DRN-3495666

## The complaint

Ms R complains that Bank of Scotland plc trading as Halifax hasn't refunded her the money she lost as the result of a scam.

## What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them in detail here. But briefly, both parties accept that Ms R was the victim of a scam when she made a Faster Payment transfer for £3,250 in December 2020.

She did so in the belief that her Halifax account was at risk, and that she was acting to protect her money. This belief was based on a telephone call she'd received, purportedly from Halifax.

Ms R says this call was not wholly unexpected. She'd called the bank a few days earlier to report that, having received an email that appeared to be from the DVLA, she'd input her details onto what she thought was a DVLA webpage. But she now had concerns that her personal details might have been compromised (in what's known as a 'phishing' attack).

When Ms R had called the bank to report her concerns she'd explained what happened, before being transferred to the fraud team. However, having been placed on hold for an hour, she'd been unable to hold on longer and had to end that call. She'd therefore been expecting the fraud team might call her back to follow up on this.

Ms R explains that the call she later received happened at an inconvenient time - she was just getting ready to leave the house for the evening. But given the importance of protecting her funds she continued.

She noted that the caller's number matched Halifax's number. The caller knew Ms R's account number and sort code and it sounded like she was speaking to her bank. Ms R explains this was all consistent with the call being genuinely from her bank and she didn't doubt this at the time.

Unfortunately, the call was from a fraudster impersonating the bank, who had been able to mimic (or spoof) the bank's phone number to make it appear that the call originated with Halifax.

Ms R was talked through what she needed to do to protect her funds. She was told a new account had been set up in her name and was given the new sort code and account number to use.

Ms R set up the new payee details on her mobile banking app. It wasn't possible for Halifax to check the name against the receiving bank account – because the recipient bank didn't support the confirmation of payee system. So, when Ms R had input her own name as the payee name, this didn't result in a warning saying the name didn't match (in other words that it wasn't her account) – just that Halifax hadn't been able to check the name.

Halifax says it displayed a scam warning before Ms R completed the payment. However, Ms R doesn't recall seeing this.

Money remained in Ms R's account after this payment had been made. Ms R was told to make a further payment (to the same destination) which would have mostly cleared the balance. When she attempted to make this, Halifax says it identified this second payment attempt might be fraudulent and blocked it from being made.

When Ms R told the caller that the second payment hadn't succeeded, the person she'd been speaking to ended the call. Ms R began to realise something wasn't right. She called Halifax and the scam was identified. Halifax attempted to retrieve the funds, but none remained in the recipient account.

Halifax is a signatory of the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code). The CRM Code requires firms to reimburse customers who have been the victims of APP scams (such as this) in all but a limited number of circumstances. Halifax says one or more of those exceptions applies here. It had given Ms R a scam warning when she made the payment. And it said Ms R had made the payment without having a reasonable basis for believing she was protecting her money. Halifax said it did not need to refund Ms R.

One of our Investigators looked into Ms R's complaint and thought it should be upheld. The Investigator didn't think Halifax had fairly assessed her claim under the CRM Code. He didn't agree that Halifax had been able to establish Ms R made the payment without a reasonable basis for believing what she did, or that she'd ignored an effective warning.

Halifax maintained its position. In particular, it disagreed that the warning it had given wasn't enough to alert Ms R to this being a scam. It thought she'd ignored an effective warning. It also thought she could not have had a reasonable basis for believing this was the bank calling, given the warning message had been displayed.

It said it couldn't now locate the call recording from when Ms R had first called about the 'phishing' attack. But it thought that maybe the staff member she'd spoken to initially wasn't trained on fraud or scam risks. However, its call notes showed that the staff member had suggested contacting Action Fraud before trying to transfer Ms R to the fraud team – and wasn't wrong to have done so. It said Ms R should have held on for longer than she did (its notes agree with her recollections that she waited on hold for over an hour).

In light of this disagreement, I have been asked to reach a final 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 done so, I have reached the same outcome as the investigator and for broadly the same reasons. I've carefully considered Halifax's representations about the warning it gave Ms R and whether she had a reasonable basis for believing the transaction to be genuine. But the bank's representations do not persuade me to reach a different view. I will explain why.

Halifax seeks to rely on two possible exceptions to reimbursement under the CRM Code:

- the customer ignoring an effective warning by not taking the appropriate steps in response; and/or,
- the customer having made the payment without a reasonable basis for believing they

were paying the person they expected to pay.

Firstly, in the circumstances of this case, I'm satisfied that the requirements of the effective warning exception have not been established.

The CRM Code defines the requirements for a scam warning to be considered an Effective Warning. Part of the requirement to be sufficiently 'impactful' includes taking steps to ensure a customer is made aware of the consequences of proceeding with an irrevocable payment (such as this Faster Payment was). But neither Halifax's warning, nor the earlier message regarding Confirmation of Payee stated that the payment would be irrevocable or mentioned the consequences of proceeding.

While I appreciate the bank may believe this meaning was implicit, I'm not persuaded the warning message met the CRM Code's minimum requirements to be an Effective Warning.

Further, the nature of this type of scam means that in general an on-screen warning would need to have enough impact to stop someone from continuing to follow urgent instructions they believe originate with their bank. Otherwise a warning is unlikely to have a reasonable prospect of "positively affect[ing] Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced" – as required by the CRM Code.

And while I consider that in some circumstances the warning shown here *could* have an impact, I don't think it was sufficiently impactful to be *generally* effective against this type of safe-account scam.

Specifically, the initial text in the warning (and shown in a larger font size in a red colour) said 'how well do you know this person?'. Typically, this type of scam operates at pace and under pressure. The victim believes they are speaking to someone trusted, someone based in the fraud team of their bank. A scammer will typically suggest the need for urgency. The potential impact of an in-app warning is thus reduced, and there is a greater chance that the victim won't read the message fully. Here the heading doesn't immediately create a link (in the moment) to the situation the victim is in. This is especially so given the pressure they are typically under.

With the above in mind, I don't consider the warning Halifax gave here fully met the requirements for an Effective Warning under the CRM Code. It follows that Halifax cannot fairly apply the Effective Warning exception to Ms R's case – it hasn't demonstrated that such a warning was provided to Ms R.

I've gone on to consider whether Halifax has been able to establish that Ms R made the payment without holding a reasonable basis for believing what she did at the time.

The CRM Code specifies that all the circumstances at the time (to include the sophistication of the scam) need to be taken into account. I also consider that any warning or other messages provided are relevant circumstances - even where those warnings weren't Effective Warnings (as I have found here).

Firstly, I consider that the scam here was relatively sophisticated and persuasive. It involved an initial phishing attack, likely used as a way to gather personal information that was later used in the main scam call. That call used phone number 'spoofing' to mimic the bank's real phone number. Based on what I've seen, I'm persuaded that in all the circumstances here, Ms R had a reasonable basis for believing she was speaking with her bank and following its instructions to transfer money to a safe account it had created in her name to protect her funds.

What's more, Ms R has described how when she received the scam call on the evening in question, she was distracted and somewhat caught off guard. This was a Saturday evening a week before Christmas and she was getting ready to go out. But because she was expecting she might hear back from her bank she took the call. I consider these circumstances are relevant here.

Halifax argues that this may well have been the case, but that when it showed Ms R the warning message this would have broken the scammer's spell. I agree with Halifax that parts of the text of the warning message it showed Ms R were exactly relevant to the scam that occurred here.

But in the circumstances here, Ms R was already under the spell of the scammer by the time that message was displayed. She explains that she doesn't recall seeing the warning message at the time. I don't find that unreasonable given what she has said was happening at the time. By the time it was displayed she was attempting to follow the instructions of the caller to move her money supposedly to safety without delay. Ms R says she was feeling rushed and pressured.

The transaction timings provided to me by Halifax suggest the payment was completed quickly and so the warning could only have been displayed for, at most, a brief period of time.

Unfortunately, it seems that here the urgent promptings of the caller (whom Ms R believed was from Halifax's fraud team) were more impactful in the moment than Halifax's fraud warning message. I consider this was likely the result of Ms R holding the strong belief by this point that she was dealing with her bank's fraud team.

All things taken into account, I don't find Ms R was at fault in those circumstances for proceeding past the warning without fully absorbing what it said.

And overall, I am not persuaded that Halifax has established that Ms R made the payment without a reasonable basis for believing she was following the legitimate instructions of her bank to secure her money.

Under the terms of the CRM Code, the victim of an APP scam such as this should reimbursed unless the bank is able to establish that one (or more) of the exceptions to reimbursement can be applied. I'm not persuaded that Halifax has been able to establish that any of the exceptions to reimbursement under the CRM Code can fairly be applied in Ms R's case. It follows that Halifax should have reimbursed Ms R under the terms of the CRM Code.

Furthermore, I am also satisfied that had Halifax adequately alerted Ms R to the potential scam risks when she'd initially called to report the phishing attack, this would likely have made a difference. I think it was reasonable to expect Halifax to have taken such steps at the time of that initial call - given its knowledge of common fraud risks. But it has not provided evidence to show that it did so, and neither does Ms R recall it making her aware of those risks.

The bank explains that had Ms R stayed on hold for longer, then it could have given her better advice. I appreciate Halifax has challenges in having sufficient specialist staff readily available and that some delays are inevitable. But I don't think it follows that Ms R is to blame for not having waited on hold for over an hour. More importantly, she'd already reported the phishing incident to her bank – an initial incident that undoubtably meant she would be a significantly higher risk of financial harm through fraud or scam in the following days.

When the extended hold time resulted in the call being ended before Ms R had spoken to the fraud team, I consider the onus was on the bank to contact Ms R by some means to ensure she didn't subsequently fall victim to financial loss. Even if logistically the bank couldn't have called Ms R back within a reasonable period of time, I don't think it's unreasonable to think it could have attempted to contact her through another communication channel. At the very least, the bank should have been more alert to any riskier transactions in the immediate follow up to the reported phishing attack – meaning it most likely would have intervened at the point of the first payment rather than the second payment.

In saying that I consider Halifax liable because it ought reasonably to have thus prevented this scam, I have considered whether Ms R should bear some responsibility by way of contributory negligence. However, it is clear that up to and including the time of authorising the payment, she was still totally in the dark and simply did not appreciate what she was doing or the consequences of her actions. She thought she was helping to stop financial crime, not facilitate it. I am satisfied there was no contributory negligence on this occasion, she was simply the unwitting and blameless victim of a clever fraudster. The bank was the professional in financial matters; Ms R was a layperson.

In the circumstances, Halifax should fairly and reasonably refund the money Ms R lost. The money was sent from Ms R's current account. It is not clear how Ms R would have used the money if Halifax had refunded it when it should have done. But if Halifax had prevented the scam (or refunded the money when it ought reasonably to have done) Ms R would not have been deprived of it for the time she has. So, Halifax should also pay interest on the loss at a rate of 8% simple per year. This interest should be calculated from the date of the payment until the date of settlement.

Although most of Ms R's distress or inconvenience resulted from the criminal acts of the fraudsters, I find that Halifax should fairly share some of the blame for the impact of what happened to her. I say this given my finding that Halifax should have taken additional steps following Ms R's call to report the initial phishing attack - and in failing to do so, contributed to the scam's success. In all of the circumstances of this complaint I think it is reasonable for Halifax to pay Ms R the sum of £350 in respect of the material distress and inconvenience she suffered as a result.

**Putting things right**

For the reasons set out above, I've decided that Ms R ought reasonably to have been fully refunded under the CRM and further, that Halifax could have prevented the loss from taking place. I therefore direct Bank of Scotland plc trading as Halifax to pay Ms R:

- the full amount of the money she lost as a result of the scam, being £3,250 less any sums the bank has already been able to return to Ms R. The bank should do so within 28 days of receiving notification of Ms R's acceptance of my final decision; plus,
- interest at the simple rate of 8% per year on that amount (less any tax properly deductible) calculated from the date Ms R made the relevant payment until the date of settlement; and,
- £350 compensation for distress or inconvenience – also to be paid within 28 days of receiving notification of her acceptance of my final decision, failing which interest will thereafter accrue at the same rate until payment.

## My final decision

I uphold Ms R's complaint about Bank of Scotland plc trading as Halifax, as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 30 September 2022.

Stephen Dickie
**Ombudsman**