DRN-5837103

The complaint

Miss C complains that Bank of Scotland plc trading as Halifax ('Halifax') declined to reimburse her when she fell victim to an investment scam.

What happened

The circumstances of this complaint are well known to both parties, so I will not go into every detail of what happened here. But, in summary, Miss C came across and investment opportunity via social media which I will call 'G'. She spoke to G over social media and was told that she could turn £200 into £2,500 in a short period, with 100% money back guarantee. Persuaded to invest, she sent a series of payments from her Halifax account to different personal accounts, totalling approximately £4,000. Some of these payments were intended to go towards the investment itself, and some were intended to go towards releasing the profits of her investment, by way of fees she was told she had to pay.

Despite sending the fees to release her funds, she kept receiving further requests for fees, and she did not receive any money from G. Miss C realised she had fallen victim to a scam, and so contacted Halifax to ask them to reimburse her losses. Halifax declined to reimburse her. It said that it had considered her claim under the Lending Standard Board's Contingent Reimbursement Model ('CRM') Code, but that she had not met the standards required of her with regard to the due diligence she did into this investment opportunity before sending the money.

Unhappy with their response, Miss C escalated her concerns to our service. One of our investigators looked into what had happened and did not recommend that Miss C's complaint should be upheld. In summary, they said that it was fair and reasonable for Halifax to apply the exception to reimbursement under the CRM Code, on the basis that Miss C did not have a reasonable basis for belief that G were offering a legitimate investment opportunity.

Miss C did not agree. Through her representatives, she said that at the time of the scam, Miss C was vulnerable to authorised push payment ('APP') scams, which under the CRM Code would mean that the exception to reimbursement would not apply. They also said that contrary to our investigator's view, they thought that the payment pattern was sufficiently unusual and out of character that Halifax ought to have intervened and provided Miss C with a warning, especially given her vulnerable status.

As no agreement could be reached, the case has been passed to me to decide.

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 broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Service Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may

sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

When thinking about what is fair and reasonable in this case, I have considered whether Halifax should reimburse some or all of the money Miss C lost in line with the provisions of the CRM Code it agreed to adhere to. I've also considered whether it ought to have done more to protect Miss C from the possibility of financial harm from fraud.

The CRM Code

Halifax was a signatory of the Lending Standards Board Contingent Reimbursement Model ('CRM') Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It sets out standards that banks, such as Halifax, are expected to meet in terms of protecting their customers from financial harm. But it also sets out expectations that a customer should meet, too. As a starting point, a customer should receive a full refund if they fall victim to an authorised push payment scam such as this one.

It is not in dispute that Miss C was the victim of an APP scam. But Miss C would not be entitled to a full refund if Halifax can fairly and reasonably demonstrate that Miss C failed to meet the requisite level of care under one of more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- The customer ignored an effective warning in relation to the payment being made.
- The customer made the payment without 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 further exceptions within the CRM Code, but they do not apply in this case.*

Vulnerability under the CRM Code

Under the CRM Code, if a customer is considered vulnerable to APP scams the exceptions to reimbursement outlined above would not apply. The Code says that:

> *"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 is a determination which is made on a case by case basis, and recognises the dynamic nature of vulnerability which can include personal circumstances, the timing and nature of the APP scam and the customer's capacity to protect themselves.

Was Miss C vulnerable to the APP scam she fell victim to, at the time that she fell victim to it, such that she was unable to protect herself from it?

Miss C, through her solicitors, made representations that Miss C was vulnerable at the time of the scam, such that she was unable to protect herself from it. I would like to say that I was sorry to read of everything that Miss C was going through at the time she became the victim of a cruel and callous fraudster. I am not meaning to diminish this at all, and appreciate what a difficult time it must have been for her. However, I am afraid I do not think the circumstances that have been explained to our service mean that she was so vulnerable to APP scams that it would not be reasonable to expect her to able to protect herself from it. I'll explain why.

Miss C's representatives explained that at the time of the scam she was the primary carer for an elderly relative who was suffering from dementia, and had been for around two years. They said she was also suffering from a variety of significant health challenges of her own, including mental ill health and chronic pain, requiring daily medication, including painkillers

which she had been taking for around a year. They said that this could cause drowsiness and difficulty concentrating. She had also lost one of her parents around 8 months before the scam. Her solicitors said that this meant that her ability to recognise the scam and carry out adequate checks could have been impaired.

Miss C's representatives did say that she had low finances at the time of the scam, but also said that she had around £30,000 which she received as inheritance from her parent. They said that Miss C was receiving emotional support from friends and family. She also said that she struggled to manage her finances and relied on friends and family for financial advice and support.

I have read the messages shared between Miss C and the scammer as the scam unfolded. She did at various points in the chat question the scammer, including why she was asked to send the money to cryptocurrency, why she was asked to send the money in USD, why she was sending money to a different person, why she had not received her funds as promised, even suggesting that the investment did not sound legitimate and that she was not going to send any more money – though she did send more. It appears that she was able to recognise that this could be illegitimate and understood to ask questions about the scam, and knew that she could stop sending money. She was not in a position of financial desperation. She was able to hold down a job, and go abroad on holiday, and her communication seemed clear and engaged with the scammer. The circumstances she found herself in, whilst difficult, were not unfamiliar as they had been ongoing for some time prior to the scam. She said she knew she could ask advice of friends and family on financial matters, but chose not to, despite the fact the scam took place over numerous days. Considering all of this, I am afraid I do not think there is enough evidence to suggest that she was unable to protect herself from the scam when it took place, and to the extent it did. And so it follows that I do not think that she was so vulnerable that exceptions to reimbursement under the CRM Code ought not be considered in this case.

Did Miss C act with a reasonable basis for belief that this was a legitimate investment?

I have carefully considered Halifax's assertion that Miss C acted without a reasonable basis for belief that this was a legitimate investment, and I think that they have demonstrated that this is the case. I say this because the investment was found via a message on social media. Miss C did not do independent checks on the company, other than looking at the page itself. The returns ought to have appeared to be too good to be true. The scammer asked for additional funds to release her funds, which had not been mentioned from the outset. She recognises that there may be some red flags in that she asks questions about the legitimacy of the payment instructions she is given, but continues anyway despite vague answers from the scammer. She was not provided with any official paperwork. She did not seek advice from any external parties. She carried on sending money even after she had said she did not trust them and was not going to do so. The scammer kept promising she would have the funds in a short time, but then asked for more money without this promise being fulfilled. So, considering all of this, I do think Halifax have demonstrated that she acted without a reasonable basis for belief that this was a legitimate investment, and so they acted fairly and reasonably in applying this exception to reimbursement under the provisions of the CRM Code.

Should Halifax have done more to protect Miss C from fraud or financial harm?

The Code sets out standards that banks are expected to meet. Halifax needed to be on the lookout for factors that might indicate an enhanced risk that Miss C's payment instructions were being made as part of a scam. Where they identify such a risk, Halifax needed to take reasonable steps to provide the customer with an effective warning.

I've also taken into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time. And based on

the other relevant rules relating to authorised push payment scams, I think Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual and out of character transactions or other signs that might indicate that its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So, I consider that as a matter of good practice, Halifax should have been on the lookout for unusual and out of character transactions and where necessary, taken proportionate interventions.

I have considered the payments that Miss C made and I do not think that it would be fair and reasonable to say that Halifax ought to have intervened. The payments were made over three days. The first day she sent two payments to someone I will call 'payee A', which totalled £1,050. The second day she sent payee A another £500, and sent someone I will call 'payee B' just under £2,000 over three payments. She then sent payee B another £200 on the third day.

Whilst I appreciate that these are not insignificant sums of money, I do not think that they were so unusual or out of character that Halifax had to intervene, or provide an effective warning. Miss C had made faster payments in the range of £500 to £2,000 in the previous year from her Halifax account. The amounts individually or collectively were not so large that I think it was clear to Halifax that Miss C was at risk of fraud or financial harm here. I do appreciate she sent multiple transactions in the same day, particularly on the second day of payments when she sent four payments. The payment to payee A was not clearly linked to the payments to payee B, and therefore the payee B payments were not clearly linked to the funds she sent the day before. Whilst scams take many forms, there was not an escalation in payment values as one might expect to see in a scam – the final payment on this day was less than earlier ones that day. Only the first payments to payee A and B were to new payees. And I do not think she sent so much within the day that it was clear here that she was falling victim to a scam. And so it follows that I think Halifax acted reasonably by following Miss C's payment instructions without intervention.

To conclude, I would like to say again how sorry I was to read of what Miss C was put through here. She was clearly going through a difficult time in her own life, before she became the victim of this cruel and callous scammer. But, I do not think it would be fair or reasonable to ask Halifax to reimburse her losses as I do not think that they were at fault here.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 20 February 2026.

Katherine Jones

Ombudsman