DRN-4895577

The complaint

Mr E complains that Think Money Limited won't refund money he lost when he was a victim of a crypto scam.

Mr E is represented by a firm that I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

Mr E says that, in 2021, he came across an online interview with Peter Jones in which he explained investing in the World Trade Centre had earnt him a significant income during the Covid-19 pandemic. Intrigued by this, Mr E clicked on a link that took him to the scam firm's website – which appeared legitimate to him. So, he left his name and contact details.

Following a conversation with the scammer, Mr E paid a £250 start up fee. This was sent from another bank account held by Mr E. The initial investment was showing as making a small profit and, as the scammer told Mr E the more he invested the greater the profits he would yield, Mr E decided to invest a further £3,500. He opened an account with Think Money on 6 September 2021 and made the debit card payment to the scammer's trading platform, via a legitimate crypto exchange, on 9 September 2021.

Mr E has said he realised he was scammed about a week later when the scammer was asking him to invest more money. But when he told the scammer he didn't have the funds, the scammer became aggressive and then cut off contact.

C complained to Think Money, on behalf of Mr E, on 24 October 2023 saying the payments were made as part of a scam. They considered Think Money failed in their duty of care to protect Mr E from the scam as they allowed the £3,500 payment to leave his account without carrying out any additional checks or providing appropriate scam warnings. This was despite Mr E making a high value payment to crypto on a newly opened account which depleted his account balance. C said Think Money didn't identify major 'red flags' and missed an opportunity to deliver effective warnings to prevent the scam. Because of this, C wanted Think Money to reimburse Mr E his loss from the scam – along with 8% simple interest and £300 compensation.

Think Money didn't uphold the complaint. They said, in accordance with their terms and conditions and in compliance with the Payment Service Regulations (PSR), they were unable to investigate the matter as Mr E had to tell them about the disputed transaction no later than 13 months after it was made.

Mr E referred his complaint to the Financial Ombudsman. Our Investigator explained to Think Money that the 13-month time limit they'd referred to was in respect of unauthorised transactions, which wasn't the case here as Mr E did authorise the payment. Think Money investigated the matter further but their position didn't change. They said they sent Mr E a text message to confirm it was himself making the £3,500 payment – to which he responded

'yes'. Think Money also noted that the payment went to a legitimate crypto site and they hadn't seen anything to show what the funds were intended for or who it went to, and so it could've been successfully used by Mr E. Think Money further added that, in accordance with the terms and conditions and relevant regulations, they executed the authorised payment instruction without undue delay as per the customer's request. And that they would deem this scam to have taken place on the crypto site.

Our Investigator didn't think Think Money had to do anything further. This was because she didn't think the payment was suspicious enough for Think Money to have significant concerns Mr E was at risk of financial harm from fraud. So, she thought the security check they did carry out was proportionate to the risk associated with the payment and she wouldn't have expected further checks to have been carried out. Our Investigator also explained that the only option of recovery was via chargeback - but this likely wouldn't have been successful as Mr E received the service from the crypto exchange.

C disagreed and requested the case be reviewed by an Ombudsman. The matter has therefore been passed to me to decide. C has, in short, added:

- They think newly opened accounts should be subjected to further scrutiny as there is no history to compare payments, which creates a higher risk.
- In 2021, Think Money should have had clear security measures in place, especially to combat Money Laundering as it is more common in new accounts.
- Although the crypto exchange was legitimate, the Financial Conduct Authority (FCA) had provided advice to banks and consumers about the prevalence of crypto scams. They don't believe Think Money had taken this on board at the time.
- Had Think Money implemented security measures in light of the FCA warnings, they would've intervened on the scam.
- The Investigator has mentioned that Think Money did flag the payment at the time, proving that it was suspicious. As such, Think Money ought to have done more.
- Mr E didn't receive any form of effective warning. They therefore cannot agree no refund is due.

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.

I'm sorry Mr E has been the victim of a scam and I'm sympathetic to the impact this matter has had on him. But I must consider whether Think Money is responsible for the loss Mr E has suffered. Having done so, and while I realise this isn't the outcome Mr E is hoping for, for similar reasons as our Investigator, I don't think they are. Because of this, I don't think Think Money has acted unfairly by not refunding the payment. I'll explain why.

In broad terms, the starting position in law is that an Electronic Money Institution (EMI) is expected to process payments that their customer authorises them to make. It isn't disputed that Mr E knowingly made the payment from his Think Money account and so, I'm satisfied he authorised it. Therefore, under the PSRs and the terms of his account, Think Money are expected to process Mr E's payment and he is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Think Money to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

So, the starting point here is whether the instruction given by Mr E to Think Money was unusual enough to have expected additional checks being carried out before the payment was processed.

When considering this, I've kept in mind that EMIs process high volumes of transactions each day. And that there is a balance for Think Money to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate. Here, the payment was made to a legitimate crypto exchange. And while there are known fraud risks associated with crypto that are well-known to EMIs, as scams like this have unfortunately become more prevalent, many individuals invest in crypto legitimately.

In this case, the account was newly opened with no prior account activity – which prevented Think Money from establishing whether the payment was out of character for Mr E. But while I've noted C's argument that a newly opened account should be subject to further scrutiny, at the time this payment was made, I think it was reasonable for Think Money to take into account a range of factors when deciding whether to make further enquiries of their customer about a particular payment. And here, I'm not persuaded the value of the payment – to a legitimate crypto exchange – indicated a heightened risk of financial harm whereby I would've expected additional checks (beyond the security check) to have been carried out before processing the payment. With consideration given to the FCA's advice that C has referred to, I'm satisfied that Think Money's security check was a proportionate response to the risk the payment presented.

On a final point, C has also argued that Think Money ought to have had security measures in place to combat Money Laundering as they consider it to be more common in newly opened accounts. There hasn't however been any suggestion that Mr E was undertaking illegal activities in respect of money laundering. I therefore can't reasonably conclude that Think Monday failed to fulfil their regularity obligations in this regard.

It follows that I think it was reasonable for Think Money to process the payment upon receiving confirmation from Mr E, in response to their security check, that he authorised it.

I've considered whether, on being alerted to the scam, Think Money could reasonably have done anything to recover Mr E's losses, but I don't think they could. The only possible option for recovery here, given the payment was made by debit card, would have been via a chargeback claim. But given the payment was for the purchasing of crypto with a legitimate firm, I don't think a chargeback claim would have been successful as Mr E received the service he paid for. I'm also mindful that Think Money were notified about scam payment roughly two years after it was processed and so, it would've likely been outside the relevant scheme providers' time limits. As such, I wouldn't have expected Think Money to have raised a chargeback claim here.

I have a great deal of sympathy for Mr E and the loss he's suffered. But it would only be fair for me to direct Think Money to refund his loss if I thought they were responsible – and I'm not persuaded that this was the case. For the above reasons, I think Think Money has acted fairly and so I'm not going to tell them to do anything further.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 3 October 2024.

Daniel O'Dell
Ombudsman