DRN-3653599

Financial Ombudsman Service

The complaint

Miss M complains that Bank of Scotland plc, trading as Halifax, won't reimburse the funds she lost when she fell victim to a cryptocurrency investment scam.

What happened

Miss M was looking for an investment opportunity and, in February 2020, was contacted by a representative of EGM Finance. Miss M says that she checked the firm's website which looked legitimate and decided to invest. EGM Finance later turned out to be fraudulent.

To facilitate her trading account with EGM Finance, Miss M first sent money from her Halifax account to a cryptocurrency exchange platform called Coinipop. It converted her funds into cryptocurrency and then sent it on to the intended destination as instructed by Miss M's *account manager* at EGM Finance.

Miss M was able to make one withdrawal of £300 after her initial deposit. The following transactions are relevant to this case:

Date	**Type**	**Merchant**	**Amount**
22 February 2020	Debit card	Coinipop.com	£1,000
29 February 2020	Credit	Coinipop.com	£300 **(credit)**
6 March 2020	Debit card	Coinipop.com	£5,000
17 March 2020	Debit card	Coinipop.com	£4,300
		Total loss	**£10,000**

Miss M eventually realised she had been scammed when repeated withdrawal requests were declined and her account manager's email address suddenly became invalid. She reported the matter to Halifax in September 2020. It declined to refund the transactions or raise a chargeback but paid £100 compensation in recognition of the delays in responding to the complaint. Unhappy with this, Miss M referred her complaint to our service.

Our investigator concluded that Halifax didn't act unfairly in raising a chargeback. He also considered whether Halifax ought to have done more to prevent the payments from being sent in the first instance. It was the investigator's view that Halifax ought to have intervened when Miss M authorised the payment of £5,000 on 6 March 2020 as it appeared unusual. But he thought that an intervention was unlikely to have stopped her from going ahead with the payment. So, he didn't think Halifax could have limited her losses.

I issued my provisional decision a few weeks ago. I explained that I intended reaching a different outcome to the investigator.

I gave both parties an opportunity to provide any more comments and evidence for me to consider. Both Halifax and Miss M accepted my provisional findings. What follows is my provisional decision made final.

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'd like to start by reassuring both parties that although I've only summarised the background and main arguments, so not everything that happened is mentioned, I've read and considered everything that's been provided in its entirety.

Recovery

The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The card scheme operator – Visa in this case – ultimately arbitrates on a dispute if it can't be resolved between the merchant and the cardholder. Such arbitration is subject to the rules of the scheme, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be considered valid, and potentially succeed.

Miss M was dealing with a broker called EGM Finance. Given the information I've found about it during my research, I'm satisfied Miss M fell victim to a scam rather than simply losing money as a result of a high-risk investment.

But Miss M didn't make the debit card payments to EGM Finance; she paid Coinipop. This is important because Halifax was only able to chargeback against the merchant she paid, not another party.

It's my understanding that Coinipop is a legitimate cryptocurrency exchange firm. The service provided by the exchange would be to convert Miss M's payments into cryptocurrency. Therefore, the merchant she made the payments to did provide the service that was requested; that being the purchase of the cryptocurrency. The fact that the cryptocurrency was later transferred elsewhere – to the scammer – doesn't give rise to a valid chargeback claim against Coinipop.

Duty of care

While I don't think that Hallifax could have done more with regards to the recovery of Miss M's funds once it was made aware of the situation, I've also considered whether it ought to have intervened *before* allowing any of the payments to be made.

The disputed payments were authorised by Miss M using her legitimate security credentials. So, under the relevant regulations, she's considered liable unless there's evidence that Halifax could and should reasonably have done more to protect her against the risk of fraud and scams, and that this would have made a difference to her decision-making.

Halifax ought to have been monitoring accounts to counter various risks; having systems in place to identify unusual transactions or other indicators that its customer was at risk of fraud; and, in some situations, making additional checks before processing payments or declining them altogether to protect its customer from possible financial harm from fraud.

I've considered that the payments were sent to a legitimate cryptocurrency exchange. And I accept that buying cryptocurrency is a legitimate exercise. But both the Financial Conduct Authority (FCA) and Action Fraud had warned of cryptocurrency exchange and forex trading scams in 2018. And in May 2019 Action Fraud published further warnings that such scams had tripled in the past year. This type of insight is something that regulated businesses, including Halifax, ought to take notice of.

What this means is that even if Miss M had been sending money to a legitimate cryptocurrency exchange, it didn't follow that her money was safe, or that she wasn't at risk of financial harm due to fraud or a scam. By the time Miss M made the payment, I think Halifax had or ought to have had a good enough understanding of how these scams worked to have been able to identify the risk of harm from fraud. Including, that the customer often first purchases cryptocurrency and moves it on to the fraudster under the assumption that they're moving it into their own wallet or account.

I've considered the operation of Miss M's account in the year leading up to the disputed payments. In my view, the first payment of £1,000 wasn't particularly unusual or suspicious such that I think Halifax ought to have intervened. But it appears that Halifax did intervene at the time – it sent a One-Time Password (OTP) to confirm it was Miss M making the payment. Given the amount involved, this type of intervention doesn't seem unreasonable.

I'm not aware of Halifax intervening in the subsequent payments. The second payment – £5,000 on 29 February 2020 – was substantially higher than other transactions on Miss M's account. Like the investigator, I'm satisfied that this was so unusual that Halifax's systems ought to have triggered an alert and the payment paused, pending further intervention.

Given the amount involved, and the fact that the payment was to a cryptocurrency exchange, I consider it would have been reasonable for Halifax to have properly questioned Miss M before executing her authorised instruction. And in this instance, I don't think a limited intervention such as an OTP would have been sufficient.

Had Halifax carried out its due diligence and duties and asked Miss M about the payment, I've no reason to doubt that she would have explained what she was doing and the true purpose of her payment to Coinipop. She had been given no reason to think she had to hide this information from her bank, and neither had she been coached to tell them something different.

At the time of the payment, there wasn't information available to Halifax that EGM Finance was involved in a scam. A warning by the FCA wasn't published until August 2020. I accept that Halifax had no duty to protect Miss M from a poor investment choice or give investment advice. But it could have provided information about the steps a customer can take to ensure, as far as is reasonably possible, that they are dealing with a legitimate person or firm – such as checking the firm was authorised by the FCA.

Halifax could have also drawn on its own knowledge and information that was in the public domain – mentioned above – about the high risk associated with trading and the potential for fraud and provided Miss M with a potential scam warning.

Had Halifax done more, I'm satisfied that Miss M would have looked further into the investment opportunity in general, including whether EGM Finance was regulated here in the UK or abroad. She could have discovered that it wasn't. Indeed, it's likely that Miss M would have come across the various warnings about cryptocurrency exchange scams.

Although our investigator's view was that it's unlikely Miss M would have acted differently had Halifax intervened, for the reasons I've given above, I'm persuaded that a meaningful intervention from it would likely have exposed the scam. And I think it's more likely than not that intervention would have caused Miss M to stop from going ahead with the payment, thereby preventing further losses. So, I find that Halifax is liable for these losses.

Contributory negligence

I’ve also carefully thought about whether Miss M is partly to blame for what happened.

Miss M told our investigator that she’d done ‘some’ trading before. Halifax’s system contact notes from 2017 also confirm this. It is noted that Miss M mentioned incurring losses on her trade, including losing the capital she’d invested.

Other than telling our investigator that she looked up EGM Finance’s website, Miss M doesn’t appear to have carried out any independent research into the investment, the firm, or the investment type to reassure herself that the opportunity as presented to her in February 2020 was genuine.

Given her prior trading experience, I think Miss M ought to bear some responsibility for her 2020 losses and that compensation should be reduced accordingly. Having thought about this carefully, I think that it would be fair to reduce compensation by 25%.

Putting things right

To put matters right, Bank of Scotland plc trading as Halifax needs to reimburse Miss M the last two disputed payments as set out in the ‘what happened’ section, making a 25% deduction for contributory negligence.

As the payments were made from a current account, I consider it would be fair and reasonable for the bank to also add simple interest at 8%, payable from the date of loss to the date of settlement (less any tax properly deductible).

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require Bank of Scotland plc trading as Halifax to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I’m required to ask Miss M to accept or reject my decision before 14 September 2022.

Gagandeep Singh
Ombudsman