DRN-3296008

The complaint

Mr B complains that Bank of Scotland plc trading as Halifax didn't help recover money he lost as part of a scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything in detail again here. In summary, Mr B decided to invest in cryptocurrency after seeing an advertisement about a broker called RI Markets on social media. He left his contact details and was subsequently telephoned by an individual claiming to be a market expert and a financial adviser.

Mr B set up an account with RI Markets (who subsequently turned out to be fraudulent) and his debit card details were used for transactions on The Change and Safe Currency – both legitimate cryptocurrency exchanges. He was persuaded by his account manager at RI Markets to invest more money after seeing the profits that were supposedly being made. Mr B also took out a loan to fund some of the payments.

The following payments were made from Mr B's Halifax debit card:

Date (on bank statement)	**Merchant**	**Amount**
8 October 2019	TheChange	£630.00
15 October 2019	Rimarkets	£1,000.00
25 October 2019	PSP*safecurrency.com	£450.00
25 October 2019	TheChange	£2,625.00
28 October 2019	TheChange	£6,300.00
1 November 2019	TheChange	£315.00
6 November 2019	bconvert*thechange.io	£1,050.00
7 November 2019	PSP*safecurrency.com	£70.08 *(plus £2.09 non-sterling transaction fee and £0.50 non-sterling purchase fee)*
7 November 2019	PSP*safecurrency.com	£389.31 *(plus £11.64 non-sterling transaction fee and £0.50 non-sterling purchase fee)*
25 November 2019	PSP*safecurrency.com	£546.09 *(plus £16.32 non-sterling transaction fee and £0.50 non-sterling purchase fee)*
25 November 2019	PSP*safecurrency.com	£3,120.54 *(plus £93.30 non-sterling transaction fee and £0.50 non-sterling purchase fee)*
	Total payments	£16.496.02 *(plus £125.35 non-sterling fee)*
	Total loss	**£16,621.37**

Each time Mr B requested a withdrawal, RI Markets declined it on the grounds of bonus limitations and insufficient trades. He eventually realised he had been scammed when he discovered that the Financial Conduct Authority ("FCA") had published a warning about RI Markets.

Mr B reported the matter to Halifax. However, it declined to refund the money he lost. It said it was unable to raise a chargeback against The Change and Safe Currency as these institutions provided a legitimate service. And Mr B was out of time to raise a chargeback against RI Markets for the payment made directly to it. Unhappy with this, Mr B referred his complaint to our service.

Our investigator concluded that Halifax hadn't acted unfairly in declining the chargeback request. But she thought that it ought to have intervened and asked suitably probing questions when Mr B authorised the fifth payment of £6,300 as it was unusual and out of character for him. It was the investigator's view that had Halifax done this, it would have unravelled the scam and limited Mr B's loss. She recommended Halifax to refund all the disputed transactions from and including the fifth payment, along with interest and fees.

Mr B agreed with the investigator's recommendations, but Halifax didn't reply to her view despite several chasers. And it didn't respond to the notification that this complaint was being referred to an ombudsman. So, it's now appropriate for the case to move to the ombudsman stage.

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.

It's common ground that the disputed payments were authorised by Mr B for the purposes of the Payment Services Regulations 2017, in force at the time. This is because he had authorised RI Markets to make 'trades' on his behalf and the payments were made using his legitimate security credentials. While Mr B didn't intend for his money to go to fraudsters, he's initially presumed liable for the loss.

As a starting position, banks should execute an authorised payment instruction without undue delay. However, in accordance with the law, regulations and good industry practice, a bank has a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. If, in breach of that duty, a bank fails to act on information which ought reasonably to alert a prudent bank to potential fraud or financial crime, it might be liable for the losses incurred by its customer as a result.

So, I've looked into what this means for this case and whether Halifax should have done more here to prevent the payments in dispute.

I've considered the operation of Mr B's account in the months leading up to the disputed payments. Like the investigator, I don't consider the first four payments to be so unusual or uncharacteristic that I think Halifax ought to have intervened. But the fifth payment of £6,300 was substantially higher than other transactions on Mr B's account. The proximity and the substantial increase in value of the payment to a cryptocurrency exchange ought to have triggered Halifax's systems. And I consider it would have been reasonable for Halifax to have properly questioned Mr B before processing this payment.

Had Halifax contacted Mr B to ask relevant questions, I'm satisfied it would have been apparent that he was falling victim to a scam. If Halifax had asked Mr B what the payment was for and the basic surrounding context, it is likely he would have fully explained what he

was doing and that everything had originated from his 'broker' i.e. the fraudsters. So, while Halifax may have known that Mr B was sending money to a legitimate cryptocurrency trader, I think it still should have provided a scam warning in light of all the information known to banks about the increasing number of scams associated with fraudsters selling what is made out to be cryptocurrency.

After all, at the time, there was information in the public domain – which a bank ought to have known even if a lay consumer ought not – about the very high risks associated with crypto trading, including many warnings of potential fraud. For example, the FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018. Regulated businesses ought reasonably to take notice of such insight.

By the time Mr B made these payments, cryptocurrency scams had risen greatly in frequency and it is reasonable to conclude that banks, such as Halifax, had also had time to digest these warnings and put mechanisms in place to detect and prevent this type of fraud.

Even if an intervention by the bank would have identified that the payment was going to Mr B's own account with the cryptocurrency exchange, the conversation should not have stopped only on the basis that the money appeared to be going somewhere safe and within Mr B's control.

I say this because, by the time Mr B made these payments, 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 a customer often first purchases the crypto asset and moves the money on to the fraudster under the assumption that they're moving the money into their own wallet.

With this in mind, I would have expected Halifax to have asked questions about the context and true purpose of the payment. While it is not up to our service to dictate which questions a bank should ask, Halifax could have, for example, asked how Mr B had been contacted, whether he had parted with personal details in order to open a trading account, whether the investment opportunity was linked to a prominent individual, or advertised on social media etc. These are all typical features of cryptocurrency scams – and form part of a reasonable line of enquiry to protect a consumer from the potential risk of a prominent type of scam.

Although there is no reason to doubt that Mr B would have explained what he was doing, I accept it was possible that he might not have revealed enough information to lead Halifax to understand whether he was at risk of financial harm from this particular type of fraud (or any type for that matter). I can't know for certain what would have happened. However, I reach my conclusions not based on mere possibilities, but rather on what I find most probable to have happened in the circumstances. And on balance, I'm satisfied that Mr B would have likely shared information which aligned with the hallmarks of this type of scam, as he had been given no reason to think he had to hide this information from his bank, and neither had he been coached to tell them something different.

In light of this, I think Mr B's losses were foreseeable to Halifax despite the payment on the face of it not leaving his control. And I'm satisfied that had Halifax, having identified the payment as unusual and suspicious, asked relevant questions of Mr B, it would have been apparent that he was falling victim to a cryptocurrency scam.

Further, even if Halifax had not worked out that this was a scam, it is likely that a warning would have alerted Mr B to the common issues arising in relation to so-called cryptocurrency 'brokers'. Had it indicated the potential for fraud and provided Mr B with a potential scam warning, I'm satisfied he would have been concerned enough to have stopped in his tracks,

and he likely would have found the on-line reviews which had referred to RI Markets being a scammer (as he did later on).

Finally, I accept that, when simply executing authorised payments, banks such as Halifax don't have to protect customers against the risk of bad bargains or give investment advice. However, the FCA has confirmed that a fraud warning would not constitute unauthorised investment advice – so I don't think Halifax would have acted out of line, had it warned Mr B along the lines that I've described.

There's a general principle that consumers must take responsibility for their decisions. I've duly considered whether Mr B should bear some responsibility by way of contributory negligence. However, in this case, I don't think he could have foreseen the risk that the company he was dealing with was a scam. He simply did not appreciate what he was doing or the consequences of his actions.

All in all, I'm satisfied there was no contributory negligence on this occasion and Mr B was simply the unwitting and blameless victim of a clever fraudster. The bank was the professional in financial matters; Mr B was a layperson.

Putting things right

To put things right, Bank of Scotland plc trading as Halifax needs to refund Mr B the stolen payments from the fifth payment – £6,300 made on 28 October 2019 – onwards, including any non-sterling fees. That would mean an award of £11,916.37.

As this was a current account, Halifax should add simple interest at the rate of 8% per year (less any tax properly deductible), calculated from the respective date of loss to the date of refund.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 11 April 2022.

Gagandeep Singh
Ombudsman