DRN-4416744

The complaint

Miss W complains that Bank of Scotland plc trading as Halifax didn't do enough to protect her from the financial harm caused by a scam, 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.

In September 2022, Miss W received a call on her landline from a withheld number. She spoke to someone I'll refer to as the "the scammer" claiming to be a police officer who told her there was fraudulent activity on her account and Halifax was involved, so she couldn't tell it about the call.

The scammer asked Miss W if she had made a transaction of £5,000 to an overseas recipient, which she had not. As she was concerned the call might be a scam, the scammer told her to call 999. She spoke to an operator who transferred the call to someone who said he was an officer in the fraud unit. He explained they suspected Halifax staff were passing counterfeit currency through its branches and some customer accounts had been compromised.

The scammer asked if Miss W would assist by going to her local branch to withdraw £6,000 in cash. They would then check the cash to see if it contained any counterfeit notes. She was told she'd probably be asked why she was making the withdrawal and that it was important to say the money was for building work as it would alert the suspects if she said she was assisting a police investigation. The scammer also asked her to stay on the phone with him throughout.

Miss W first went into her local branch and asked to withdraw £6,000. She was told the maximum she could withdraw without prior notice was £2,500. She was also asked what the money was for and she said it was for building work. She was then allowed to withdraw £2,500 in cash.

Miss W then used the ATM to withdraw a further £500 before attending another branch and asking to withdraw £2,500. The cashier noted she'd already withdrawn £2,500 over the counter and she was refused the cash.

At this point, the scammer instructed Miss W to go to her local supermarket to withdraw some Euros, but the exchange had closed. When she arrived at the next exchange, she paid for £2,000 worth of Euros using a debit card connected to her Halifax account, before attending a third exchange at another supermarket where she paid for a further £1,000 worth of Euros.

When Miss W got home, the scammer asked her to put gloves on and read out the serial numbers of four notes from each withdrawal. He confirmed there were a number of counterfeit notes and that they were now Police property. He said she would be reimbursed

later that day and asked if she would take the money to Scotland Yard, which she refused to do. He then said he would send a courier to collect the cash and when a vehicle pulled up she handed over the cash in several envelopes in a clear zip seal bag.

She contacted Halifax when she realised she'd been scammed. She said it had failed to have scam conversations with her when she attended the branches. She accepted she was instructed to lie, but she said that if she'd been asked if she'd been pressured to withdraw funds or if she'd received any phone calls, the scam could have been prevented. She said the activity was unusual and Halifax missed an opportunity to intervene when she was in the second branch.

Halifax refused to refund any of the money. It said it could have carried out an investigation sooner, but it maintained the outcome would have been the same. It explained the Contingent Reimbursement Model (CRM) code doesn't apply to cash withdrawals or debit card payments and there were red flags which should've alerted Miss W to the fact she was being scammed, including the fact she was told to call 999 and to withdraw Euros.

It said the transactions weren't flagged as high risk or unusual because Miss W said the money was for building work, so it had no reason to question her further or give scam education. Further, it said the debit card payments were made using her card and PIN and wouldn't be classed as high risk.

Miss W wasn't satisfied and so she complained to this service. She said she had called 999, so she did take steps to protect herself. She didn't notice any scam posters in the branch and she originally asked to withdraw £6,000, so she should have been questioned about the amount at that point. She explained she finds it difficult to think clearly in certain situations and she fell for the scam because Halifax failed to educate her about scams.

Halifax said Miss W had followed the instructions of the scammer and lied to branch staff when she was asked why she was withdrawing the cash, which prevented it from identifying and alerting her to the scam. It said she should have questioned why she was being asked to lie to the bank and why she was told to withdraw Euros from several different places, including somewhere that no longer existed. It maintained Miss W didn't do enough to protect herself and that she should have been concerned about the fact the scammer's story changed three times and she was asked to take the counterfeit notes to Scotland Yard rather than the station the officer had claimed to be calling from. Finally, it said the payments were made using chip and pin so it had no reason to be concerned that they weren't authorised.

Our investigator didn't think the complaint should be upheld. She didn't think the payments were particularly unusual or suspicious considering Miss W's normal account activity, noting she'd made similar payments from her account including £1,459 on 11 January 2022 and £2,814 on 28 January 2022. She also noted Miss W wasn't honest during her interaction with Halifax when she made the cash withdrawal and she didn't think it missed an opportunity to identify the payment was being made in relation to a scam as she had provided a plausible reason for making the withdrawal.

Further, she was satisfied the questioning was proportionate to the risk in terms of the amount Miss W was trying to withdraw and she didn't think more questioning would have made any difference.

She explained she'd seen nothing to suggest that Miss W told Halifax about her mental health or her mother's passing so it wasn't in a position to better protect her or put specific measures in place. And finally, she explained that recovery wasn't an option as Miss W handed the funds to the scammer.

Miss W has asked for her complaint to be reviewed by an Ombudsman. She's said the payments she made on 11 January 2022 and 28 January 2022 were her mother's funeral costs which she paid with a debit card ad not cash, and there were no other large payments on her account.

She believes £6,000 was highly unusual. And she maintains that she was concerned but she'd called 999 and spoken to someone she thought worked for the police, which had reassured her. She felt she had no choice but to hand the money over when she was told it was now police property.

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 W 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 Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams. Halifax has said the CRM code didn't apply in this case because it doesn't apply to cash withdrawals or card payments, and I'm satisfied that's fair.

There's no dispute that Miss W was scammed, but although Miss W didn't intend her money to go to scammers, she did withdraw the funds and hand it to the scammers. However, 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 and these transactions were made by Miss W as a result of a scam, so I need to consider whether it ought to have intervened to warn her when she tried to make the withdrawals.

If there are unusual or suspicious payments on an account, I'd expect Halifax to intervene with a view to protecting Miss W from financial harm due to fraud. Miss W has said that it was unusual for her to her to have asked to withdraw £6,000 in cash and I agree she doesn't have a history of making high-value cash withdrawals. But she was only allowed to withdraw £2,500, and I agree with our investigator that the transactions of £1,459 on 11 January 2022 and £2,814 on 28 January 2022 mean £2,500 were for similar amounts. I note Miss W has said the January payments were for funeral expenses but I'm afraid the purpose of the payments doesn't alter the fact there was a history of similar spending on the account.

In any event, I'm satisfied Miss W was questioned about the withdrawal when she attended the first branch and as she said she was paying for building work, Halifax was prevented from identifying that she was withdrawing the money with the intention of passing it to scammers. Unfortunately, in the circumstances, I don't think there was anything else it could reasonably have done or asked which would have uncovered the scam at that point and I'm satisfied the intervention was reasonable and proportionate to the risk. So, there wasn't anything else Halifax could reasonably have done to prevent the scam.

After making the first withdrawal, Miss W made a cash withdrawal from an ATM. She then attended a second branch where she tried to make a second cash withdrawal but was prevented from doing so because £2,500 was the maximum she could withdraw in branch without notice. I'm satisfied that was reasonable and having told her she was unable to make the withdrawal there would have been no reason to provide warnings or scam education.

On the instructions of the scammer, Miss W then made two further transactions using her debit card. As these transactions were made using chip and PIN and there's no dispute that they were done by Miss W herself, I'm satisfied the transactions were authorised and that there was nothing further Halifax could have done to protect her from the scam or that it missed any further opportunities to intervene.

Recovery

There was no realistic prospect of a successful recovery because Miss W handed the cash to the scammer.

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 Miss W 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

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 W to accept or reject my decision before 23 April 2024.

Carolyn Bonnell
Ombudsman