

## **The complaint**

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

Mrs B 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 several transactions which Mrs B made from her Chase account in March and April 2023. She's explained they were made in connection with two investment opportunities, both of 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 Mrs B throughout the scam until she discovered she'd been duped into sending money to them. Mrs B made deposits into her Chase account from accounts held with other payment service providers, before making payments to purchase cryptocurrency. The cryptocurrency was then sent on to wallets as instructed by the scammer. Taking into account one credit (or reversal of a payment), the loss being claimed is just under £27,000.

This decision solely relates to Mrs B's complaint about Chase's acts and omissions in relation to the scam. Mrs B has also complained about other payment service providers she made scam payments from. Those complaints will be dealt with separately. Where relevant, I've taken into account information available on those complaints.

## **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 agree with the conclusions reached by the investigator for these reasons:

- 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 Mrs B made the payments using her security credentials, 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 disputed transaction – £15 on 8 March – to be unusual such that I think Chase ought to have taken

additional steps before executing Mrs B's authorised instructions. However, in my view, the next transaction – £5,000 on 9 March to the same payee – should have prompted further enquiries. And I can see that it did since Chase contacted Mrs B to discuss the payment.

- I've listened to the call recording and Chase's agent started by asking Mrs B if she'd been asked to move money to a safe account or been told that her account was under attack. Mrs B answered no to both questions and said she was using her money to trade. When asked to elaborate on the payment purpose, she said, "*its for my crypto*". The agent then asked if she would be sending more payments to the beneficiary and Mrs B said not for the rest of that day. The agent then read out a warning about cryptocurrency markets being a target for fraud and scams and about being cautious before investing. Typical features of investment scams were covered – guarantee of high returns, opportunity being too good to be true, pressured to act quickly, etc.
- Mrs B was then asked to confirm if she was in control of her account and whether anyone else had access to it. She initially said yes to the latter question but changed her answer when the agent repeated the question. The agent recommended making a card payment where possible and offered to keep the transaction on hold to give Mrs B an opportunity to carry out due diligence, including reviewing the website of a national fraud campaign. Mrs B said she was happy for the payment to be processed instead and it was subsequently released.
- A similar intervention took place on three further occasions over the following week. The payee at these times was the same, although it wasn't the same payee as earlier transactions. Having listened to the calls, Mrs B's responses indicate that she was getting irate that Chase kept blocking her payments. She questioned why she was being asked about moving money from her account, saying it was her business not Chase's. In the last two intervention calls, Mrs B told Chase's agents the payments were for her clothes business. She said she was purchasing them to sell them on. And that the beneficiary was her business partner who she had known for a few years. Each time, Chase read out a warning and Mrs B told the agents she wanted the payment released.
- Having reviewed all the intervention calls, I agree with our investigator's findings that Chase didn't sufficiently probe into Mrs B's answers. In the first call, she had confirmed the transaction was to purchase cryptocurrency. While Chase warned her that cryptocurrency was a target for scams, it didn't question her what she intended to do with the cryptocurrency once she'd purchased it. For instance, it could have asked her how she got into trading, whether there was a broker involved in this instance, etc. I acknowledge that Chase asked Mrs B if anyone else had access to her account (cryptocurrency wallet), but that isn't the same thing. So, I think an opportunity to get a better understanding of what Mrs B was doing was missed.
- But that's not the end of the matter. As Mrs B's representative knows (or ought to know), causation is a critical determinative factor in every scam case. It isn't enough that Chase failed to sufficiently intervene; 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 Mrs B further when it first intervened. 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.

- Having carefully thought about this, I'm not persuaded that Mrs B would have been forthcoming about what was actually going on at the time. I accept that she acknowledged the payment was to buy cryptocurrency. But I'm not convinced that, if pressed about it, she would have told Chase a third party was involved. I say this because that is how she responded when another payment service provider asked her that question only a few days later when a transaction linked to the same scam triggered. Mrs B also misled that payment service provider when it asked if someone had asked her to install a remote access software. Also, it seems to me that the scammer instructed Mrs B to open an account with that payment service provider when Chase started blocking her transactions.
- I've also listened to call recordings between Mrs B and a third payment service provider – these also took place in the days following Chase's intervention. Although those transactions didn't go directly to the scammer – they were transfers between Mrs B's accounts with different payment service providers – it is clear that Mrs B was willing to mislead when questioned about the transactions. Despite what her representative states, the evidence strongly suggests that Mrs B was being coached by the scammer at the time. Although she acknowledged that enquiries were being made to protect her from falling victim to a scam, Mrs B didn't engage with the agents. She wanted the payments to go ahead even though certain scam scenarios she was told about fitted her situation. For instance, it was explained to her that scammers often spend days and weeks building trust. And that they tell victims to move money to different accounts to potentially invest in cryptocurrency.
- I'm also mindful that during the later interventions by Chase, Mrs B lied about the purpose of the payment. We know she wasn't sending money to a business partner. Chase couldn't reasonably have known that at the time though, given those transactions weren't identifiably cryptocurrency related. But even if Chase had somehow established that the cover story Mrs B had given didn't add up, I'm conscious several payment service providers were involved here. I'm not convinced that Chase's refusal to process the triggered transactions would have stopped Mrs B from continuing to make the scam related payments from one of her other accounts. In the circumstances of what happened here, I think it's unlikely that further questioning would have broken the spell Mrs B was under.
- I've also gone on to consider the terms and conditions of Mrs B'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 Mrs B's case, her payments were made to cryptocurrency wallets in her name. The money didn't directly go to the scammer from her Chase account. So, Mrs B wouldn't be entitled to a refund under Chase's terms and conditions either.
- Recovery wise, given Mrs B had legitimately bought cryptocurrency before sending it on to wallets in control of the scammer, it's unlikely recovery would have been successful. For completeness, Chase could have only attempted a recall from the payees Mrs B paid (the cryptocurrency exchange), not the scammer.

In summary, I recognise that this will come as a considerable disappointment to Mrs B and I'm sorry that she'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 her for her

losses. Any failure on Chase's part in relation to its intervention is not the dominant, effective cause of Mrs B's 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 Mrs B to accept or reject my decision before 22 August 2024.

Gagandeep Singh  
**Ombudsman**