DRN-4355704

The complaint

Mr V complains that Starling Bank Limited didn't do enough to protect him from the financial harm caused by an investment scam company, 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.

Mr V responded to a job advert and was sent a number for someone who I'll refer to as "the scammer" who claimed to work for Company G. The scammer, who Mr V understood to be the hiring manager, contacted him via WhatsApp told him about an opportunity to make money by buying USDT through a cryptocurrency exchange company and using it to make orders on G's website.

The scammer told Mr V to buy cryptocurrency and then send it to the scam company as payment for the orders. Between 12 December 2022 and 14 December 2022, he made sixteen transfers to six different accounts totalling £2,367 from his Starling account. During the scam period he also received three credits into his account totalling £34.

Mr V realised he was the victim of a scam when he was asked to pay money to withdraw funds from the website. He complained to Starling, and it refused to refund any of the money he'd lost. It said it was unable to consider the claim under the CRM code because the funds were paid into an account in his control, and the money was lost after the USDT credited the cryptocurrency exchange account. It said it was unable to provide any reimbursement and his claim lay directly with the cryptocurrency exchange. It also said it wouldn't be able to mediate the payments as faster payments aren't covered under the Mastercard chargeback scheme.

Mr V wasn't satisfied and so he complained to this service. He said Starling should have done more to protect him against the scam by stopping the payments and calling him to warn him that the job was a scam.

Starling said the payments weren't high value or high risk, however Payment 11 was flagged on 13 December 2022 and Mr V stated he was paying for 'web services' and had received the service/item. It said Mr V's responses didn't reflect the situation and as he confirmed he'd already received the item/service, it had no cause for concern and released the payment. Later the same day Mr V was presented with a scam warning when he set up the payee details for Payment 13 and the details didn't match. On this occasion he acknowledged this and proceeded with the payment.

Starling further stated there was no evidence Mr V had done any background research on G and if he'd researched the opportunity, he would have realised it wasn't genuine. In particular, he ignored the fact he wasn't given any employment documentation, he was asked to use his own money and he was communicating with the scammer via WhatsApp.

Our investigator didn't think the complaint should be upheld. She explained the CRM code wouldn't apply to the payments because there was no evidence the beneficiary account holders intended to defraud Mr V. She explained the beneficiaries were third parties who were selling the cryptocurrency and Mr V received cryptocurrency, which he then sent to the scammers.

She didn't think Payments 1 to 10 were unusual as the account had a history of transfers of similar value as well as multiple credits and transfers made on the same day. She said Starling contacted Mr V when he tried to make Payment 11 and that he confirmed was for 'Web services', and that he'd received the services he paid for. Considering the value of the payment, she was satisfied the intervention was proportionate and that his response meant it was reasonable for Starling to have released the payment.

She explained Starling intervened again when Mr V made Payment 13 because the beneficiary account name didn't match the name Mr V provided. She noted the warning shown on the screen didn't have any information relating a particular scam, but she didn't think the payment was unusual or that the fact the beneficiary didn't match was reason to block the payment, so she was satisfied it was reasonable for Starling to have released the payment.

Finally, she noted the remaining payments were in line with the earlier spending on the account, so she didn't think Starling needed to intervene again.

Mr P has asked for his complaint to be reviewed by an Ombudsman. He's questioned why our investigator has rejected his complaint having said Starling should have done more and why she said the CRM code didn't apply.

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. I'm sorry to hear that Mr V has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr V says he's fallen victim to, in all but a limited number of circumstances. Starling has said the CRM code didn't apply in this case because the money was lost after the USDT credited the cryptocurrency exchange account, and I'm satisfied that's fair. The payments weren't fraudulent because Mr V received the cryptocurrency he paid for, so the CRM Code would not apply to the disputed payments.

Similarly, as he received the cryptocurrency, I wouldn't expect Starling to recover the funds from the recipient accounts.

I'm satisfied Mr V '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 V is presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing

returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I've carefully considered the circumstances, and I am persuaded this was a scam. But, although Mr V didn't intend him 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 to legitimate accounts. However, Starling had an obligation to 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 V 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 V from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr V normally ran his account and based on the fact the payments were low value payments to different beneficiaries, I don't think the Payments 1 to 11 were suspicious or unusual. Payment 11 is the fifth payment to the same beneficiary on the same day and so its reasonable that it flagged, and I'm satisfied the nature of the intervention was proportionate. Mr V stated he was paying for Web services and that he'd received the service he paid for and so I'm satisfied it was reasonable for Starling to have released the payment based on the information it had.

Starling intervened again on the same day because the payee details didn't match the name Mr V provided. On this occasion, he was given a generic scam warning, which he acknowledged before proceeding with the payment. I'm satisfied the nature of the intervention was appropriate and I don't think it needed to do anything else in respect of that or any of the later payments.

I'm sorry to hear Mr V has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Starling is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr V to accept or reject my decision before 16 November 2023.

Carolyn Bonnell
Ombudsman