DRN-4676782

The complaint

Mr S complains that Starling Bank Limited didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

At the start of 2021, Mr S decided to look into cryptocurrency investments and came across someone who claimed to work for an investment company which I'll refer to as T", which was unfortunately a clone of a genuine company.

He received a call from someone who I'll refer to as "the scammer" who told Mr S he could make substantial returns by investing in cryptocurrency and before deciding to go ahead, he conducted internet searches to check T was legitimate.

The scammer asked him to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Between 1 March 2021 and 26 March 2021, he made nine debit card payments and four faster payments to three cryptocurrency exchange companies totalling £67,025.38.

Mr S maintained regular contact with the scammer who regularly updated him on how his trades were performing and showed him his profits on the account, encouraging him to invest more funds to increase his earnings. Mr S also verified the performance of his trades on third party websites which confirmed the trades were correct and reflected in the market.

Mr S realised he'd been scammed when he tried to make a withdrawal and was unable to do so. He complained to Starling stating it should have stopped the payments, but it refused to refund the money he'd lost. It said that when he set up a new payee, he was given warnings which he read before proceeding with the payments. It said the payments weren't deemed suspicious by its systems, he had authorised each payment and had a duty to exercise good judgement when instructing it to execute a genuine payment instruction.

Mr S wasn't satisfied and so he complained to this service with the assistance of a representative who said Mr S had no experience of online investing and the lost funds represented a large proportion of his personal savings. He wasn't aware of the risks associated with cryptocurrency and it wasn't reasonable to expect him to have protected himself.

They said Starling should have intervened because Mr S had made numerous large payments to cryptocurrency exchange platforms, which was unusual compared to his normal spending habits. It should have performed further checks and provided warnings to ensure he was aware of the potential risks.

Starling said it wouldn't have been possible to recover the funds because the payments were reported nearly two years after the scam had occurred. It explained the payments weren't covered under the Contingent Reimbursement Model ("CRM") code because Mr S had paid accounts in his own name.

It maintained it had provided a sufficient warning when Mr S set up the payee details, which he acknowledged before proceeding with the payments. The account was blocked on 15 March 2023 due to the merchant not accepting its security rules. Mr S contacted it and said he wanted to make further payments to B and a referral was made to its fraud team. In a further call, Mr S explained that he was paying his personal cryptocurrency account and that he had full access to the account. He was asked if he'd done any research, checked the Financial Conduct Authority ("FCA") website and if he'd set up the account himself. He said he'd uploaded his ID documents himself and that he was sending funds directly to the trading platform on the advice of a broker.

Our investigator felt the complaint should be upheld. She explained that a chargeback claim wouldn't have been successful because Mr S paid legitimate cryptocurrency exchanges and received a service, which would have involved changing his payments into cryptocurrency before sending it to the wallet address he supplied it with. She also accepted there would have been no chance of a successful recovery because the funds were paid into account in Mr S's own name and moved on from there.

She didn't think the first nine payments were unusual because Mr S had made payments for similar amounts in the months prior to the disputed payments. He'd also made multiple larger payments in consecutive days. And in February 2021, he'd made payments to two different cryptocurrency merchants, so the account had previously been used for payments to cryptocurrency merchants.

But she noted that during the calls on 15 March 2021, Mr S had said he was buying cryptocurrency and he had a broker who worked for a London based company called T. He said T was a large company and that it was regulated by the FCA, and the call handler said he was happy for Mr S to make the payment. There was no scam warning and no further discussion about T.

Our investigator thought that if Starling had asked further questions, it would have been apparent that Mr S was falling victim to a scam. She noted the genuine T is based in Cyprus and the logo and background information on the scam website is very different to the website of the genuine company. So, if the call handler had told Mr S how to check for clone companies, he would have detected the scam.

She recommended that Starling should refund the money Mr S had lost from 15 March 2021 onwards. However, she noted he was contacted out of the blue by the scammer and even though he had said he'd completed some checks, the information which showed T was a clone company would have been easily discoverable. Further, she'd seen an email dated 22 March 2021 which confirmed Mr S had over $178,000 in his trading account, making over $90,000 profit at a margin level of 61%. She felt this was too good to be true and should have raised concerns. And he'd invested over £72,000 in just over three weeks without attempting to make a withdrawal, which would have uncovered the scam sooner.

Consequently, while she was satisfied Mr S had fallen victim to a sophisticated scam, she didn't think he'd acted reasonably in the circumstances therefore the settlement should be reduced by 50% for contributory negligence.

Starling has asked for the complaint to be reviewed by an Ombudsman arguing that Mr S had said he was investing in cryptocurrency and had full access to the funds. It has

questioned why it was Starling's responsibility to offer warnings about clone companies when Mr S had confirmed that he'd completed due diligence and had access to the platform. It has argued that if it had any reason to believe that T wasn't a genuine company, it would have offered specific warnings, but it doesn't think this would have prevented him from making the payments because he was confident he knew what he was doing.

It has further argued that Mr S didn't say the broker had control over the funds or that he was telling Mr S what to do and it maintains it met its responsibility by offering warnings based on the information provided to it by Mr S.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. But the code didn't apply to these payments because it doesn't to debit card payments. And it doesn't apply to the faster payments because Mr S paid accounts in his own name.

I've thought about whether Starling could have done more to recover the debit card payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Starling) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Ms S).

Ms S's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr S's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Starling's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I'm satisfied Mr S 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr S didn't intend his money to go to scammers, he did authorise the disputed payments. Starling is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Starling could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to genuine cryptocurrency exchange companies. However, Starling ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr S when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Starling to intervene with a view to protecting Mr S from financial harm due to fraud.

The first nine payments didn't flag as suspicious on Starling's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr S normally ran his account, which he opened in December 2020, and I don't think they were. This is because all the payments were to legitimate cryptocurrency exchange companies and as Mr S had made payments for £5,000, £1,000, £5,000, £4,250, £1,000, £10,000, £5,000, and £1,000 between 24 February 2021 and 26 February 2021, the amounts weren't unusual for the account. He'd also made payments to cryptocurrency merchants on 1 February 2021 and one 22 February 2021.

However, there was an intervention on 15 March 2021 when Mr S tried to pay £9,000 to B and so I've considered what took place during that interaction. During the two calls, Mr S said he was sending money to his Bitcoin account and that the account was in his name. He also said he'd sent money to the account before and that the payment had been received.

Significantly, he told the call handler that he was taking advice from a broker who worked for T, and while I accept he didn't say the broker had control over the funds, or that he was telling Mr S what to do, he did say he'd been advised by the broker to make an onwards payment from B to the trading platform. This ought to have raised red flags that Mr S was being scammed and the call handler should have picked up on this and asked some probing questions around how he'd met the broker, whether he'd been told to use remote access software, whether he'd been promised unrealistic returns and whether he'd made any withdrawals. And as there's no evidence Mr S had been coached to lie and he was honest during the calls, I'm satisfied he'd have been completely open about the circumstances.

I accept the call handler did discuss due diligence with Mr S but as there were some very clear red flags present, he ought reasonably to have been given a tailored warning about cryptocurrency scams including the risk of clone companies and specific information about how to check the investment company wasn't a clone of a genuine company. Had it done so I'm satisfied he'd have followed the advice to do more checks and realised that the genuine company was based overseas (and not in London) and that the website and logo was different and that this would have uncovered the scam. Because of this I think Starling should refund the money Mr S lost from 15 March 2021 onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and in the circumstances, I think Mr S did contribute to his own risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mr S to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

I'm also satisfied that he'd done what he considered was reasonable due diligence in that he believed T was regulated by the FCA. He also believed the trading platform was genuine and was reflecting the fact his investments were doing well.

This was a sophisticated scam, Mr S hadn't invested in cryptocurrency before and this was an area with which he was unfamiliar, so I wouldn't expect him to have been concerned that T could be a clone of a genuine company without having been warned by Starling that this was a potential risk. However, as our investigator has pointed out, a simple google search would have shown that T was based overseas and not in London as Mr S had been led to believe, and as I've stated above, I'm satisfied this was information which would probably have led to further enquiries which could have detected the scam. He also invested over £70,000 in three weeks without making any withdrawals, which might also have uncovered the scam sooner.

Because of this I agree with our investigator that the settlement should be reduced by 50% for contributory negligence.

Compensation

I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I don't think Starling needs to pay any compensation given that I don't think it acted unreasonably when it was made aware of the scam. And he wasn't entitled to compensation for legal fees, as our service is free to access.

Recovery

Mr S has described that he paid accounts in his own name and from there the funds were moved to an online wallet in the scammer's control, so I'm satisfied there was no prospect of a successful recovery.

My final decision

My final decision is that Starling Bank Limited should:

- Refund the money Mr S lost from 15 March 2021 onwards.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Starling Bank Limited deducts tax in relation to the interest element of this award it should provide Mr S with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 8 July 2024.

Carolyn Bonnell
Ombudsman