DRN-3387388

The complaint

Mr M is unhappy that Bank of Scotland plc won't reimburse money he lost as a result of falling victim to a scam.

What happened

Mr M received what he thought was an email from a friend about an investment opportunity. He had been interested in cryptocurrency and believed this to be a good starting place and he knew of other people doing something similar. He saw some negative and positive reviews about the trader – Olympia Markets, later changed to Olympius Global.

He called the number in the email and was told he would be called a short time later. He was given a four-digit security number and was specifically told this was used to prevent scams. This led Mr M to believe it was legitimate. He started off with a small investment which increased over time. By his third payment, he was asked to download Anydesk and asked to apply for internet banking.

Around two weeks into the investment opportunity Mr M discovered his friend hadn't sent the initial email. But as he was already making a profit, and had been presented with an investment plan, he continued to invest. Mr M was also persuaded to take out a loan of £45,000 to place into his investment. Although the 'trader' completed the loan application on Mr M's behalf, he did confirm to Bank of Scotland the borrowing was for home improvements.

The transactions made are set out in the table below.

Date	Type	Merchant	Amount
07/10/2019	Debit card	SQPAY	£88.72
10/10/2019	Debit card	XCHANGEPRO+	£1,862.97
12/10/2019	Debit card	XCHANGEPRO+	£7,160.53
22/10/2019	Faster payment	CB Payments Ltd	£2.00
29/10/2019	Faster payment	CB Payments Ltd	£21,000
21/11/2019	Faster payment	CB Payments Ltd	£20,050
22/01/2020	Faster payment	CB Payments Ltd	£25,000
23/01/2020	Faster payment	CB Payments Ltd	£2,000
07/02/2020	Faster payment	CB Payments Ltd	£24,999

07/02/2020	Faster payment	CB Payments Ltd	£21,450
			£123,613.22

It was after the loan funds were invested that things started to go wrong, and losses were incurred. The trader suggested Mr M borrow more – another £50,000 – and it was at this point he became suspicious and contacted the bank. The bank strongly advised Mr M against having any further contact with the 'trader' informing him that he'd been the victim of a scam.

Bank of Scotland declined to raise a chargeback for the transactions, and it said they didn't meet the criteria. It also declined to provide any refund under the Lending Standard Board's Contingent Reimbursement Model (CRM) as it wasn't persuaded Mr M had taken reasonable care to confirm who he was paying was genuine. It said the faster payments likely triggered a warning but accepts it can't be sure Mr M would have seen them. It did agree to write off the loan.

Our investigator upheld the complaint. He said that under the CRM Bank of Scotland ought to refund customers who are victims of authorised push payment scams except in limited circumstances; and he didn't think those circumstances applied here. He also found that the bank ought to have intervened on the final payment made by debit card as the transaction was unusual and uncharacteristic for Mr M. So he asked Bank of Scotland to refund all transactions from the final debit card payment less the loan amount that had already been written off (and less a credit) and to add 8% simple interest to that sum.

Bank of Scotland never responded to the view, nor the notification it was being referred to an ombudsman. I'm satisfied the bank has been provided with sufficient opportunity to respond and so it's now appropriate for the case to reach this stage.

Bank of Scotland accepted my provisional decision. Mr M provided a copy of the investment plan he was provided by the 'trader' and said he was going to try and obtain a copy of the email purportedly sent by his 'friend'. The investigator explained they didn't think this was necessary given the findings in the provisional decision about what happened after it was sent. Mr M accepted that and the outcome reached.

I thank Mr M for going to the trouble of providing the investment plan. But I'm not persuaded this evidence means I should alter my provisional outcome or that it's no longer fair. As I've not been persuaded to alter my provisional decision, I make it final below.

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.

Under regulations, and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even if they were duped into doing so, for example as part of an investment scam.
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 banker to potential fraud or financial crime, it might be liable for the losses incurred by its customer as a result.

These transactions need to be dealt with in two parts; those made by debit card and the others by faster payment. That's because different considerations apply to the different types of payment.

The card payments

There doesn't appear to be any dispute that Mr M has been the victim of a scam. The payments made to SQPAY and XCHANGEPRO+ were made by Mr M using his card and associated security credentials. I therefore conclude these were authorised payments – for which Mr M is liable unless there is evidence the bank could and should reasonably have done more to protect him, which issue I now turn to.

Mr M made three payments using his card and so I have considered whether these ought to have triggered the bank's alert systems such that it ought to have questioned whether he was a victim of a scam and intervened. I have considered the operation of Mr M's account in the preceding months. I think it fair to say Mr M's first two debit card payments weren't so unusual or uncharacteristic that I think the bank ought to have intervened. It appears the bank did intervene at least to some degree with the first payment, although we haven't been provided with detail. But given the very low monetary value of the transaction it was likely seeking confirmation the transaction had been carried out by him. I don't consider the bank ought to have done more than that.

But the third payment of £7,160.53 was substantially higher than other usage on the account. And it was the second payment in a matter of days to a new payee which was a cryptocurrency exchange. I'm persuaded the close proximity, the substantial increase in value and that this was only the second payment to this payee ought to have triggered the bank's systems and paused the payment pending further intervention – such as making enquiries or giving a scam warning.

Had the bank asked appropriate probing questions, I've no reason to doubt that Mr M would have explained what he was doing. Like the investigator, I accept Bank of Scotland had no duty to protect Mr M from a poor investment choice. 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 – such as checking the payee was authorised by the regulator. And it could have drawn on its own knowledge and information that was in the public domain about the high risks associated with cryptocurrency trading, just as it did when Mr M contacted it to report the scam. Had it indicated the potential for fraud and provided Mr M with a potential scam warning, I'm satisfied he would have been concerned enough to have stopped, and he likely would have heeded the on-line reviews which had referred to Olympia Markets being a scammer.

I'm therefore minded to ask Bank of Scotland to reimburse the final debit card transaction of £7,160.53.

The faster payments

I have considered whether Bank of Scotland ought to have reimbursed Mr M under the provisions of the CRM, and whether it ought to have done more to protect him from potential financial harm from fraud. The CRM also places a level of care on customers such as Mr M, I have considered whether he met this. The CRM isn't applicable to card payments.

The CRM

The CRM requires payment services providers to reimburse customers who have been the victim of authorised push payment (APP) scams like this, in all but limited circumstances. It

is for Bank of Scotland to establish that a customer failed to meet a requisite level of care under one or more of the listed exceptions set out in the CRM.

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, but these aren't applicable here.

Bank of Scotland has said the size of the payments would likely have triggered a warning being provided but it no longer has a log of that. But it has also acknowledged that in the process of allowing the 'trader' access to his computer to the make the payments and trades, Mr M is unlikely to have seen any warnings. I agree with that.

So my consideration is in relation to whether Mr M had a reasonable basis for belief?

Under the CRM, Bank of Scotland can choose not to reimburse Mr M if it doesn't believe he took the requisite care to ensure he had a reasonable basis for belief that the person/business he was paying was legitimate and for genuine goods or services. It isn't enough for Mr M to believe that he was paying a legitimate business for genuine goods or services, he had to have a reasonable basis for belief; that needs to be in relation to each payment made. It's here I disagree with the some of the investigator's findings.

Mr M came across the trader after being sent an email from a friend. I understand the email contained a video of a well-known breakfast television show speaking to someone about investing in cryptocurrency. It was following the receipt of this email and Mr C providing his contact number, that he was given a four-digit code for security reasons. I can understand why this, along with the apparent involvement of a television programme, would have led to an air of authenticity.

However, about two weeks after the receipt of the email (around 21 October 2019), Mr M discovered his friend actually hadn't sent it to him. I think this ought to have raised enough suspicions for Mr M to have questioned whether he was paying a legitimate person or business. At that point he would have known that someone had lied by pretending to be his friend and had somehow gained his email address to provide a 'investment opportunity'. He ought to have questioned the lie and therefore whether the investment opportunity was legitimate. I'm not persuaded seeking out reviews then or relying on the previous reading of both good and bad reviews, is taking a sufficient level of care to ensure he had a reasonable basis for belief.

I also understand that the final two payments were made as a result of a loan being taken out with Bank of Scotland. I accept what Mr M says when he explains the loan application was actually completed by the 'trader' when he had access to Mr M's on-line banking. But I'm also aware that Mr M needed to call the bank to approve the loan application and he was told to say the loan was for home improvements, which he did. But that wasn't correct, Mr M had been asked to lie about the purpose of the loan by the 'trader'. I think this ought to have also alerted Mr M to something being wrong. If this had been a legitimate investment opportunity, then why would he need to lie to his bank about it? This simply isn't the type of instruction a legitimate person or business would ask its customer to do. I'm not aware that Mr M questioned this or satisfied himself that all was well.

Under the CRM where a business has failed to provide an effective warning, but the customer hasn't met the requisite level of care, each party must accept equal responsibility. In these situations the CRM requires the payment service provider to reimburse 50% of the losses.

I am satisfied that would be a fair and reasonable way to resolve this complaint. Whilst Bank of Scotland has accepted Mr M wouldn't have seen a warning, effective or otherwise, Mr M hasn't met the requisite level of case to ensure he was paying a legitimate business for genuine services. He gave little time or attention to the warning signs and gave credence to instructions that required him to lie to his own bank. In making this award, it's also fair I take into account that Bank of Scotland has already agreed to write off the loan.

My final decision

For the reasons given, my final decision is that I uphold this complaint in part, and require Bank of Scotland plc to:

- reimburse the final debit card transaction of £7,160.53. It should also add 8% simple interest per annum to that sum from the date of payment to the date of settlement; and
- reimburse 50% of the faster payments, less the loan amount already written off and less £169.61 credit he received, totalling £33,856.39. It should also add 8% simple interest per annum from the date it declined to reimburse Mr M to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 19 April 2022.

Claire Hopkins
Ombudsman