DRN-3793827

The complaint

Mr T complains that Starling Bank Limited hasn't refunded him the money he lost when he fell victim to an investment scam in 2021.

Mr T brings his complaint with the aid of professional representation, but for clarity in what follows I will refer throughout just to Mr T.

What happened

Mr T says he'd been researching potential investments for some time. He was recommended to contact a specific trader by someone he'd spoken to on social media.

Mr T made contact with the trader through an instant messaging platform. The trader claimed to a be involved in foreign exchange (forex) trading. Mr T was told about a range of trading options and was told these would give a return of nearly ten times his initial investment within a week, or more after two weeks. The broker said this was a guaranteed return.

Keen to proceed, Mr T made initial payments from his account held with another bank. He appeared to be making significant profits but was told he needed to pay fees.

The first payment he made from his Starling account was a debit card payment of £996.73. This payment was made on 10 November 2021, to Mr T's account at a legitimate cryptocurrency exchange.

Once the funds had been received at the exchange, Mr T purchased cryptocurrency which he then sent to the destination wallet he'd been instructed to use by the trader. He was told this would credit his account with the trader's online platform. Mr T was able to log on to this platform and view the credits and subsequent trades being made.

Over the course of the next five weeks, Mr T made further payments from both his Starling account and from his account with another bank. From his Starling account, in total, Mr T sent eight card payments and four Faster Payments transfers, amounting to a net figure of over £14,000. These went to several different destinations.

But despite having already paid for multiple fees he hadn't been expecting, Mr T was asked to pay more. Mr T realised this couldn't be right and when he spoke to Action Fraud it was confirmed he'd been scammed.

He then reported what had happened to Starling on 24 November. After reporting the scam, Mr T made two further faster payment transfers for smaller sums to one of the accounts in his own name. However, Mr T explains these were also connected to the scam.

Starling said it had no rights to chargeback the card payments Mr T had made to his accounts with the cryptocurrency exchanges. This was because Mr T wasn't disputing having been provided the service he'd paid for from those merchants (the purchase of cryptocurrency). The loss had happened later - when Mr T sent that cryptocurrency onwards

to the destinations specified by the scammer.

Of the four bank transfers Mr T had sent, three were made to accounts he held and controlled in his own name. No funds remained for possible recovery because he'd used all of the money he'd sent to buy cryptocurrency, which he'd then sent onwards to the scammer. But for the single payment Mr T had made to another person, Starling contacted the recipient bank and attempted to recover the money he'd sent. Unfortunately, the scammer had moved the money on, and none could be recovered.

Starling didn't think it was liable to reimburse Mr T. It had carried out the transactions he'd authorised and had no reason to have prevented him from making these payments. It pointed out that all but one of these payments had gone to accounts in Mr T's own name, so the point of loss hadn't been the payments from Mr T's Starling account but had occurred when he'd subsequently sent the funds onward from his accounts elsewhere.

For the single payment Mr T had transferred to another person, Starling thought he hadn't held a reasonable basis for believing he was paying for a legitimate investment or paying the person he expected to pay. Mr T didn't accept what Starling said.

Our Investigator looked into Mr T's complaint about Starling. He was sympathetic to the loss Mr T had sustained through this scam. But he didn't think Starling had treated Mr T unfairly in declining to reimburse him. He didn't think that the payments would have appeared sufficiently remarkable that Starling ought to have intervened to discuss the payments with Mr T before processing them.

The Investigator noted that the Lending Standard Board's Contingent Reimbursement Model Code (the CRM Code) can provide additional protection to victims of some Authorised Push Payment scams. But he said this could only be applied to payments made to an account not controlled by Mr T – which in this instance meant it could apply to just one of the twelve payments Mr T had made.

In relation to that one payment, the Investigator thought Starling was entitled to choose not to refund Mr T under the terms of the CRM Code. He didn't think Mr T was vulnerable under the terms of the code, didn't think Mr T had held a reasonable basis for believing what he did, and didn't think the provision of an effective warning by Starling would have had a material effect on preventing the payment.

Mr T didn't accept this. He thought Starling should have identified the payments as being unusual. It had required him to authenticate some of the payments using One Time Passcodes (OTPs) and using his mobile app to verify the instructions. He'd spoken to Starling about at least one transaction.

The Investigator asked Starling to clarify these points. Starling explained that its records showed only one time where it had spoken to Mr T during the sequence of these payments. That had been when Mr T had called to request a payment was cancelled as he had been unable to complete ID verification when opening a new account with the merchant. That payment had not gone ahead. The call hadn't prompted any concerns.

Mr T remained dissatisfied with the Investigator's findings. In light of this disagreement, I have been asked to review everything afresh and reach a final decision on the matter.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

I'm sorry to hear about what happened to Mr T. I can understand entirely why he considers his money should be returned. He's been the victim of a crime here, and he's explained the impact it's had. He was deceived by a scam that led him to believe the trader was investing his money and making a significant profit. Mr T's been left out of pocket by a significant sum as a result. So, I can appreciate why he'd now like Starling to refund what he's lost, and why he wants Starling to take the blame.

However, the main cause of these losses were the scammers who deceived Mr T. For me to say Starling is liable in this type of situation, I would need to find that the bank could and should have acted to prevent the eventual loss, or that it failed to meet its obligations in some other way.

Here the payments Mr T made during the course of the scam were a mixture of card payments and Faster Payments bank transfers.

A voluntary code does exist to provide additional protection against some scams (the Contingent Reimbursement Model Code – CRM Code). Starling is a signatory to the code. But as the Investigator explained, the CRM Code does not apply to card payments, only to some faster payment transfers. And transfers made to accounts under a customer's own control won't normally be covered by the CRM Code.

That matters because all but one of the accounts to which Mr T sent money from his Starling account were accounts registered in his own name and in his control. He'd set these up and knew they were being used as a route to move money on to the trading platform. So, based on what I have seen, I find that the CRM Code provisions don't apply to eleven of the twelve payments Mr T made. I find it does apply however to the single payment he made to an account held by another person - the £2,800 transfer he sent on 20 November 2021. I will address this payment first.

The payment covered by the provisions of the CRM Code: £2,800 on 20 November 2021

In relation to this payment, I've considered whether Starling has fairly declined to reimburse Mr T under the terms of the CRM Code, or whether it should have done more.

The CRM Code permits a bank to decline to reimburse a customer when, amongst other things, it can establish that the customer made a payment without a reasonable basis for believing that they were paying for a legitimate service or that they were paying the person they intended to pay. Starling seeks to rely on this here.

I have considered the circumstances surrounding this payment, to determine whether I think Starling has fairly assessed Mr T's claim. Firstly, based on the evidence available, including the chat history between Mr T and the scammer, I don't find Mr T was unable to protect himself at the time from this scam. I don't find he met the definition of vulnerability in the CRM Code.

While aspects of the scam were undoubtably convincing, I think there were significant red flags that ought to have prompted Mr T to have doubts about the legitimacy of the payments he was making. And I consider Mr T did have concerns that the payments he was being

asked to make weren't being properly explained to him, including the fees he was asked to pay. However, I think Mr T was willing to overlook these concerns in the hope of achieving returns that were simply too good to be true.

I consider that Starling should have provided Mr T with a warning at the time he was making this payment. This was required to meet the requirements of an Effective Warning under the provisions of the CRM Code. While Starling did give a scam warning, I am not satisfied that what it provided was sufficient to meet the Code's minimum requirements. However, I don't find this shortfall was material to the success of the scam – all taken into account I consider it most likely Mr T would still have gone ahead with the payment even had Starling provided an Effective Warning at that point.

I say this in light of the fact that the scam had been in operation for some time and Mr T was considerably under the scammer's spell. And even after Mr T had identified he'd likely been scammed and had discussed this with Action Fraud, he still made two further transfers. On balance I find it unlikely that even an effective warning message at the time of this payment would have stopped him.

Overall, having carefully considered the representations made by both sides, I think Starling has established that it can fairly choose not to reimburse Mr T for the payment covered by the CRM Code.

Considerations besides the CRM Code

However, while I therefore find the CRM Code does not apply to all but one of the transactions Mr T made, that Code is not the full extent of the relevant obligations that could apply in cases such as this.

First of all, under the relevant regulations, and in accordance with general banking terms and conditions, banks have a primary obligation to execute an authorised payment instruction without undue delay. As a consequence, the starting position is that liability for an authorised payment rests with the payer, even if they made that payment as the consequence of a fraud or scam - for example as part of an investment scam such as this was.

However, where the customer made the payments as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though the customer authorised the transactions. I consider that a bank also has a duty to take reasonable steps to protect its customers against the risk of fraud and scams.

In particular, I consider that as a matter of good industry practice Starling should have been looking out for payments or payment patterns that were significantly out of character or unusual and that might therefore be indicative of the potential for financial detriment to its customer through fraud or a scam.

In short, the test I need to apply here is whether the evidence is such that I consider Starling ought to have had significant concerns that these transactions could be indicative of possible financial harm through fraud or a scam – to the extent that this would have overcome its primary obligation to carry out Mr T's payment instructions.

With all of the above in mind, I've thought carefully about whether the available evidence demonstrates that Starling did enough given the specific circumstances here.

While I've carefully considered all the evidence and points raised by Mr T, I don't consider these payments, were so significantly unusual that I could find Starling at fault for not having taken further steps than it did. Mr T had only held the account for a few months prior to the

scam, so Starling had limited prior history against which to compare these payments.

I've reviewed the call Mr T has referenced. But I am satisfied that Starling reasonably didn't have concerns based on that call. There was nothing in the call to suggest Mr T would be about to fall victim to a scam.

And I consider it relevant that all (bar one) were made to accounts held in Mr T's own name, which all things being equal would have had the effect of reducing the apparent risk of loss through fraud or scam. When some weeks after the initial scam had come to light Mr T sent two smaller payments to his cryptocurrency exchange wallet, I don't think Starling, in the circumstances would have had cause to think these weren't now legitimate transactions. These were payments to a wallet Starling knew was held by Mr T, and I don't find it was unreasonable for it to have assumed he was pursuing legitimate, if risky, investments now - having already uncovered and reported the scam and knowing what he now knew about scam risks.

On balance, and taking everything into consideration, I do not find that there was enough here for me to say Starling should have intervened rather than fulfil its primary obligation to carry out Mr T's instructions.

Further I am satisfied that when Starling was made aware of the scam, it took the appropriate actions. This included its attempts to recover Mr T's lost funds. However, those funds had already been moved on from Mr T's own accounts in the course of the scam, and nothing remained in the one account that hadn't been in Mr T's own name. So, it simply wasn't possible for Starling to recover the money he'd lost.

Overall, I don't find Starling was at fault here. I can't fairly require Starling to refund these payments.

In saying this, I want to stress that I am very sorry to hear about what happened to Mr T and I am sorry he has lost out. Mr T was the victim of a crime, and what was a cruel scam designed to defraud him of his money. I appreciate that what he's lost here adds up to a significant sum. But it is simply the case that I don't find Starling was at fault in making these payments in line with the instructions he gave at the time, and I don't find the bank liable to refund him for any other reason.

My final decision

For the reasons given above, I do not uphold Mr T's complaint about Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 27 July 2023.

Stephen Dickie
Ombudsman