DRN-4809854

The complaint

Mr and Mrs D complain that Bank of Scotland plc trading as Halifax ('Halifax') won't reimburse the money they lost when they fell victim to a scam.

What happened

Mr and Mrs D hold a joint account with Halifax and are represented in this case.

As Mrs D was involved in the scam, I'll mainly refer to her in my decision.

Mrs D says that in early July 2023 she provided her account details in response to an email about her television license which she now knows was fake. On 17 July 2023 Mrs D received a phone call from someone who claimed to be from Halifax's fraud department. Mrs D didn't know it at the time, but the call was from a scammer. The caller told Mrs D that the email she had received about her license was fraudulent and her bank account was compromised, meaning her funds weren't safe. As a result, Mrs D was told she needed to move her funds to protect them.

Mrs D was advised to install a screen sharing app so that the scammer could guide her through the process. She was asked to open a new 'safe' account at a cryptocurrency exchange I'll refer to as C and to transfer £1,200 to the newly opened account. Mrs D was then asked to open another 'safe' account at a bank I'll refer to in this decision as K and transfer further funds as set out in the table below.

Date	Time	Amount	Payee
17/07/23	18:52	£1,200	C
17/07/23	19:34	£3,400	K
17/07/23	19:40	£3,890	K
17/07/23	19:44	£3,890	K
17/07/23	19:46	£2,400	K
Total		**£14,780**	

Soon after making the transactions Mrs D's husband came home and saw that she was in a state of panic. He asked the scammer what was happening, at which point the scammer terminated the call. Mrs D reported what had happened to Halifax.

Halifax didn't agree to reimburse Mr and Mrs D. It said it hadn't made any errors and didn't stop the transactions as they were in line with normal spending on the account. Halifax also said that Mrs D could have done more to protect herself.

Mr and Mrs D were unhappy with Halifax's decision and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He said that the first two transactions didn't stand out as unusual given the previous activity on the

account. The position changed when the third payment was made, and Halifax should have intervened. But Mrs D has already received £10,180.96, which is more than he would recommend as he felt a 50% deduction was fair.

Mr and Mrs D didn't agree with the investigator's findings, so the complaint has been passed to me to review. They said that Halifax should have intervened from the outset and at the latest when the second payment was made. Had it done so, Mr and Mrs D believe that intervention would have made a difference and prevented the loss.

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.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

The Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case because it only applies to payments to another person and Mrs D made payments to accounts in her own name.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr and Mrs D's account is that they are responsible for payments either one of them has authorised. It's not disputed that Mrs D made and authorised these payments so I need to decide whether Halifax acted fairly and reasonably in its dealings with Mrs D when she did so, or whether it should have done more before processing them.

Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.
- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

In this case £1,200 went from Mr and Mrs D's joint account to C and £13,580 went from Mr and Mrs D's Halifax account to Mrs D's new account with K. K has refunded £8,193.51 and at the point K blocked Mrs D's account there was a balance of £1,986.49. So, the only losses from Mr and Mrs D's account that haven't been refunded are £1,200 to C and a further £3,400 to Mrs D's account with K. These are the only transactions I will discuss in this decision.

I consider that at the time the payment was made to C, banks should have been aware that payments for cryptocurrency carry an elevated risk. But many transactions to cryptocurrency exchanges are legitimate and I'm not satisfied that a one off, low value payment that is in line with usual account activity ought to have caused Halifax sufficient concern that it needed to intervene when it was made. Mr and Mrs D had made transfers of much higher values in the 12 month period before the scam took place.

I also don't consider the £3,400 transaction to an account with K was so unusual and out of character that Halifax ought reasonably to have done anything more when it was made. Mr and Mrs D made a transfer of £5,194 in January 2023 and had transferred £8,000 to what appears to be their business account a few days before the scam transactions. In the circumstances, I can't reasonably conclude that Halifax ought to have had concerns about a transfer of £3,400 to an account in Mrs D's name.

There's a balance to be struck; firms have obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments.

Mr and Mrs D's representative has said she was vulnerable at the time of the scam and her vulnerability affected her decision-making. Whilst I'm sorry to hear about this, I've not seen any evidence to suggest Halifax was made aware. And as the CRM Code doesn't apply to this case, I can't consider its provisions in respect of vulnerability here.

Overall, whilst I appreciate my decision will disappoint Mr and Mrs D, I can't reasonably ask Halifax to reimburse their loss.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D and Mrs D to accept or reject my decision before 10 July 2024.

Jay Hadfield
Ombudsman