DRN-4056488

The complaint

Miss L complains that Bank of Scotland Plc trading as Halifax did not do enough to protect her from the financial harm caused by an investment scam company, or to help her recover the money once she'd reported the scam.

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.

Ms L was a victim of an investment scam. She came across the scammers while she was on social media and noticed a friend had uploaded a post about an investment opportunity. The post claimed an investment of £1,000 could generate a return of £14,000 within four hours.

Miss L contacted her friend to check she hadn't been hacked and her friend told her the investment was genuine and that she'd made a large profit. The friend recommended a broker who claimed to work for a trading platform I'll refer to as "M" who she said Miss L should speak to. Before contacting the broker, Miss L checked her social media account which had 115,000 followers and featured photographs of her with her family.

Miss L contacted the broker on her social media page and found her to be friendly and approachable. The broker advised Miss L to invest in cryptocurrency and assured her the process was safe. She told Miss L to download an app which would be used to place the actual trades. Miss L thought the app seemed legitimate as it had sections on how to make safe and secure deposits, and there was a section at the bottom of the website stating the company was regulated by the Information Commissioner's Office ("ICO"). The website also suggested M had been featured in NASDAQ, Yahoo, and Bloomberg and was regulated by the US government, the FCA, and CySec.

Before going ahead with the investment, Miss L read reviews about M and noted it's conflict handling policies seemed legitimate. The broker asked her to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. Between 10 January 2022 and 19 January 2022, she made nine payments to a cryptocurrency exchange company totalling £15, 817.09 using a debit card connected to her Halifax account.

On 10 January 2022 Miss L made an initial payment of £313.27 to a cryptocurrency exchange company I'll refer to as "C". The scammer did the trading on her behalf, and Miss L could see the trades on the app. Soon after making the initial deposit, Miss L's trading account showed a negative figure and she was told she'd need to pay a maintenance fee. The broker reassured her this was correct and so on 14 January 2022 she made a payment of £523.34.

When Miss L's account began to show a profit, the broker told her she'd need to pay a commission fee on all successful trades, so on 17 January 2022, she made a payment of £1,092.83. She was then told she needed to pay mandatory tax, which she did.

On 17 January 2022, believing the reasons given by the broker, Miss L made a further five payments totalling £10,837.09. Unfortunately, the broker continued to give excuses as to why Miss L couldn't access her money, including the fact they'd a lost a portion of her money, at which point she realised she was the victim of a scam.

Miss L contacted Halifax on 27 July 2022 asking it to refund the money she'd lost, but it said it was unable to do so as the disputed transactions were paid to a cryptocurrency exchange company who had successfully transferred her money to M via an e-wallet, as per their Terms and Conditions. As the exchange had completed their services, it was unable to raise a chargeback request. It also said that as the payments were made with a debit card, it couldn't use the Contingent reimbursement Model Code ("CRM").

When Miss L complained to Halifax it said it would pay her £50 compensation for the inconvenience caused by the fact it didn't process her new debit card correctly, but it maintained its position that it wouldn't refund the payments.

Ms L wasn't satisfied and so she complained to this service. She explained she'd been experiencing financial difficulties and had wanted to invest to regain her independence and position on the property ladder. She said she hadn't invested before, there had been no obvious red flags and she had trusted her friend. She said she thought the broker was genuine and had understood this was her first time investing. She had family members who had met brokers on social media and the broker had sent compliance documents and asked her to verify her own identity.

She explained she hadn't wanted to get into trouble for not paying taxes as she knew this was required by law, and the later payments were driven by a fear of not being able to access her money and felt she had no choice.

Miss L complained about the way she was treated when she first reported the scam, explaining she didn't feel Halifax had properly reviewed her complaint. She argued the payments were unusual in comparison to her normal account activity, that Halifax should have contacted her to ask some questions and that in failing to do this it failed to protect her from financial harm.

Miss L's representative argued that even though the CRM code didn't apply, Halifax still had a duty to look out for unusual or suspicious payments which might indicate the consumer was at risk of financial harm and to ask relevant questions which would uncover the fact they were falling victim to a scam.

They've suggested that if Halifax had asked her what the payments were for and the basic surrounding context, it's likely she would have fully explained what she was doing and told it about the existence of the broker. And that while the money was being paid to a legitimate cryptocurrency exchange company, Halifax should have provided a scam warning in light of all the information known to banks about the increasing number of cryptocurrency scams.

The representative argued the payments were suspicious because they were large, Miss L hadn't made payments to cryptocurrency exchanges before, they put Miss L into her overdraft which she hadn't done in the months prior and they were made in quick succession with many of them being in the same day (six transactions were on 17 January 2022). They said Halifax should have measures in place to identify unusual activity on its customer's accounts and as it had failed to identify these payments as unusual, it had failed in its duty of care to protect Miss L. And that if it had stepped in to ask her about the transactions, she would not have proceeded with the transactions.

Miss L's representative also argued that Halifax failed to take necessary steps to recover the funds once she'd reported the scam and to be more proactive in taking action to try and recover the money she'd lost.

Our investigator didn't think the complaint should be upheld. She accepted Halifax could have done more in the circumstances, but she didn't think a warning or intervention would've made a difference to Miss L's decision to go ahead with the payments.

She explained that on 17 January 2022, the combined debits made were the highest amount paid by Miss L. But she noted she'd carried out due diligence on M before proceeding, she'd trusted the person who'd introduced her to M and its website had confirmed it was regulated by the Financial Conduct Authority (FCA), so she didn't think Miss L would have felt there was any cause for concern.

Miss L's representative has asked for the complaint to be reviewed by an Ombudsman. They explained they don't agree an intervention from Halifax wouldn't have made a difference as Miss L has said she would have listened to the bank had they intervened and they don't accept the fact Miss L had performed due diligence means she wouldn't have listened to Halifax. They've argued that Halifax is an expert in financial matters and Miss L would have welcomed the advice and any scam education provided by Halifax especially as she was unaware how common these types of scams are.

They believe that with probing questions Halifax would have realised Miss L was likely falling victim to an elaborate investment scam. It would have learned she discovered the investment opportunity via social media, which would have been an immediate red-flag, as would the existence of a third-party broker acting on her behalf and asking her to make payments to cover commission fees and other taxes. And that with that information, Halifax could have made Miss L aware she was the victim of a scam by providing an effective warning which could have indicated she was being scammed.

The representative had argued these are common hallmarks of cryptocurrency scams and if Miss L had known about this, she'd have acted in the advice she was given. Further, the representative explained that even though Miss L thought M was regulated by the FCA, it doesn't mean she wouldn't have acted on advice.

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 Miss L 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.

CRM Code

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss L says they've fallen victim to, in all but a limited number of circumstances. Halifax had said the CRM code didn't apply in this case because the payments were made using a debit card, and I'm satisfied that's fair and applies to all the payments.

Chargeback

I've thought about whether HSBC could have done more to recover Ms L's payments when she reported the scam to it. Her own testimony supports that she used a cryptocurrency exchange to facilitate the transfers to M. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Miss L'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 the cryptocurrency exchange company was fair.

I'm satisfied Miss L '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 his bank account, Miss L is presumed liable for the loss in the first instance. 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).

I've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. I say this because I've seen evidence of communications between Miss L and the scammer along with Miss L's submissions about the tactics the scammer used to persuade her to invest more money, which are plausible and persuasive, and I'm satisfied this is all consistent with M operating a scam.

But, although Miss L didn't intend her 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 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 exchange company. However, Halifax had an obligation to 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 Miss L when she 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 Miss L from financial harm due to fraud.

The payments didn't flag as suspicious on Halifax's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Miss L normally ran her account and I think they were. Over the nine payments, the largest was the eighth payment, which was £5109.47. Significantly, on 17 January 2022, Ms L made six payments in one day which added up to £10,837.09. By the time Miss L mad the fourth payment that day, she'd paid £5,727.62 in one day which far exceeded her usual spending and I'm satisfied Halifax should have called her to ask her about that payment and the other payments she'd made that day.

During this call I would expect Halifax to have asked some probing questions about the payments including whether there was a third-party involved, how she came into contact with the third-party, whether she'd researched the scam company and the rate of return she'd been promised.

I'm satisfied that if Miss L had been asked these questions, she'd have answered truthfully because there's no evidence of her having misled the bank before or that she was told to do so by the scammers. And, consequently, I'm satisfied that she'd have explained how she came into contact with the broker, the returns she'd been promised and the tactics the broker had used to persuade her to invest more money.

Based on this information, I'm satisfied Halifax would likely have gathered enough information to suggest the investment could be a scam, and I would then expect it to warn Miss L about the risks associated with the investment and explain the investment had some of the hallmarks of a cryptocurrency scam.

However, there were no warnings about M on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites and our investigator has said she doesn't believe a call from Halifax would have made a difference to Miss L's decision to go ahead with investment.

I've carefully considered this and while I accept M was advertised on social media and promised high returns, there were no checks which Halifax could have recommended which would have confirmed it was operating a scam. I accept Miss L didn't have a history of high risk investing and that she would have taken Halifax's advice seriously, but she trusted the broker who she said had appeared knowledgeable and competent and had lots of followers on social media, and she was convinced by the professional looking website, in particular the fact she'd had to provide ID verification before opening the account and the live chat option. She was also confident the investment was legitimate because the broker had been recommended by a friend who she trusted and I think that, on balance, in the absence of actual evidence that M was operating as a scam, she would probably have gone ahead with the investment, notwithstanding a scam warning from Halifax.

Overall, I accept Halifax missed an opportunity to intervene but, on balance, I think it's unlikely an intervention from Halifax would have made a difference to Miss L's decision to go ahead with the payments.

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 Miss L to accept or reject my decision before 25 July 2023.

Carolyn Bonnell
Ombudsman