DRN-3190957

The complaint

Mr C complains that Bank of Scotland plc trading as Halifax (Bank of Scotland) won't refund the money he lost when he was the victim of a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. But in summary and based on the submissions of both parties, I understand it to be as follows.

In December 2020, Mr C has said that he received a call from somebody claiming to be from Bank of Scotland. He's said the caller took him through verification and then asked him if he recognised some transactions on his account. Mr C told the caller he didn't recognise them and was told that, in order to keep his money safe, his account would need to be closed and he would need to move his money to another account. Mr C has told us that he'd previously been the victim of fraud, and so thought this might have happened again.

Mr C told Bank of Scotland that it was an 0800 number that had called him, but that he hadn't verified the number. He later went on to tell our service that the caller had asked him to check the number, he was being called from, was the same as on the back of his Bank of Scotland card.

Unknown to Mr C at the time he was speaking to a fraudster. But believing everything to be genuine and thinking his money was at risk, Mr C went ahead and made the following payments, totalling £926.45, from his Bank of Scotland accounts, to account details that the fraudster provided;

8 December 2020	@ 14:06	£550.00 (from savings account)
8 December 2020	@ 14:07	£ 94.08 (from savings account)
8 December 2020	@ 14:09	£182.37 (from current account)
11 December 2020		£100.00 (from current account)

The fraudster told Mr C that an appointment had been arranged for him to visit his local branch on 12 December 2021. When he attended the branch as arranged, it became apparent that there was no appointment, and the scam came to light.

Mr C raised the matter with Bank of Scotland. Bank of Scotland is a signatory of the Lending Standards Board Contingent Reimbursement Model (the CRM code) which requires firms to reimburse customers who have been the victims of authorised push payment scams like this, except in limited circumstances. Bank of Scotland investigated Mr C's complaint and issued its final response in February 2021, not upholding the complaint as it said one or more of the exceptions applied.

In summary, it said Mr C had made the payments without a reasonable basis for believing they were genuine and that he had ignored effective warnings at the time the payments were made, so he wasn't entitled to a refund under the CRM code.

Unhappy with Bank of Scotland's response Mr C brought his complaint to this service. One of our investigators looked at Mr C's complaint and thought the complaint should be upheld. In summary, this was because they didn't think Bank of Scotland had established that Mr C had ignored an effective warning, or made the transfer without a reasonable basis for believing it was legitimate. So she felt Mr C was entitled to a full refund under the CRM code and the Bank of Scotland should refund him the money he lost, along with interest.

Bank of Scotland didn't agree with our investigator's opinion. In summary, it maintained that Mr C didn't have a reasonable basis for belief when he made the payments. It added that he'd ignored warnings about this type of scam, and a warning that the payee name and account details didn't match.

As agreement couldn't be reached the complaint has now been passed to me for a decision.

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 considered everything, I'm satisfied that:

- Under the terms of the CRM Code, Bank of Scotland should have refunded Mr C the full amount he lost. And I am not persuaded any of the permitted exceptions to reimbursement apply in the circumstances of this case.

- In the circumstances Bank of Scotland should fairly and reasonably now refund Mr C the money he has lost.

I have carefully considered Bank of Scotland's representations about the warnings it gave and whether Mr C had a reasonable basis for believing the transaction to be genuine. But they do not persuade me to reach a different view. In particular I am not persuaded that Mr C failed to take the requisite level of care required for Bank of Scotland to choose not to reimburse under the terms of the CRM Code. I'll explain why;

Effective Warnings

Under the provisions of the CRM Code, as a minimum, an "effective warning" needs to be understandable, clear, timely, impactful and specific. It must also provide information that gives customers a better chance to protect themselves against being defrauded and should include appropriate actions for customers to take to protect themselves from APP scams.

Bank of Scotland has provided a copy of the warning it said it presented to Mr C, before he made the first payment to the fraudster;

did you know?
- *We'll never call to ask you to move your money to another account.*
- *if you buy something online, pay by card.*
- *Before you pay an invoice, double-check the account number, sort code and name.*

Mr C has said that he does not recall seeing the warning and that he was following the instructions of the fraudster, who was telling him what options to select.

The CRM Code sets out minimum criteria that a warning must meet to be an 'effective warning'. In very broad terms, it requires that a warning will be capable of countering the typical features of the generic scam type identified during the payment journey.

But I don't find the warning given by Bank of Scotland meets the definition of an effective warning. The warning that was presented doesn't meet all those requirements. For one, it doesn't make it clear that any money sent as a result of a scam would be lost and likely irrecoverable. And while I appreciate that the warning Bank of Scotland gave here was, in part, relevant to the type of scam Mr C fell victim to, in that it does mention that it would never ask a customer to move money to another account, it does so in amongst other potential types of scam and is not specific to the circumstances Mr C found himself in. I don't think this wording is specific enough about what the scam would look or sound like, to make it clear to Mr C that this was the type of scam he could be falling victim to. It doesn't mention the caller saying the account is at risk of fraud or the need to move money to a safe account.

Bank of Scotland has also highlighted that it presented Mr C with a 'Confirmation of Payee' (CoP) warning indicating that the name of the account he was paying didn't match. I think it is important to distinguish an 'effective warning' and negative CoP results under the CRM Code. Effective warnings are intended specifically to address the risk of, and enable customers to protect themselves from, APP scams. As I've explained above, an effective warning must, as a minimum, meet the definition under the Code – that is to be understandable, clear, impactful, timely and specific. Messages accompanying negative CoP results, though sometimes mentioning the possibility of fraud (although from looking at the message Bank of Scotland presented this didn't mention fraud) are primarily intended to warn customers that payment details do not match (as was the case here) so as to warn customers about the risk of misdirecting a payment.

Overall, while I acknowledge Bank of Scotland provided a warning (albeit I have already explained why I don't find this to have been an effective warning) and a negative CoP result within the same payment journey, I don't find the two together to be sufficient to amount to an effective warning in this particular case.

Did Mr C have a reasonable basis for belief?

I have also carefully thought about Bank of Scotland's representations about whether Mr C had a reasonable basis for belief. Overall they do not persuade me to reach a different view. I say that because;

- Mr C had previously fallen victim to card fraud and where the fraudster, here, told him that his card would be cancelled Mr C, albeit maybe incorrectly, likened the scenario the fraudsters portrayed, to something he had previously experienced. So, I think it is understandable and not unreasonable why he may have thought what was happening seemed plausible, given it was consistent with his recollections of a genuine conversation he'd had with his bank previously about a fraud matter.

- It follows, that I think it reasonable that he could have considered his bank would genuinely want to discuss matters with him if his accounts were at risk.

- Bank of Scotland has said that when Mr C had been the victim of fraud before it had educated him about the risks of fraud. But I note from the information that Bank of Scotland has provided that at the time, the education it gave did not cover the possibility of fraudsters impersonating a customer's bank.
- I don't think Bank of Scotland has given enough consideration to the fact the fraudster had created an environment where Mr C thought he had to act quickly to protect his accounts from an attack. With the benefit of hindsight and the removal of the pressured environment, it's easier to identify elements where Mr C may have had an opportunity to ask further questions. But the convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day, they might not otherwise take. Especially in the

absence of a warning around how these scams typically feel and play out.

- I'm also mindful that Mr C was being coached by the fraudster and was following their instructions. I think this would reasonably have given some credibility to the fraudster being knowledgeable of the bank payments systems and coupled with Mr C being put under time pressure, to make a payment to protect his money, I think it's understandable that he acted in the way he did.

Given the specific circumstances of this case I do think it is finely balanced, but overall I'm not persuaded Bank of Scotland has established Mr C didn't have a reasonable basis for belief that he was making legitimate payments. It follows that I'm not persuaded the exception for reasonable basis for belief applies to the payments Mr C made and that Bank of Scotland can choose not to reimburse Mr C.

Putting things right

Bank of Scotland should now;

- Refund Mr C the money he lost, being £926.45.

- Pay 8% simple interest per annum on the amount that was transferred to the fraudster from Mr C's current account, from the date it declined Mr C's claim under the CRM Code to the date of settlement.

- Pay interest at the savings account rate, on the amount that was transferred to the fraudster from Mr C's savings account, from the date it declined Mr C's claim under the CRM Code to the date of settlement.

My final decision

My final decision is that I uphold this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 30 August 2022.

Stephen Wise
Ombudsman