DRN-4813492

The complaint

Mr T 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 T was the victim of an investment scam. In January 2018, he was cold called by someone who said he worked for an investment company I'll refer to as "S".

He had no investment experience, but he looked at the reviews of the company, which were all positive and satisfied him that he was dealing with a legitimate company. Further, the broker seemed professional and gave Mr T confidence that the investment was genuine.

The broker told Mr T he could make a return of 20% by investing in cryptocurrency and between 12 April 2018 and 23 May 2018, he made four credit card payments to two companies using a debit card connected to his Halifax account totalling £1427.43. During this period, he also made payments from accounts he held with Bank B and Bank S.

Mr T contacted Halifax in October 2019 stating that he'd fallen victim to a scam, but it refused to refund any of the money he'd lost. Unfortunately, he was then contacted by scammers claiming they could recover his lost funds. Believing this to be a genuine opportunity to recover his losses, Mr T made fourteen payments using his Halifax debit card and thirty payments via faster payment. These payments were to cryptocurrency exchange companies I'll refer to as "J" and "C" to buy cryptocurrency which he then transferred to the scam recovery wallets to pay costs such as insurance, litigation fees and charges.

When he realised he'd been the victim of a recovery scam, Mr T complained to Halifax with the assistance of a representative. Halifax said it had been unable to recover any funds from the beneficiary accounts. It said the first four debit card payments weren't unusual considering the account history. It accepted Mr T had sent a letter in October 2019 explaining he was worried he'd been scammed. It explained it didn't raise a chargeback claim as it was outside of the Visa chargeback timescales, but it had asked him to speak to Action Fraud. It also said the faster payments weren't covered under the Contingent Reimbursement Model ("CRM") code because they were to accounts in Mr T's own name.

It explained payments 5 to 20 weren't concerning because Mr T was making payments following credits into the account, which was normal. But it had contacted him on 9 October 2020 regarding a loan application which had raised concerns he could be the victim of a scam. At the conclusion of the call, he was asked to visit a branch to discuss the payments he'd been making, but he chose not to and instead made further payments to the scam. Acknowledging it should have blocked the account and invoked banking protocol on 9 October 2020, it offered to refund 50% of Mr T's loss from the payment on 30 October 2020 onwards. It explained that although the scammers were convincing and Mr T believed the

investment was genuine, he should have checked S was authorised by the Financial Conduct Authority ("FCA") and looked for reviews away from the company website. It also agreed to pay him £150 compensation for failings when he initially logged the complaint.

Mr T wasn't satisfied and so he complained to this service with the assistance of a representative who explained that Mr T continued to send money to the scam from 2020 to 2022 and that this was a result of not receiving any advice or warnings in relation to recovery scams when he contacted Halifax in October 2019.

The representative commented that Mr T was completely honest when Halifax contacted him on 9 October 2020, but no probing questions were asked and if he'd been questioned appropriately the scam would have been uncovered and the necessary warnings could have been provided.

Halifax explained that in October 2019, Mr T had said he had a company to recover his funds and he was advised to contact Action Fraud. It also said he was made aware of the scam risk during a call on 6 June 2020, but he was adamant the investment was genuine and that he wanted to go ahead.

Our investigator didn't think the complaint should be upheld. He explained there were no warnings on either the Investor Alerts Portal of the International Organization of Securities Commissions ("IOSCO") or the Financial Conduct Authority ("FCA") warning lists about the companies Mr T had paid between 12 April 2018 and 23 May 2018. And there was no evidence available online that the companies were fraudulent. So, he didn't accept Mr T had shown those payments were made to a scam. He also commented there was no evidence that the payments he made to J between 6 June 2020 and 27 November 2020 were fraudulent. But he accepted Mr T had produced statements indicating the payments he made to C in 2021 and 2022 were most likely fraudulent.

He explained a chargeback claim would have been out of time, and the faster payments were to an account in Mr T's own name, so they weren't covered under the Contingent Reimbursement Model ("CRM") code. He also commented that he didn't expect Halifax to have been able to recover any of the funds as they were sent via his own cryptocurrency accounts and moved on from there.

Our investigator didn't consider Halifax's actions before 9 October 2020 because there was no evidence the payments Mr T made before that date were fraudulent. He agreed it should have required Mr T to attend the branch following the call on 9 October 2020 and that this might have uncovered the scam, even though Mr T was determined to make further payments to the recovery firm. So, he was satisfied its offer to refund the payments Mr T made after that date was fair.

Our investigator explained that he'd listened to the call recordings dated 3 October 2019, 6 June 2020, 9 October 2020 and 18 May 2022 and he felt Mr T ought to have realised that being asked to pay fees to a recovery firm was unlikely to be genuine, especially as he was being asked to buy cryptocurrency. He didn't think he gave Halifax enough information to allow it to stop the scam during the 6 June 2020 call, having reassured Halifax he was investing, not paying to recover his lost funds. He also noted Halifax warned Mr T he was likely the victim of a scam on 9 October 2020 and suggested he visit branch to discuss the payments further, yet he failed to do so and continued making many further payments to something he'd been told was a likely scam. Because of this, he was satisfied Mr T had contributed to his own loss and he agreed the settlement should be reduced by 50% for contributory negligence.

Mr T's representative has asked for the complaint to be reviewed by an Ombudsman arguing the payments should have been flagged earlier. They've also argued that Mr T contacted Halifax in 2019 to tell is he'd been the victim of a scam, yet he received no warnings about the risk of future recovery 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 T 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 T 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 the faster payments were to accounts in Mr T's own name, and I'm satisfied that's fair.

I've thought about whether Halifax could have done more to recover the debit card payments 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. Halifax) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr T).

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 T's case, the claim was referred to Halifax after this time, so this wasn't an option.

Further, 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 Ms T's 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.

I'm satisfied Mr T '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 T is presumed liable for the loss in the first instance.

Were the payments fraudulent?

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false

representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

The first four payments were to companies in respect of which there were no warnings on either the Investor Alerts Portal of the International Organization of Securities Commissions ("IOSCO") or the Financial Conduct Authority ("FCA") warning lists about the companies Mr T had paid between 12 April 2018 and 23 May 2018. And there was no evidence available online that any of the companies were fraudulent. So, I'm not satisfied Mr T has shown the first four payments were made to a scam.

Mr T has also failed to show that the two payments he made to J in 2020 were fraudulent. He has explained he closed the account he held with J and is no longer able to access the account statements. Because of this I can't conclude these payments were made to a scam.

There's no dispute the faster payments to C were fraudulent, but although Mr T 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. Halifax ought to fairly and reasonably be alert to fraud and scams, so I need to consider whether it did enough when Mr T tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting Mr T from financial harm due to fraud.

Because I'm not satisfied that Mr T has shown the payments he made between 12 April 2018 and 27 November 2020 were fraudulent, I haven't considered whether Halifax ought to have intervened before that point. However, as Halifax's offer is based on what took place during the call on 9 October 2020, I've considered what happened during that call with a view to commenting on whether the offer is fair.

I've listened to the call and its clear the call handler considered there was a high risk that Mr T was being scammed and so she declined the loan application and advised him to attend the branch to discuss the payment. Unfortunately, because she didn't also block the account, Mr T was able to make further payments without attending the branch. Halifax has offered to refund the payments Mr T made after that call on the basis that the account should have been blocked and I'm satisfied that's reasonable.

Contributory negligence

Halifax has limited its offer to 50% because it says Mr T should have checked S was authorised by the Financial Conduct Authority ("FCA") and looked for reviews away from the company website.

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. Mr T hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He wouldn't have known it was a red flag to be asked to pay money to recover funds and this was compounded by the sophisticated nature of the scam.

However, Mr T contacted Halifax in 2019 to tell it he'd lost money to a scam, that he'd been contacted by a recovery agent and that he was worried it might be a scam. The call handler

told him not to use the recovery agent and to instead contact Action Fraud. It's clear from this exchange that Mr T considered he'd already been scammed and that he reasonably suspected he might fall victim to another scam, yet he went on to make further payments in an effort to retrieve his funds. He also took out loans to fund those payments.

Mr T also went ahead with payments to C after being warned during the call on 9 October 2020 that the company had poor reviews and that he wouldn't be granted a loan because it was likely he was being scammed. Critically, he was told at that point to attend the branch to discuss the payment, but he ignored that advice and made further payments to the scam.

While Halifax accepts it should have done more at that point, I'm satisfied this exchange shows that Mr T made further payments in the face of a clear warning that he was being scammed. Its clear he was desperate to retrieve his money and that he was willing to risk further funds to do so. In those circumstances I'm satisfied he failed to take reasonable care and that Halifax's decision to reduce its offer by 50% for contributory negligence is fair.

Compensation

Halifax paid Mr T £150 compensation for delays when Mr T first reported the scam and I'm satisfied that was fair and reasonable in the circumstances.

Recovery

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

Overall, I'm satisfied that Halifax's offer is fair, so I can't fairly tell it to do anything further to resolve this complaint.

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 Mr T to accept or reject my decision before 26 June 2024.

Carolyn Bonnell
Ombudsman