DRN-3856626

The complaint

Mr D complains that Bank of Scotland plc (trading as "Halifax") won't refund £21,750 he lost to a bank impersonation scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Mr D fell victim to a bank impersonation scam in July 2022. He was contacted by someone purporting to be from the Halifax fraud team ("the scammer"), who said that someone was attempting to take out an £18,000 loan at his local branch. The scammer told him there were 22 similar cases of fraud that had occurred in the same branch and that they were investigating the staff that worked there.

Mr D was told that in order to counteract the fraudulent loan application, he would need to take out an £18,000 loan himself, and that he would need to send the money to a new account they had set up for him under the dummy name of "Marius Rugu". Mr D applied for the loan through his mobile banking and was coached through what to do by the scammer, such as selecting the reason for the loan as "home improvements", which he was told to always tell the bank if questioned so as not to tip off the branch staff.

The loan was approved, and Mr D made the following payments (which included money from his own savings account):

Date	Payee	Amount	Payment method
7 July 2022	Marius Rugu	£17,750	Faster payment
7 July 2022	Marius Rugu	£4,000	Faster payment

Halifax intervened and questioned Mr D about the payments he was making, where he was asked to come into his local branch to discuss what they were for. But in line with the scammer's instructions, Mr D explained that they were towards home improvements, so Halifax didn't consider him to be at risk of falling victim to a scam.

Mr D reported the fraud to Halifax after he realised he had been scammed. Halifax considered his claim under the Contingent Reimbursement Model (CRM Code) but said he wasn't eligible for a refund. It said it had provided Mr D with an effective warning in line with its obligations under the Code and said that Mr D didn't have a reasonable basis for believing the payments to be genuine. Mr D complained this was unfair and was also unhappy that he was being held liable to repay the loan he was tricked into taking out as part of the scam.

Our investigator didn't uphold Mr D's complaint. She was satisfied that Halifax had assessed the claim fairly and that it could rely on the exceptions to reimbursement under the CRM Code. She also didn't think it was unfair for Mr D to be held liable for the loan given he had

applied for it and received the proceeds.

Mr D disagreed, so the matter has been escalated to me to determine.

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 agree with the conclusions reached by the investigator and have decided not to uphold it for the reasons set out below.

It isn't in dispute that Mr D has fallen victim to a scam here. It also isn't disputed that he authorised the faster payments he made to the scammer's account. The payments were requested by him using his legitimate security credentials provided by Halifax, and the starting position is that banks ought to follow the instructions given by their customers in order for legitimate payments to be made as instructed.

However, I've considered whether Halifax would be liable to refund any the payments Mr D made in line with its obligations under the CRM Code.

Under the provisions of the CRM Code, both the bank and its customer have obligations. If it can be shown that the customer has met their requisite level of care, then they will receive full reimbursement. If the customer has not done this, then it is for the firm to show that it has met its obligations under the Code, one of which is the provision of an Effective Warning when the firm identifies an APP scam risk in a payment journey. If a firm has not met its obligations then it, subject to any liability by the bank which received the money, will be liable for 50% of the customer's loss.

In this case, Halifax has argued that exceptions to reimbursement under the Code apply such that none of the payments Mr D made would qualify for reimbursement. It says that it provided him with an effective warning under the Code, which Mr D ignored. It also said that Mr D lacked a reasonable basis for believing the payments or payee to be genuine, and therefore did not meet his requisite level of care.

Did Mr D have a reasonable basis for belief when making the payments?

Having reviewed this aspect, I'm satisfied there was enough going on from the outset that should have given Mr D serious cause for concern that something wasn't right:

- I appreciate the number Mr D was called from had been spoofed to appear as though it was a genuine call from the bank. But I don't think this ought to have been enough to satisfy him that he was speaking to his genuine bank. It doesn't appear as though the caller knew any account specific information, or carried out any sort of caller verification to demonstrate it was in fact a genuine call. The caller also had to ask questions such as how much Mr D held in his account, and whether he had made payments to anyone else recently, which his genuine bank would not need to ask as they would already have access to this information. So, I don't think Mr D should have readily accepted that he was speaking to his bank in these circumstances.

- I also don't consider it was reasonable for Mr D to think he would have to take out a loan himself in order to *stop* an allegedly fraudulent loan application from being granted, or that he would need to send it to an account in another name for safe keeping. If there were any concerns about his account being compromised, then a genuine bank would have taken steps to block the account. It would not have asked

him to continue making payments from it, and it certainly wouldn't have set up another account for him under someone else's name.

- Mr D was told by the scammer to lie to Halifax and give a fake reason in order to obtain a loan. The fact that he was being told to lie in order to obtain finance should have given him significant cause for concern, as he was essentially being asked to obtain the loan by fraudulent means. And I don't consider it reasonable to think that a genuine bank would ever ask its customers to do something like this.

- Mr D didn't appear to question that he was being asked to send a significant amount of money to an account that was not in his name, and which he did not have access to at the time he was making the payments.

So, with all the warnings signs present here, I don't consider that Mr D had a reasonable basis for belief when making the payments and I'm satisfied Halifax has correctly demonstrated that this exception to full reimbursement under the Code applies.

Did Halifax meet the standards expected of a firm under the CRM Code?

Even though I don't think Mr D had a reasonable basis for belief when making the payments, he would still be entitled to a refund of 50% of the money he lost if Halifax didn't meet the standards it has agreed to adhere to under the CRM Code.

The CRM code says that, where a firm identifies APP scam risks, it should provide "Effective Warnings" to their customers. It sets out that an Effective Warning should enable a customer to understand what actions they need to take to address a risk and the consequences of not doing so. And it says that, as a minimum, an Effective Warning should be understandable, clear, impactful, timely and specific.

It isn't in dispute that an APP scam risk was identified here, given that Halifax blocked both payments Mr D made as part of the scam and spoke to him about them. Accordingly, it's just a question of whether it did enough to ensure it provided an Effective Warning.

When Mr D set up the first scam payment through his mobile banking app, he was asked to provide the reason for the payment, to which he selected "invoice or bills". It generated a bill payment scam warning, and the transaction was stopped by Halifax, where it asked him to get in touch with the bank. Mr D called Halifax from his mother's phone while keeping the scammer on the other line through his own phone so they could tell him what to say. When asked what the payment was for, Mr D said he had taken out a loan for home improvements (in line with the scammer's instructions), and said he was paying for building work. Halifax asked if he had been contacted by the bank asking him to move money, or if he had been asked to lie to the bank, to which he said he hadn't.

After receiving a scam warning from Halifax, Mr D said he would try making the payment by debit card as this would be safer. He then attempted to make the payment again via faster payment, which was stopped a further time by the bank. Mr D said that the builder working on his house would not accept debit card payments. He explained how he knew the builder and that he had completed work on his neighbour's house, but the bank was concerned that he didn't have any paperwork, so they asked him to visit his local branch.

Mr D then called Halifax again from his local branch, while the scammer was listening in through the phone in his pocket. He was questioned further about the building work, but Mr D assured the representative that he knew the builder.

Mr D was asked again if anyone had asked him to lie about the payments. Halifax explained

that scammers will often pretend to be from the bank and would ask their victims to take out loans and move money. It said they would tell him to lie to about the reasons for moving the money if questioned and asked if he had received any suspicious phone calls like this, to which he again said he hadn't and that he was not being asked to lie to the bank, despite this being the exact scenario that was unfolding. It also warned him of the consequences of proceeding with the payment and said that he would not be able to get his money back. The Halifax representative googled the name of the payee and saw that it was associated with a building company based in London. As Mr D had not been honest with Halifax, it didn't have any further concern that the payment was related to a scam, and it was released.

Halifax also spoke to Mr D when he attempted to make a transfer of £3,700 from his savings account. It stressed to him that it was important he was being honest, and it asked him again if he had received any unusual calls, or if he had been asked to lie to the bank. It again warned that he wouldn't be able to retrieve the money once it had left his account, which Mr D acknowledged, and the second payment was released.

Overall, in the circumstances of this case, I'm satisfied the warnings Halifax gave to Mr D in relation to each payment was understandable, clear, impactful, timely, and specifically identified the type of APP scam that he risked losing his money to, such that it can be considered an "Effective warning" under the CRM Code. Mr D ignored the warnings he was given, and I'm satisfied this was material to the success of the scam. As a result, I'm satisfied it has established this exception to reimbursement as well, meaning it does not need to refund any of the payments in this case.

Even if it couldn't be considered an Effective Warning and that Halifax ought to have done more for it to be regarded as such, I don't think it would have ultimately prevented the scam in any event. This was because Mr D did not give honest answers to the questions he was being asked, which would have prevented Halifax from providing an Effective Warning in line with the Code. And despite being warned several times not to make the payment if anyone from the bank asked him to move money, it appears Mr D already understood the scam risk and would 've likely gone ahead regardless of what Halifax did or didn't do.

I've also thought about whether Halifax could've done anything more to recover the funds after Mr D reported the scam. However, I can see that it reached out to the beneficiary bank soon after the scam was reported, but it was unable to recover any of the money. So, I don't think it could've done anything further here.

Has Halifax acted fairly by holding Mr D liable to repay the loan?

As part of the scam, Mr D took out an £18,000 loan under the instruction of the scammer, which he is now having to repay. I've therefore considered whether it's fair and reasonable for Halifax to expect him to pay this back, or if it should write the debt off.

Section 83 of the Consumer Credit Act (CCA) 1974 sets out that a person won't be held liable for a debt if it was taken out by another person who wasn't acting as their agent. But in this instance, the loan wasn't fraudulently taken out by anyone else. I accept Mr D was tricked into taking it out, but ultimately, he knew he was applying for a loan and also misled the bank as to its purpose.

Mr D received this money into his account, which he would've known were the proceeds of the loan that would need to be paid back with interest. He didn't take any action to try and return the funds to Halifax and instead transferred them to an account that wasn't in his name, and which he had no control over. As a result, I don't think it would be fair and reasonable to ask Halifax to write off the debt in these circumstances.

I appreciate this will likely come as a disappointment to Mr D, and I'm sorry to hear he has been the victim of a cruel scam. However, I'm not persuaded Halifax has acted unfairly in these circumstances.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 5 December 2023.

Jack Ferris
Ombudsman