DRN-4607796

The complaint

Mr W complains about Bank of Scotland plc (trading as Halifax).

He says that Halifax didn't do enough to protect him when he became the victim of a scam and would like to refund him the money he has lost as a result.

What happened

Mr W was looking to purchase a new car and found an advert on social media that he was interested in, for a 2016 model priced at £4,500.

Mr W says that as he was not confident in his ability to assess the risks associated with the purchase, he asked his son to look at the advert to see if he thought it was genuine. Mr W's son looked at the advert and said that he thought it seemed genuine, and so Mr W made contact with the seller.

The seller told Mr W that they were out of the country at present, and that the car was in storage. They provided details of the logistics company looking after the car, and that they would then deliver the car after payment. Mr W explained that he was willing to collect the car, but the seller explained that this was not possible, and that the car would be delivered within 10 days of payment.

After checking this with his son to make sure this was legitimate, Mr W decided to proceed, and made the payment on 5 March 2020, but soon after realised he had been the victim of a scam when the seller cut contact and didn't respond to his emails.

He then made a complaint to Halifax about what had happened and said it should have warned him about making a payment of this nature.

Halifax didn't uphold his complaint as it said that Mr W didn't have a reasonable basis for belief that the advert was genuine. He then brought his complaint to this Service.

Our Investigator looked into things and thought that the complaint should be upheld in part. They said that Halifax had failed to give Mr W an effective warning, and while Mr W says he was a vulnerable individual, he had effectively asked someone else to make the checks for him and didn't have a reasonable basis for belief – and so Halifax should refund Mr W 50% of his payment.

Both Halifax and Mr W's representative responded to the Investigators view. Halifax said that it wasn't required to give a warning to Mr W, and so it didn't think that it had to refund any of the payment he made. While Mr W's representatives said that Mr W was vulnerable, and so should receive a full refund.

As no agreement could be reached, the complaint has been passed to me to make 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.

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 be good industry practice at the time.

I've considered whether Halifax should reimburse some or all of the money Mr W lost in line with the provisions of the Lending Standards Board Contingent Reimbursement Model CRM Code (CRM Code) it has agreed to adhere to, and whether it ought to have done more to protect Mr W from the possibility of financial harm from fraud.

The CRM Code requires firms to assess whether a customer was vulnerable to the APP scam they fell victim to at the time it occurred. The relevant sections state:

"A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.

This should be assessed on a case-by-case basis.

In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the Firm had previously identified the Customer as vulnerable. […]

Factors to consider include:
(a) All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer
(b) A Customer's personal circumstances which lead to vulnerability are varied, may be temporary or permanent, and may vary in severity over time
(c) APP scams may include long-running APP scams or in the moment APP scams."

In this case, Mr W asked his son to complete the necessary checks to establish the validity of the advert. So, although Mr W's representative has said that Mr W himself was vulnerable, his son was not – and it was him that completed the checks and provided reassurance on his father's behalf. Therefore I don't think that Mr W's apparent vulnerabilities impacted on his choice to make the payment.

The CRM Code also requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances which I have set out below:

- 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.

- The customer made payments 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.

There are other exceptions that do not apply to this case.

It is for Halifax to establish that it can rely on one of the exceptions to reimbursement set out under the CRM code.

In this case, Halifax has said that under the CRM code it is only required to provide an effective warning if it suspects that the payment being made is part of an APP scam – however it also earlier said that although it doesn’t hold online banking records going back to March 2020, it would have provided a warning for payments to new payees between certain amounts, which would apply to Mr W’s transaction and provided an example of this.

In any event, given the amount of the payment, and considering Mr W’s account history, I think that Halifax should have provided Mr W with an effective warning about what he was doing.

The warning says the following.

> *‘Just a minute… Be sure that you know who you’re sending money to. Please check the account details with a trusted source. Fraudsters invent persuasive reasons to get you to make a payment. See all the latest scams fraudsters use on our fraud hub page. Failure to take precautions before you make your payment could mean we are not able to get your money back in the event of fraud. What do you want to do?’ (Two options to cancel or continue).*

I don’t think that this warning was effective – it wasn’t specific enough to the type of scam Mr W was falling victim to and failed to bring to life the main features of common APP scams. I also don’t find that the warning was clear, or set out in a way that Mr W would have understood the risks of making the payment,

So, I don’t think that Halifax can rely on the exception that Mr W ignored an effective warning when making the payment.

Did Mr W have a reasonable basis for belief that the payment he made was legitimate?

As I understand, Mr W was concerned that he wasn’t able to do the necessary checks himself to make sure that the purchase he was making was legitimate – and so asked his son to do these checks for him. I know that Mr W’s representative says that he was vulnerable – but in this instance, Mr W was aware that he may have difficulties in completing the checks, and effectively appointed his adult son to take on this responsibility for him. Mr W’s son had no vested interest in making the payment, and there is no indication that he himself was a vulnerable individual.

I also think that there were several red flags that Mr W’s son should have noticed when he was asked to look into the purchase for his father.

- The price of the car was too good to be true considering its age and model

- When asked if the car could be collected, the scammer explained that the car was in storage, and would be delivered after payment. While it isn't unusual for a deposit to be paid prior to collecting a car, it is unusual for full payment to be required before an individual receives the car or goes to view it in person
- I haven't been provided with any evidence that shows what checks Mr W or his son did on the car or the supposed seller prior to making the payment

So, I think that there was enough going on to have caused concerns, and more should have been done to establish the legitimacy of the purchase, and I don't think that there was a reasonable basis for believing everything was ok.

Recovery of the funds

Once the scam was reported to Halifax, I can see that it tried to recover the funds from the receiving bank – but unfortunately the money had already been moved on by this point, so I think it did all that it could to try and get Mr W's money back.

Overall, I don't think that either Halifax, or Mr W did enough to prevent what happened, and so responsibility should be shared equally between both parties.

Putting things right

Bank of Scotland plc (trading as Halifax) should refund Mr W 50% of the payment he made. I calculate this to be £2250.

On top of this, it should also pay Mr W 8% simple interest from the date the payment was made until settlement, minus any lawfully deductible tax.

My final decision

I uphold this complaint in part, Bank of Scotland plc (trading as Halifax) should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 12 December 2024.

Claire Pugh
Ombudsman