DRN-4473251

The complaint

Miss R is unhappy that Bank of Scotland plc trading as Halifax ('Halifax') won't refund the money she lost after falling victim to a scam.

What happened

In November 2020, a work colleague introduced Miss R to a cryptocurrency investment opportunity. Initially Miss R made payments to her work colleague – who I'll refer to as P.

The first three payments made to P were for less than £2,500 in total and were made in November and December 2020.

Between 1 January and 26 January 2023, Miss R made multiple payments to a cryptocurrency account in her name. Miss R says she did some trading but didn't make any money, but she built up the balance in her cryptocurrency account and then transferred it to the investment platform recommended by P.

Miss R made two further payments from her Halifax account on 19 April 2021, for £9,700 and £200. Both of these payments went to Miss R's existing cryptocurrency account, with the funds then forwarded to the investment platform.

Miss R was made aware it was a scam by another work colleague, so she raised a fraud claim with Halifax. The fraud claim Miss R raised only included the payments she made to her cryptocurrency wallet – not the payments she made to P.

Halifax considered Miss R's fraud claim but declined to refund her. Halifax are a signatory to the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code) but said the CRM Code doesn't apply to these payments as they went to an account held in Miss R's name. They highlighted that Miss R didn't complete any checks on the company she was investing with and that they'd given her advice on how to protect herself from scams after falling victim to a similar scam a few months before she made the payments in April.

Miss R wasn't happy with Halifax's response, so she brought a complaint to our service.

While Miss R's case was with our service, it became clear that her claim included the payments made to P, so we asked Halifax to investigate these transactions and provide a response.

Halifax considered those three payments under the CRM Code but declined to refund Miss R saying an exception to reimbursement applied, as Miss R didn't have a reasonable basis for believing the investment was genuine.

Miss R wasn't happy with their response, so an investigator looked into Miss R's complaint about all of the transactions she raised.

The investigator agreed with Halifax that the payments Miss R made to her cryptocurrency account aren't covered by the CRM Code and said they wouldn't have expected Halifax to

intervene before processing the payments. With regards to the three payments to P, they agreed that Halifax could rely on an exception to reimbursement, saying the returns Miss R was promised were too good to be true and she should've completed checks on the investment company.

Miss R disagreed with the investigator's opinion, saying other victims of the same scam had been refunded by their banks.

As the case couldn't be resolved, it was passed to me to review.

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 carefully considered all of the evidence, I've reached the same outcome as the investigator, and I'll explain why.

The payments Miss R made to P

The three payments that Miss R made to P, are covered by the CRM Code.

The CRM Code requires firms to reimburse customers who have been the victims of APP scams like this, in all but a limited number of circumstances.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that an exception applies. In this case Halifax say Miss R 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.

Having considered the information carefully, I agree that Halifax can rely on an exception to reimbursement for the following reasons:

- Miss R says the investment involved her buying a package, which would provide her with a return. She was told that the highest package would return £10,000 per week. The package she was on, would return £7,000 per week. This return was too good to be true, especially considering how much she had invested, and she should've been concerned.
- P introduced Miss R to the investment on the basis that P would get paid commission for each new investor. I'm not satisfied that a genuine investment company would do this.
- While Miss R was referred to this investment by P, I'm not satisfied that Miss R clearly understood what she was investing in or knew anything about the investment platform that she would be using. Basic online searches would've shown Miss R numerous links to negatives reviews about this investment platform and suggestions that it was a scam.

Taking all of these points into consideration as a whole, I think Miss R should've had concerns about the information she'd been given and whether this was a legitimate investment opportunity. As a result, I would've expected her to complete some checks on the investment platform, which would've highlighted that this was most likely a scam.

I have also considered whether Halifax have met their obligations under the CRM Code.

Based on the low value of the payments, I'm not satisfied Halifax should've identified a scam risk and therefore weren't required to provide Miss R with an effective warning. So, I'm satisfied that Halifax have met the standards set for them under the CRM Code.

This means I can't fairly ask Halifax to refund Miss R for the first three payments.

The remaining payments that Miss R made as part of the scam

The CRM Code doesn't apply to payments made between accounts held by the customer.

So, where Miss R transferred the funds from her Halifax account to a cryptocurrency account in her name, the payments aren't covered by the CRM Code.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. When Halifax made the payments, it was complying with Miss R's instructions. The payment was made to the intended bank account, although I appreciate that Miss R made the payments without realising she was the victim of a scam at the time.

However, I would expect Halifax to be on the lookout for, and to protect its customers from, potentially falling victim to fraud or scams. This includes monitoring accounts and identifying suspicious activity that appears out of character.

In Miss R's case, I'm not satisfied that Halifax should've been concerned about Miss R's payments as I'm not persuaded that they were particularly unusual or out of character.

The largest payment was for £9,700 but it was made to an existing payee that Miss R used regularly. This included sending payments of between £1,000 and £2,000, and even sending multiple payments on the same day totalling up to £6,000. Based on this, I don't think the payment was so unusual or out of character that I think Halifax should've been concerned or intervened before following Miss R's payment instructions. On that basis, I can't fairly ask them to refund Miss R.

Miss R has raised a concern that other victims of the same scam have been refunded. However, each complaint is considered on its own individual merits and circumstances. And, while I appreciate that Miss R is going to be very upset as she has lost a significant amount of money, I can't fairly ask Halifax to refund her.

My final decision

My final decision is that I don't uphold this case against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss R to accept or reject my decision before 30 January 2024.

Lisa Lowe
Ombudsman