DRN-4590007

The complaint

Mrs D 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 D is being represented by solicitors 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 totalling around £56,000 which Mrs D made from her Chase account between May and August 2023. These were made in connection with an investment opportunity offered by a company "O" who Mrs D came across on a social media platform in early 2023. Unfortunately, it turned out to be a scam.

Mrs D's representative has explained that the scammer encouraged Mrs D into making deposits throughout the scam (after seeing her profits rise) until she discovered she'd been duped into sending money to them. Mrs D made deposits into her Chase account from her account with another payment service provider, before making payments to purchase cryptocurrency. The cryptocurrency was then sent on to wallets as instructed by the scammer.

In their assessment, the investigator incorrectly stated that all but one of the disputed payments from Mrs D's Chase account were made using her debit card. They were in fact all faster payments made to the cryptocurrency exchange's account.

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 overall 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 D 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.

- Chase contacted Mrs D to discuss the first disputed transaction of £1,000. I've listened to the call recording, and Chase's agent asked Mrs D to confirm the purpose of the payment. She confirmed she was purchasing bitcoin. The agent then asked

her if she had been forced to make the payment or told that she needed to move money to a safe account or that her account was under attack. Mrs D answered no to questions and said she was using her money to trade. The agent also asked if she would be sending more payments to the beneficiary and Mrs D said she would in the near future.

- 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 D was then asked to confirm if she was in control of her account and whether anyone else had access to it. She confirmed only she had access to her cryptocurrency wallet. The agent offered to keep the transaction on hold to give Mrs D further opportunity to carry out due diligence, including reviewing the website of a national fraud campaign. Mrs D said she was happy for the payment to be processed instead and it was subsequently released.

- A similar intervention took place on 27 June, when Mrs D attempted to send £7,500 to the same payee. On that occasion, the agent also asked Mrs D how she came to know about the payee. She said it came up as being part of the cryptocurrency exchange that she was purchasing cryptocurrency from. Mrs D was given the option to carry out further checks but she told the agent she was happy to continue with the payment.

- I think that Chase could have probed Mrs D further in these calls. For instance, it could have asked her how she got into trading, whether she there was broker involved in this instance, etc. I acknowledge that Chase asked Mrs D if anyone else had access to her cryptocurrency wallet, but that isn't the same thing. So, I think an opportunity to get a better understanding of what Mrs D was doing was missed.

- But that's not the end of the matter. As Mrs D'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 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 Mrs D further when it spoke to her on those occasions. 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.

- Chase also discussed Mrs D's next payment with her – £5,000 to the same payee on 29 June – before releasing it. During this interaction, in addition to the questions previously asked, Chase's agent also asked Mrs D if she'd spoken to a trusted friend or family member or sought advice from someone other than the person she was dealing with. Mrs D's response was that she was doing this all on her own, indicating that there was no one else involved with the investment trading. The agent then asked Mrs D if she had checked the Financial Conduct Authority's Register to make sure she was dealing with an authorised company, and whether she had also checked its Warning List. Mrs D answered yes to both questions. She also confirmed that she had received returns and reassured Chase that this wasn't a scam.

- Having thought carefully about the third intervention call, I'm not convinced that Mrs D would have mentioned a third party's involvement had Chased asked her

about it during the earlier intervention calls. It's possible that she might have mentioned that her ultimate dealings were with O. But she'd already said yes when Chase asked her if her due diligence into the investment opportunity included checking the FCA's Register and its Warning List. I'm also mindful that when Mrs D set up the payee for the first time and confirmed that the payment was in relation to an investment, Chase displayed a scam warning. It said *"Do your research and consider getting independent advice… Scammers often post adverts online. They also create fake documents, companies and websites that may look genuine. You can use the FCA Warning List to check if a company is legitimate and to help you avoid scams."* We know that the FCA had published a warning in December 2022 which said O may be providing financial services or products without authorisation. The warning also said, *"You should avoid dealing with this firm and beware of potential scams."*

- Given my observations, I'm not persuaded that further questioning by Chase would have led to the scam being unravelled as Mrs D's representative has suggested. On balance, I think it's more likely that she would have answered in the same reassuring way, telling Chase that she had carried out her due diligence and checked the FCA Register and Warning List. I should also mention that Mrs D told both Chase and our service that she had researched O before deciding to invest. Even if she hadn't specifically checked the FCA's website (even though she told Chase otherwise), the importance of doing so had been brought to her attention. I think it's also important to note that the bank isn't expected to play an amateur detective in such situations.

- I've also gone on to consider the terms and conditions of Mrs D'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 D's case, her payments were made to a cryptocurrency wallet in her name. The money didn't directly go to the scammer from her Chase account. So, Mrs D wouldn't be entitled to a refund under Chase's terms and conditions either.

- Recovery wise, given Mrs D had legitimately bought cryptocurrency before sending it on to wallets in control of the scammer, it's unlikely recovery would have been successful. And I can see that is the response Chase received from the beneficiary account provider when it requested a recall after Mrs D reported the scam.

In summary, I recognise that this will come as a considerable disappointment to Mrs D 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

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 D to accept or reject my decision before 31 October 2024.

Gagandeep Singh
Ombudsman