DRN-4394086

The complaint

Ms Y complains that Halifax didn't 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 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.

On 25th June 2022, Ms Y received a message on social media from someone claiming to work for a company I'll refer to as "C", who I will refer to as "the scammer". The scammer said they were recruiting for online part-time investment assistants and Ms Y had been looking for employment, so she responded to the message.

The scammer told Ms Y she could work from home by investing her own money into cryptocurrency and that she could receive a commission of £120-£130 for a £100 investment and £360-£390 for a £300 investment. Ms Y provided her details to the scammer and was given a link to a trading platform, and details of a 'mentor'. She contacted the mentor who said she must follow their instructions to win investment revenue.

After Ms Y had completed her first task, she received a credit of £20. She was then instructed to purchase cryptocurrency by transferring money through "S" and transferring it onto the trading platform. She made several payments from another account before transferring £6 and £1,800 from her Halifax account on 4 July 2022.

When she decided she wanted to make a withdrawal, she was told she'd have to pay £4,000 within 24 hours or further fees would be added. So, she borrowed £3,000 and made the payment from her Halifax account, but the mentor said she'd have to pay a more fees.

Ms Y realised she'd been the victim of a scam when she was unable to raise any more money and she lost contact with the broker. She complained to Halifax arguing the transactions were out of character as they were much larger than her standard monthly payments and were transferred to a payee that was associated with cryptocurrency.

She told Halifax she was suffering financial difficulties, and it should have known this because she was a long-standing customer. She said it didn't warn her she could be the victim of fraud and it didn't complete adequate checks in relation to the identity of the recipient account.

Her representative said Halifax failed to stop the payments and complete investigations into any fraud concerns or to discuss the basis of the transactions before releasing the funds to the recipient account.

Halifax refused to refund any of the money Ms Y had lost. It said she didn't carry out any checks on C, or query how they had got her contact details or why they were contacting

people in the UK when they are based in America. And it said that if she'd googled the phone number, she'd have seen a warning that C was associated with a scam.

It said the first payment was for £6, so she didn't receive an online scam warning. And the other two payments were within her normal spending pattern, so it didn't miss an opportunity to intervene. It said it was signed up to the Contingent Reimbursement Model ("CRM") code, but as the money was going to an account in M Y's name, it wasn't covered by the code.

Ms Y wasn't satisfied and so she complained to this service with the help of her representative. They disagreed the payments weren't covered under the CRM on the basis Halifax would have been fully aware the payments related to cryptocurrency and should have been deemed high risk.

The representative said the transactions were out of character as they were larger than her historic transactions and the payee was out of the norm for payments from her account. They explained Ms Y was desperate for a job and had accepted the opportunity as she was in financial difficulties. She doesn't know how the scammer got her details, but she had completed online job searches and applications. She's never been a victim of fraud and had no investment experience, so she didn't know to check the FCA website.

Our investigator didn't think the payments were unusual when compared to Ms Y's regular account activity, so she didn't think Halifax missed an opportunity to intervene. She accepted the payment of £1,800 reduced the account balance significantly, but she said Ms Y regularly entered her overdraft, so this wasn't unusual.

Ms Y has asked for her complaint to be reviewed by an Ombudsman. Her representative doesn't agree £1,800 and £3,000 weren't unusual as she rarely made transactions over £900, so the fraudulent sums were out of character. They also reiterated the recipient bank was out of the norm and argued that Ms Y doesn't regularly enter her overdraft.

They further argued Halifax ought reasonably to have considered the initial payment was out of character for Ms Y's account as it was towards the top end of the value of transactions, and it was associated with cryptocurrency. They have stated Ms Y's statements show the average outgoing payment in June 2022 was £110, so £3,000 was an increase of approximately 2,627% and ought to have flagged as suspicious. They accept Ms Y made some large payments in the twelve months before the payments, but argue these were to well-established payees and friends, as opposed to unregulated cryptocurrency platforms.

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 Ms Y 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.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Ms Y says she's fallen victim to, in all but a limited number of circumstances. Halifax said the CRM code didn't apply in this case because the payments were to an account in Ms Y's own name, and I'm satisfied that's fair.

I'm also satisfied Ms Y '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, Ms Y 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. But, although Ms Y 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 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 Ms Y 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 Ms Y 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 Ms Y normally ran her account, and I don't think they were. This is because all the payments were to a legitimate payee and none of them were for particularly large amounts, nor were they out of character for the usual spending on the account.

The first payment was only £6, so even though it was to a new payee which was associated with cryptocurrency, it wasn't unusual for the spending on the account, and I don't think it ought to have triggered Halifax's fraud systems.

By the time Ms Y made the second and third payments, the payee wasn't new, and they weren't so large that Halifax needed to intervene. I note Ms Y's representative has said the £1,800 payment took her into her overdraft, but this wasn't the first time her account had been in overdraft, so it wasn't cause for concern. Her representative has also said it was unusual for Ms Y to pay a cryptocurrency merchant, but it was a legitimate company who Ms Y had paid before, so I don't accept the payments were suspicious.

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 Ms Y has lost money and the effect this has had on her. 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 Ms Y to accept or

reject my decision before 9 November 2023.

Carolyn Bonnell
Ombudsman