DRN-6056183

The complaint

Mr S complains that Bank of Scotland plc trading as Halifax ('Halifax') did not reimburse the funds he says he lost to a scam.

What happened

In September 2024 Mr S saw a luxury car hire business advertised on a well-known social media platform. I'll refer to the business as "L". Mr S made enquiries about a specific vehicle he was interested in hiring. Having exchanged messages with L, he received details of the price and confirmation that the vehicle could be delivered on the day agreed.

Mr S was told that the cost to hire the car for two days was £160 plus a refundable security deposit, originally priced at £685. Mr S was told that in order to book the vehicle he would have to pay the deposit upfront by bank transfer and then pay the rest when the vehicle arrived. Mr S was then told the security deposit was actually only £650 – so the total cost, including insurance and delivery/pickup costs was £810.

Believing everything to be genuine, Mr S made a payment of £810 on 10 September 2024 from his Halifax account to the account details provided by L.

Delivery was arranged for 14 September 2024 but unfortunately the vehicle wasn't delivered to Mr S as agreed. He tried to contact L but they wouldn't respond to him. Mr S raised a scam claim after it became apparent that the vehicle wasn't going to be delivered as promised. Halifax opened a claim and got in touch with the bank that received Mr S's money, but the other bank later confirmed that nothing was able to be recovered from the account that received the funds.

Halifax reviewed the case under the provisions of the Contingent Reimbursement Model Code ('CRM Code'). It decided that Mr S could have done more to protect himself, and that Halifax had met the standards expected of it as per the CRM Code, so it wouldn't be reimbursing him.

After raising a complaint, Halifax provided its response and reiterated its original outcome. Unhappy with this, Mr S asked our service to look into things. Our investigator reviewed the case and broadly agreed with Halifax's reasoning and didn't think it owed Mr S a refund under the terms of the CRM code. Mr S disagreed with the outcome and explained why.

As the complaint has not been resolved informally, it has been passed to me for 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.

I have summarised this complaint in less detail than the parties involved. I want to stress that no discourtesy is intended by this. If there is a submission I have not addressed, it is not because I have ignored the point. It is simply because my findings focus on what I consider to be the central issues in this complaint.

Having considered all the available evidence, I agree with the conclusions reached by the Investigator. I'll explain why.

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

Mr S authorised the payments. So in line with the Payment Services Regulations 2017 Mr S is deemed liable for the transaction in the first instance. But he says he has been the victim of an authorised push payment (APP) scam.

Halifax has accepted that Mr S was the victim of an APP scam and assessed Mr S's claim under the provisions of the CRM Code. Under the CRM Code, the starting principle is that a firm should reimburse a customer who is the victim of an APP scam (except in limited circumstances).

So I've gone on to consider whether Halifax should have reimbursed Mr S under the CRM Code.

Is Mr S entitled to reimbursement under the CRM Code?

Under the CRM Code, a Sending Firm (in this case Halifax) may choose not to reimburse a customer if it can establish that*:

• …The customer made the payment without having a reasonable basis for believing that:

- the payee was the person the Customer was expecting to pay;
- the payment was for genuine goods or services; and/or
- the person or business with whom they transacted was legitimate.

• The customer ignored what the CRM Code refers to as an 'Effective Warning' by failing to take appropriate action in response to such an Effective Warning.

**Further exceptions outlined in the CRM Code do not apply to this case.*

When assessing whether it can establish these things, Halifax must consider whether they would have had a '*material effect on preventing the APP scam'*.

Reasonable basis for belief

I assure Mr S that I have carefully considered all of the points he's raised with our service – particularly his reasons why he believes he had a reasonable basis for belief.
But taking into account all of the circumstances of this case, I don't think Mr S had a reasonable basis for believing the payments were for genuine goods or services; and/or the person or business with whom he transacted was legitimate.

I consider there to have been enough warning signs that ought to have caused Mr S concern and led him to complete more extensive research before making the payment he did. I say this because;

- Mr S said that he thought he was dealing with a limited company, having looked up L on Companies House. But he was given the bank details for a personal account. Mr S has said that many small businesses, particularly one's trading through social media, operate using personal bank accounts. But L was supposedly a limited company registered with Companies House, which Mr S says he checked. It is less common for legitimate registered companies to use personal bank accounts for their business dealings. And legitimate businesses often offer other methods of payment such as card payments. And I can't see that Mr S was ever given, nor did he ask for, any evidence that clarified how the individual he was paying was linked to the company he thought he was dealing with or confirms that L was actually the company that he saw on Companies House.

- The price quoted by L to hire this particular vehicle was £80 per day. Mr S says he had seen other adverts on social media where the advertised price to rent a similar vehicle was around the same price. But I do think this price was too good to be true. Though it generally varies depending on age, location, mileage and car specifications, online research suggests the average cost to hire this particular model of vehicle is between £350 - £450, or more, per day. This is significantly more than the £80 per day Mr S saw advertised. The price also seemingly included the cost of insurance, delivery and pickup at no extra cost. I can't see that Mr S was provided with an explanation as to how such a good deal was possible.
- I'm also mindful that Mr S was provided with no documentation. Mr S has said he was expecting to receive this when the vehicle was delivered, and that this wasn't unusual compared to his previous experience hiring vehicles, particularly abroad. But I think it's reasonable to expect that when hiring a vehicle there would be, as a minimum, a rental agreement, or some discussion about the terms on which the rental is being made, and that Mr S would receive an invoice for the payment he was being asked to make. But Mr S wasn't provided with anything like this. The available evidence suggests that apart from being told insurance was included, and the security deposit was refundable, no other terms and conditions, or rules, of hiring the vehicle were discussed or shown to Mr S before he made the payment. I think Mr S ought reasonably have requested more information about what he was paying for, and on what terms, before he made the payment.
- I appreciate that it's now common for legitimate businesses to use social media to promote their business. But most, if not all, reputable vehicle hire companies also have a website and independent reviews online. L doesn't appear to have a website, nor are there any reviews of L online. And I think this should have been concerning. And while I wouldn't expect Mr S to have acted as a fraud investigator, I do think he ought reasonably have looked for further information about L before making his payment.
- Mr S was originally told that he had to pay the deposit up front and the remaining balance when the vehicle was delivered. However, when Mr S was provided with the payment details, including the amount, it was the full amount up front. While Mr S was expecting to pay the full amount in a few days from then anyway, Mr S didn't query this considering it was different to what he'd been told earlier.

I might understand, when taken in isolation, how any one of these things may not have prevented Mr S from proceeding. But when taken collectively I think there were sufficient unusual factors here that Mr S ought to have acted more cautiously than he did, but rather he appears to have taken things at face value. I'm satisfied, therefore, that on balance Mr S

didn't have a reasonable basis for believing he was making a payment for a legitimate service.

That's not to say what happened is Mr S's fault. He has been the victim of a cruel scam. But I'm persuaded there were enough signs that he ought to have reasonably questioned the legitimacy of what he was being told and acted more cautiously than he did.

So, I think Halifax can fairly rely on one of the exceptions to reimbursement – that Mr S made the payments without a reasonable basis for believing that the payments were for genuine goods or services and/or the person or business with whom he transacted with was legitimate.

Did Halifax meet its standards?

The CRM Code also sets out standards that firms are required to meet. Where these are not met, the firm may still be liable to reimburse a victim in part, even where it has been able to establish that an exception to full reimbursement may be fairly applied (as I am satisfied Halifax can establish here).

Those requirements include the provision of what the CRM Code defines as an 'Effective Warning' when a firm identifies an APP scam risk in relation to a payment. In short, the CRM Code said that where the firm identifies an APP scam risk it should take reasonable steps to provide their customer with 'Effective Warnings'. It goes on to say that as a minimum, an Effective Warning should be understandable, clear, impactful, timely and specific.

Halifax only needs to provide an Effective Warning when it identifies APP scam risks during a payment journey.

Based on what Halifax could reasonably have known at the time, I don't consider the payment Mr S made would have particularly stood out as being at risk of being connected to a fraud or scam.

I say this because, while it was to a new payee this isn't on its own indicative of a fraud risk. In the months before the disputed payment, it wasn't uncommon for Mr S to make payments of similar, and sometimes larger, amounts from his account with no issue. The value of the payment, while significant, wasn't so large or unusual that it would have stood out to Halifax. And being a one-off payment, it didn't follow any known scam patterns.

Mr S has made the point that Halifax should have been alerted that the payee details didn't match that of a business. But Halifax relied on the information Mr S gave it. The name on the account and the account details matched. It appears Halifax did alert Mr S that it was a personal account and not a business account. But the name on the account doesn't suggest the account should have been a business account. And I don't think anything else Halifax would've known at the time would have suggested the payment was going to a fraudster.

With the above in mind, I don't think the payment Mr S made looked unusual enough to Halifax to suggest he could be falling victim to an APP scam and therefore require an Effective Warning.

Should Halifax have done anything else to prevent the loss?

Outside of the CRM Code, good industry practice requires that regulated firms such as Halifax engage in the monitoring of customer accounts and to be on the lookout for

suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm.

As mentioned above, I don't think the payment Mr S is disputing would have looked suspicious or indicative that Mr S was at risk from fraud. With that in mind, I don't think Halifax should have intervened at the point of the payment.

Recovery of funds

Finally, I've considered whether Halifax did all it could to try and recover the money Mr S lost once he had reported the scam to it. From the evidence I've seen, I'm satisfied Halifax did what it could to try and recover the money from the bank that received it. Though it took a while for the other bank to reply, Halifax did reach out to the other bank during the call Mr S made to report the scam, or at least very shortly after. Unfortunately, the other bank confirmed it was unable to recover the money that had been paid. But I do think Halifax has done what it could reasonably have been expected of it to try to recover the money.

Summary

I don't find Halifax is to blame for Mr S's losses. I don't find it is liable to refund Mr S under the terms of the CRM Code either.

In saying this, I want to stress that I am very sorry to hear about what happened to Mr S and I am sorry he has lost out here. He was the victim of a cynical scam designed to defraud him of his money and provide nothing in return. But I can only look at what Halifax was and is required to do – I have no power to consider the actions of the criminal scammers who were ultimately responsible for Mr S's loss. And I don't find Halifax is required to refund him under the CRM Code, nor that the bank was at fault in making the payments Mr S instructed it to make or for any other reason.

Having considered everything very carefully, in my judgment, this is a fair and reasonable outcome in the circumstances of this complaint.

My final decision

For the reasons set out above I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 12 March 2026.

Mike Southgate
Ombudsman