DRN-4603823

The complaint

Mr M 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 M was the victim of two scams. He met someone on a on a dating app who told him they'd made money by investing in real estate and forex. He was put in touch with someone I'll refer to as "the scammer" who contacted him on WhatsApp and who claimed to work for and investment company I'll refer to as "S". Mr M reviewed the company website and the documentation he was given to verify S's status. He also spoke to company representatives who sounded professional and knowledgeable about investing.

The scammer told him he could make a 25% return on his investment and encouraged him to making payments through a cryptocurrency merchant I'll refer to as "B" to avoid paying tax. He also was given access to an online portal where he could monitor his investments and see his deposits in real-time.

Mr M started with a small initial investment and the scammer kept in touch with him via WhatsApp and Telegram. She also told him she'd personally made money investing in stocks and shares under the guidance of a broker, who she recommended to Mr M.

Mr M contacted the broker who advised him to invest in cryptocurrency. He noted the broker was registered in the USA and that her details matched accurately with an address he was able to find online. She was also verified with a blue tick on Telegram.

The broker told him to download remote access software to his device and that he could make good returns from investing in cryptocurrency. She asked him to first purchase cryptocurrency through B and then load it onto an online wallet.

Between 9 December 2023 and 9 February 2023, he transferred 22 payments to B totalling £94,705 from his Halifax account. This was partly funded with a loan of £25,000 from Halifax which he took out on 20 January 2023.

Mr M was told he would have to wait several months for his profit to increase and when he eventually tried to withdraw his money he was asked to pay a withdrawal fee. When he said he couldn't afford to invest any more money or pay the withdrawal fees, he lost touch with the broker and realised both investments had been a scam.

Mr M complained to Halifax but it refused to refund any of the money he'd lost. It said it had stopped the first payment and during the calls it had with him he was told about the Financial Conduct Authority ("FCA") warning about cryptocurrency investments and advised to check the FCA website. It said Mr M had said he was paying an account in his own name which no

one else had access to. He also said no one else was helping him, it was his choice to make the payments and he'd done his own research. It also said the payments weren't covered by the Contingent Reimbursement Model (CRM) Code because he was paying accounts in his own name.

Mr M wasn't satisfied and so he complained to this service with the assistance of a representative who explained he was unfamiliar with cryptocurrency and didn't know about the risks. Further, the returns didn't seem unreasonable given the coverage that surrounds investing and he was unaware of the importance of FCA registration, believing both S and the broker were operating legitimately from the USA.

The representative said Mr M didn't have a history of large payments and used the account for day to day spending, yet he was able to send large payments to a cryptocurrency exchange in a short space of time without sufficient intervention from Halifax. They said large amounts of money were transferred into his account from personal savings and a loan before being paid straight out to cryptocurrency exchanges, which was out of character especially as he frequently reached the transaction limit for the account.

They said that when Halifax did intervene he was asked a few questions about why he was sending the money and he answered truthfully and to the best of his ability. He didn't understand all the questions and terms such as FCA and open banking weren't properly explained. They also said he doesn't recall Halifax having explained how cryptocurrency scams operate.

The representative argued that Halifax failed to provide an effective warning despite the numerous red flags and they argued Mr M's losses could have been prevented if it had correctly identified the scam and invoked the Banking Protocol, which it should have done due to size of the payments.

Halifax said Mr M was given a warning when he made the first payment and there were numerous interventions where extensive questioning was carried out. It argued that if he had told it about the true nature of the payments, it would have been able to provide more relevant advice.

Our investigator didn't think the complaint should be upheld. She explained that during the first call on 15 December 2022, the call handler said he needed to ensure Mr M wasn't falling victim to a scam and asked him a series of questions about the payment. She was satisfied he was asked relevant questions but Mr M said he wasn't talking to a broker or financial advisor and he'd done his own research. She noted the call handler checked Mr M hadn't been told to buy cryptocurrency then send it to a different wallet, and Mr M didn't mention he'd been referred to the investment through someone he met on social media.

She explained there was a further call on 17 December 2022, when Mr M wasn't entirely truthful in his responses. And in a further call the following day, he was asked similar questions and gave the same responses before being asked to visit a branch with photographic ID. On 20 December 2022, Mr M had a call with an advisor while he was in the branch. After the call, he attempted to make a payment in the branch which was also blocked. He called back the same day and spoke to someone from the fraud team. He said he was getting frustrated as the payment kept being blocked, he confirmed he was making the payment all by himself, no one was guiding or advising him and he had sole access to the cryptocurrency account.

Overall, our investigator was satisfied that Halifax had intervened on more than one occasion and there was nothing else it could have done to protect him. Mr M was convinced the investment was genuine and Halifax did all it could with the information it had. She was

also satisfied that everything was properly explained and she didn't accept Mr M misunderstood what Halifax had said.

Mr M has asked for the complaint to be reviewed by an Ombudsman. His representative has said that Halifax failed to ask open-ended probing questions, despite its fraud systems showing the account activity was risky enough to warrant multiple interventions.

They have argued that Halifax allowed Mr M to take out a £25,000 loan which he had said was for a car purchase but was instead used to finance payments to a cryptocurrency exchange. They accept Mr M wasn't truthful in the loan application or in his answers to Halifax's questions, but they have argued the payments Mr M made after the loan was granted should have alerted it to the fact he was being scammed.

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 M 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 M says he's fallen victim to, in all but a limited number of circumstances. But the CRM Code doesn't apply to these payments because Mr M was paying an account in his own name. I'm satisfied Mr M '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 M is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr M 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 a genuine cryptocurrency merchant. 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 ought to have intervened to warn Mr M 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 M from financial harm due to fraud.

The payments did flag as suspicious on Halifax's systems and there were several interactions between Halifax and Mr M during the scam period, so I've gone on to consider whether Halifax did enough during these interactions.

I've listened to the seven calls that Halifax has provided and I'm satisfied that Halifax did enough and there was nothing else it could reasonably have done to prevent Mr M's loss. Over the course of the calls, Mr M was repeatedly asked whether he'd been contacted by

anyone claiming to be a broker or a financial advisor, whether anyone was telling him to move the money or buy cryptocurrency, whether he'd done his own research, how he got the details of the account he was paying, whether he'd opened the account himself, whether anyone else had access to the account and whether he'd been told to lie. He was also asked whether anyone was helping him or showing him what to do and whether he'd been told to download remote access software.

He was warned about the number of scams involving cryptocurrency and that if anyone else was involved it would indicate that he was being scammed. He was also warned that scammers want their victims to pay money into cryptocurrency exchanges before making an onwards payment. He was also given detailed advice on additional due diligence including checking online for negative reviews and checking the FCA website.

Mr M repeatedly said he was sending money to his own account and denied that there was any third party involvement whatsoever. He said he was acting alone, he was aware of the risks and had done his own research, which included checking for negative reviews. He said he'd opened the account with B himself, no one had helped him or showed him how to do it and he hadn't been told to lie. He also expressed frustration that the payments kept being blocked.

Mr M's representative has suggested that he didn't understand what he was told but I'm satisfied he engaged in lengthy conversations with the call handlers, he asked questions and that he clearly understood what he was told. He also gave assurances that he would do more research and twice made a note of how to check the FCA website.

I'm satisfied that across the various calls, Mr M was asked relevant questions and given robust advice which was tailored to the circumstances. Unfortunately, he repeatedly failed to answer the questions openly and this meant the call handlers didn't have enough information to identify that he was being scammed. Notwithstanding the limited information, I'm satisfied he was given appropriate scam warnings and advice on additional due diligence and in the circumstances there was nothing further Halifax could reasonably have done to prevent his loss.

Mr M's representative has said that Halifax should have asked him why he was funding the investment with a loan that he'd said would be used to buy a car. But even if Halifax had asked questions about the recent activity on the account, as the evidence shows he'd most likely been coached to lie, I can't fairly say additional questions would have uncovered the scam because its more than likely he would have been told to provide a plausible explanation for having diverted the loan money to the investment. The representative has also suggested that better questioning would have uncovered the scam, but I'm satisfied Halifax did everything it could have done and there was nothing else it could have done in terms of questions or additional interventions.

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 M 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.

Compensation

Mr M isn't entitled to any compensation or legal costs.

Recovery

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

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 M to accept or reject my decision before 25 April 2024.

Carolyn Bonnell
Ombudsman