DRN-4725083

The complaint

Miss A complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund money she lost in an advance fee scam.

What happened

What Miss A says:

Miss A was a student and was looking to earn extra money to pay rent and living costs. She was approached on or around 8 April 2023 by someone representing a 'recruitment firm'. She was told about a job she could do from home, and it was flexible. She was told the company she would work for was a digital marketing agency which worked to boost the sales of online items by making them seem more popular. Miss A went through the training which appeared professional. She was asked to create an account for herself on the firm's website.

Miss A was told she needed to complete 40 reviews to be able to access her income. She spoke to the firm's representatives over WhatsApp. To complete the tasks, Miss A used the funds the scammer had firstly put into her online account. Then, to complete further tasks, she was required to put more funds herself into the account. This included special tasks which promised more money.

Miss A had to set up a crypto wallet, from where the funds were sent to the scammers' platform.

Miss A did receive some funds from the scammers – which made the scheme more believable.

Miss A made several payments as well as receiving some funds:

Date	Payment	Amount
11 April 2023	Received from crypto platform	(£93.19)
11 April 2023	Received from crypto platform	(£145.85)
11 April 2023	Debit card payment to crypto platform	£15
11 April 2023	Debit card payment to crypto platform	£52
11 April 2023	Debit card payment to crypto platform	£130
13 April 2023	Debit card payment to crypto platform	£20
13 April 2023	Debit card payment to crypto platform	£187

17 April 2023	Received from crypto platform	(£776.88)
18 April 2023	Faster payment to individual	£269
18 April 2023	Faster payment to individual	£750
18 April 2023	Faster payment to individual	£2,330
18 April 2023	Debit card payment to crypto platform	£20
18 April 2023	Debit card payment to crypto platform	£302.80
19 April 2023	Debit card payment to crypto platform	£386.82
Total losses		**£3,446.70**

The scam ended when Miss A used up her funds in the online account and couldn't put anymore in - as she ran out of money. Miss A asked that she withdraw her funds but this proved impossible.

As a result of what happened, she has become anxious and depressed, suffers from sleepless nights and loss of appetite. She's had to leave university and return home – she has lost her life savings.

Miss A complained to Halifax. She says Halifax had several opportunities to intervene and warn her about the scam. She made high value payments in quick succession which should've triggered Halifax's fraud detection systems – starting on 11 April 2023, with payments to a new payee.

And then again on 18 April 2023 when she made five payments in quick succession. On that day, when the bank did contact her, they let the payment go through once she explained what she was doing. But this was by then a huge red flag. She says the payments were out of character with how she used her Halifax account.

Miss A says Halifax should refund the money plus interest at 8% per annum simple, and compensation of £300.

What Halifax said:

- The Contingent Reimbursement Model (CRM) Code didn't apply as the payments were either made by debit card (which wasn't covered by the Code) or faster payments to an account in Miss A's name (which also weren't covered by the Code.

- Miss A shouldn't have trusted the scheme.

- She didn't research the job opportunity and relied on the scammers' word.

- She should've questioned the scheme – to pay money to get paid for a job didn't seem credible.

- When Halifax blocked the payment for £2,330 on 18 April 2023, they advised Miss A it was very likely a scam and told her about the risks. But she went ahead with that payment. And she then made more payments after that.

- Halifax didn't attempt to recover the funds as the payments were to an account in Miss A's name at the crypto exchange. And the debit card payments couldn't be the subject of a chargeback claim.

Our investigation so far:

Miss A brought her complaint to us. Our investigator didn't uphold it. He said:

- The payments up to the one for £2,330 weren't unusual or suspicious.

- The payment for £2,330 was blocked by Halifax and the bank warned Miss A it was likely a scam. This was repeated a number of times, but Miss A confirmed she wanted to go ahead. Even if the payment had been refused, he was persuaded that Miss A would've made the payment through another method in any case.

Miss A didn't agree. She said Halifax should have refused to put the payment of £2,330 through. She asked that an ombudsman look at her complaint, and so it has come 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.

I'm sorry to hear that Miss A has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although Miss A didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking 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, I consider 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 transactions or other signs that might indicate that its customers were at risk of fraud (among 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 make 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.

I need to decide whether Halifax acted fairly and reasonably in its dealings with Miss A when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't

apply in this case. That is because it applies to faster payments made to another UK beneficiary – and in this case, the payments were made to Miss A's own account – her crypto wallet. And some payments were made by debit card – which also isn't covered by the CRM Code.

The first consideration here is: if the payments were of a sufficient size and were out of character with how Miss A normally used her account – then I need to consider whether Halifax should have intervened and spoken to Miss A. I looked at Miss A's account, and it's fair to say that the payments were unusual – she used her account to make day to day expenditures of low value. Most payments were well below £50. There were monthly rent payments of about £512.

But - there's a balance to be made; Halifax has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. And here – the payments up to the one for £2,330 were for relatively low amounts. Therefore, in this case, I think Halifax acted reasonably in processing those payments – I don't think that I could reasonably say that Halifax should have stopped the payments for further checks.

Then, Halifax did intervene in the payment on 18 April 2023 – for £2,330. I listened to the call, and I'm satisfied that the bank gave sufficient and clear warnings to Miss A – that this was very likely part of a scam. Miss A told him she was paying money as part of a task/job; that she was dealing via WhatsApp; had done no research into the company. The call handler – who was clearly experienced in such matters – said:

"I've come across many other (schemes) like this…customers are losing a lot of money"

"You are putting in £2,330 to get £1,000 out? That's a loss of £1,330… "

(after seeing the other payments she'd sent) *"You've put in more money than you're taking out"…*

" A legitimate company wouldn't operate in this way…"

"I believe this is a scam…"

"you are transferring money to various different individuals, which doesn't appear credible…"

"If this turns out to be a scam, we can't help you, there is slim to no chance of getting it back…"

"You are not sure (about this scheme) so I am putting this payment on hold…"

I heard the call handler say several times this was very likely a scam.

The call handler suggested she reconsider what she was doing and speak to friends and family first. But Miss A said she wanted to go ahead, and the payment was released.

So here, I'm satisfied Halifax did all they could to:

- Warn the payments were likely part of a scam;
- Warn they wouldn't be able to get the money back;
- Advised Miss A to take advice.

And Halifax acted reasonably in then releasing the payment. And after that, Miss A made a further three payments, despite the warnings Halifax had given. And based on the low value of those three payments (and the answers given by Miss A on the call), I wouldn't have expected Halifax to intervene in those.

Therefore, I don't hold Halifax liable to refund the payments made by Miss A.

Recovery
We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Halifax took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. Halifax said they didn't try because:

- It was likely no funds would've remained – as she'd moved them into the crypto trading platform; and from there the scammers would've removed them quickly.
- Any chargeback claim for the debit card payments would've failed - as those were authorised payments by Miss A, and a chargeback had no reasonable prospects of success.

Miss A has lost a lot of money. She's explained why the money was important to her, and the impact her losses have had. I was sorry to learn of her circumstances. She will therefore be disappointed by my decision, but I'm not going to ask Halifax to do anything here.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss A to accept or reject my decision before 7 May 2024.

Martin Lord
Ombudsman