisfied that it was. Mr I's representative has argued that he would have been honest if Halifax had intervened sooner but it's clear he believed the scammer was genuine to the extent that he followed her instructions to lie to Halifax and ignore the warnings it gave. So, while I agree that Halifax could have intervened sooner, I don't think this represented a missed opportunity to have stopped the scam.

Recovery

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

Mr I's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr I's card payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Halifax's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr I to part with his funds. I haven't found any errors or delays to Halifax's investigation, so I don't think he is entitled to any compensation.

I'm sorry to hear Mr I 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 I to accept or reject my decision before 23 August 2025.

Carolyn Bonnell
Ombudsman