DRN-4771243

The complaint

Mr H complains that J.P. Morgan Europe Limited, trading as Chase, won't refund the money he lost when he fell victim to an investment scam.

Mr H is being represented by a claims management company in this complaint.

What happened

The details of what happened are well known to both parties and have been previously set out by the investigator in their assessment. So, I won't repeat the background and the arguments again here, Instead, I'll focus on giving my reasons for my decision.

The complaint concerns three transactions – two card payments and a faster payment – totalling £6,250 which Mr H made from his Chase account in September and October 2023. These were made in connection with an investment opportunity which turned out to be a scam.

The Chase account was opened just prior to the transactions, under the instructions of the scammer who guided Mr H throughout the scam until he discovered he'd been duped into sending money to them. Mr H made deposits into his Chase account from his account held with another bank, before making payments to purchase cryptocurrency. The cryptocurrency was then sent on to wallets as instructed by the scammer.

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.

The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr H made the payments, and so they are authorised. But a payment service provider has a duty to protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert it to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

This was a newly opened account, so there was no previous spending activity for Chase to compare the transactions with. I don't consider the first two disputed transactions – card payments of £250 and £1,000 on 15 and 30 September respectively – to be *that* unusual such that I think Chase ought to have taken additional steps before executing Mr H's authorised instructions. However, in my view, the next transaction – a faster payment of £5,000 on 9 October – should have prompted further enquiries. And I can see that it did since Chase discussed the payment with Mr H before processing it.

I've listened to the call recording, and Chase's agent asked Mr H to confirm the purpose of the payment. He confirmed he was purchasing cryptocurrency. The agent asked him if he'd moved money to that account before and it was established that Mr H had previously used his card to make the payment. Mr H also confirmed that he was funding the payments from

his account with another bank, and he couldn't transfer the funds to his cryptocurrency wallet directly from that account. He also told the agent that he'd been investing in cryptocurrency for two months had had received returns in that period. Mr H was also asked and he confirmed that he had not been forced to make the payment and not been told he needed to move money to a safe account.

Chase's agent also asked Mr H if he'd spoken to a trusted friend or family member or sought advice from someone other than the person he was dealing with. His response was that he was doing this all on his own, indicating that there was no one else involved with the investment trading. The agent then asked Mr H if he had checked that the company he was dealing with was registered with the Financial Conduct Authority to make sure he was dealing with an authorised company. Mr H answered yes.

The agent then read out a warning about cryptocurrency markets being a target for fraud and scams and about being weary of advertisements online and on social media promising high returns on cryptocurrency products. Typical features of investment scams were also covered – being asked to move money between bank accounts and then asked to open a cryptocurrency account and move money into it; being given promises of huge investment returns; the opportunity being too good to be true; being pressured to act quickly, etc. The agent offered to keep the transaction on hold to give Mr H further opportunity to carry out due diligence, including reviewing the website of a national fraud campaign. Mr H said he was happy for the payment to be processed instead and it was subsequently released.

I understand the point Mr H's representative is trying to make about Chase probing further during the intervention call. It's easier to be critical with the benefit of hindsight. But as the representative knows (or ought to know), causation is a critical determinative factor in every scam case. For me to uphold this complaint, it isn't enough to make a finding that Chase failed to sufficiently intervene during the calls; its acts or omissions must be the immediate and effective cause of losses that were reasonably foreseeable at the time of the breach.

I can't know for certain what would have happened if Chase had questioned Mr H further when it spoke to him. In such situations, I reach my conclusions not based on mere possibilities but rather on what I find most probable to have happened in the circumstances. In other words, I make my decision based on the balance of probabilities – so what I consider most likely to have happened considering the evidence and wider circumstances of the case.

The warning Chase provided included features that ought to have resonated with Mr H's circumstances – an online advertisement about an investment opportunity that came with a guarantee of making huge returns. I should also mention that Mr H told both Chase and our service that he had researched the scam firm before deciding to invest.

Having thought carefully about Mr H's answers to the questions he was asked, on balance, I'm not convinced that he would have mentioned a third party's involvement had Chase asked him about it.

Even if he had, Mr H had already said yes when during the intervention call Chase asked him if his due diligence into the investment opportunity included checking the FCA's Register. If he hadn't specifically checked the FCA's website (even though he told Chase otherwise), the importance of doing so had been brought to his attention. I think it's important to note that the bank isn't expected to play an amateur detective in such situations.

I've considered the terms and conditions of Mr H's Chase account which set out the circumstances in which it will refund customers if they've been tricked into sending money. But these only cover scenarios where money is sent to someone else, i.e., a third party. In

Mr H's case, his payments were made to a cryptocurrency wallet in his name. The money didn't directly go to the scammer from his Chase account. So, Mr H wouldn't be entitled to a refund under Chase's terms and conditions either.

Recovery wise, given Mr H had legitimately bought cryptocurrency before sending it on to wallets in control of the scammer, it's unlikely recovery would have been successful. So, I don't think Chase could or should have done more to attempt recovery.

In summary, I recognise that this will come as a considerable disappointment to Mr H and I'm sorry that he's lost a large sum of money to a cruel scam. But in the circumstances, I'm not persuaded that Chase can fairly or reasonably be held liable to reimburse him for his loss.

My final decision

For the reasons given, 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 H to accept or reject my decision before 31 March 2025.

Gagandeep Singh
Ombudsman