DRN-5085964

The complaint

Ms D is unhappy J.P. Morgan Europe Limited (trading as Chase) won't refund the money she lost to a scam.

What happened

In 2022 Ms D fell victim to a cryptocurrency scam. She'd seen an advert for the investment online – and had recently seen information in the news about people successfully making money from cryptocurrency investments – so she submitted her details to show her interest. Ms D was contacted by a representative of an investment firm who said they could help her to trade – I'll call this investment firm X. X encouraged Ms D to open accounts with a cryptocurrency exchange and with X directly, they also encouraged Ms D to download some remote access software so they could help her. Unfortunately, and unknown to Ms D, X was not legitimate, she was being scammed.

Ms D made an initial investment in September 2022, and when she could see on X's platform that she was making profits, X encouraged her to invest more so she could maximise her profit. In November 2022, Ms D's account with X suddenly showed a significant loss, and she was told that her account manager had lost her money, a new account manager took over and encouraged her to invest more to recoup her losses. Ms D borrowed funds to enable her to do this. In April 2023, having seen a steady increase in her profits, Ms D asked to withdraw her money from the scheme. She was told she'd need to pay taxes to facilitate this, and made some final payments to the scheme in May 2023. When her withdrawal did not materialise, and she was then unable to contact X, Ms D realised she had been the victim of a scam.

Over the course of the scam Ms D made the following payments, from Chase, to an account she held with another bank (R), from where funds were moved on to her cryptocurrency account and then to the scammer:

01/09/22	£5,000
13/09/22	£13,500
11/10/22	£25,000
12/10/22	£1,500
12/10/22	£14,000
26/10/22	£10,000
15/11/22	£12,000
17/11/22	£500
24/11/22	£100
16/12/22	£500
18/12/22	£8,000

12/05/23	£11,999

Ms D raised a scam claim with Chase, but it rejected her claim. Chase says that as the payments were made to another account in Ms D's own name, it does not have liability for the loss.

One of our investigators looked into the complaint, they felt that Chase should have intervened at the time of the third payment, for £25,000 on 11 October 2022. They felt that Chase should have contacted Ms D directly to establish the circumstances surrounding this payment and that, had it done, it was more likely than not that the scam would have been uncovered and Ms D would not have gone on to make any further payments. However, they felt it would be fair for Ms D and R to also share responsibility for the loss. So, they recommended Chase refund 33% of Ms D's loss from the £25,000 payment onwards, plus interest.

Ms D accepted the investigator's recommendations, as did R. Chase didn't agree. It maintains that it should not share any liability for the loss as the payments were to an account in Ms D's own name, were not in quick succession, and were to a trusted payee.

As the case could not be resolved informally, it's been passed to me for a decision.

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 broadly for the same reasons.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Where the evidence is incomplete, inconclusive or contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. And I have taken that into account when looking into what is fair and reasonable in this case. But a bank also has to be on the lookout for, and help to prevent, payments that could involve fraud or be the result of a scam.

It is not in dispute that Ms D authorised the scam payments. It is also not in dispute that Ms D was duped by the scammer into instructing the bank to transfer money to her account with R and ultimately on from there to the scammer's account. The scammer deceived her into thinking she was making a legitimate cryptocurrency investment. So, although Ms D did not intend the money to go to the scammer, under the Payment Services Regulations 2017, she is presumed liable for the loss in the first instance.

I appreciate the loss did not occur directly from Ms D's Chase account. But, taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Chase should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.
- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

I don't consider that because Ms D's R account and various cryptocurrency exchanges were used as an intermediary between Chase and X means that these responsibilities don't apply.

Taking the above into consideration, I need to decide whether Chase acted fairly and reasonably in its dealings with Ms D, or whether it should have done more than it did.

The first two payments to the scam – which were made from Ms D's chase current account - were not so large that, in the context of Ms D's usual account usage, I think they should have given Chase any particular cause for concern. Particularly as they were going to an account in Ms D's own name, albeit one that had apparently only recently been added as a payee.

I do however think the third payment, for £25,000 made on 11 October 2023 from Ms D's Chase savings account, ought to have warranted an intervention from Nationwide. This was significantly higher than any previous payments made by Ms D, and would be considered a high payment even in isolation. And while it was to an account in Ms D's own name that recipient account was at an e-money institution, and was a relatively new payee. I think it's reasonable that, by the time of this payment, Chase would have been aware of the increasing incidence of e-money institutions being used in this kind of multi-stage scam. So, I'm satisfied that, bearing in mind all these factors, it would have been reasonable for Chase to intervene at this stage to reassure itself that Ms D was not at risk of financial harm.

And, bearing in mind the value of the payment, I consider that reasonable intervention here would have been direct contact with Ms D to establish the circumstances surrounding the payment. So, what I now need to decide, based on the available evidence, is what would most likely have happened, had Chase intervened in that way.

I would expect Chase to have asked Ms D questions such as who the payment was going to, what it was for, and for the basic surrounding context of the payment - it could, for example have, asked how she had found the investment opportunity, whether she'd parted with personal details in order to open a trading account, whether she was being helped by any third parties and had they used remote access software, whether the investment opportunity was linked to a prominent individual, advertised on social media etc. These are typical features of cryptocurrency scams.

I've not seen anything to suggest that Ms D was told to be dishonest about what she was doing, or given any cover story to tell to Chase. So, I think effective questioning would likely have quite quickly unearthed that something untoward may be going on. I think Chase could

have quickly learned from any conversation with Ms D the basic background to the payment instruction – that she was moving money to then invest in an opportunity which she'd decided to pursue after learning about it online, and that she had been guided by a third party using remote access software, all common hallmarks of investment scams.

Even though the conversation would have identified the payment was going to Ms D's own account with R (before being sent onto the scammers), the conversation shouldn't have stopped there on the basis that the money appeared to be going to somewhere safe and within Ms D's control. This is because by 2022 Chase was well aware – or ought to have been well aware – of how scams like this work – including that the customer often moves money onto an account in their own name before moving it on again to scammers.

So, in the round, I think Chase would have been concerned by what the conversation would most likely have revealed and so warned Ms D, explaining the typical characteristics of scams like this. Had it done so I think Ms D would have listened and recognised she was at risk. It follows I think Ms D would not have gone ahead with the £25,000 payment, nor any subsequent payments.

I'm therefore satisfied that Chase should bear some responsibility for the scam payments, and I'm aware that in Ms D's complaint against R we have also found that R should share some responsibility for that loss. I'm satisfied that is also reasonable. So, the remaining issue to consider is whether Ms D should share in the responsibility for her losses. I won't go into detail here as Ms D accepted the investigator's conclusions but for completeness I agree – broadly for the same reasons.

Ms D has said she carried out an online search to check that X was legitimate, but I cannot see that she would have found much at all at the time of the scam which could have convinced her this was a legitimate investment opportunity. And given the large amount that Ms D invested, and the potential large returns she had been told she could expect, I think it is reasonable to say she should have carried out further due diligence before making those payments.

I've also thought about whether Chase could have done more to recover Ms D's funds once it was made aware of the scam, but I'm satisfied that there was nothing more Chase could have done here.

With all this I mind, I think it's reasonable for Ms D, Chase, and R to share responsibility for Ms D's loss.

Putting things right

To resolve this complaint Chase should:

- Refund 33% of Ms D's loss from the £25,000 payment onwards (inclusive).
- pay interest on this amount calculated at 8% simple per year from the date the transactions were made to the date of settlement.

My final decision

I uphold this complaint in part. J.P. Morgan Europe Limited (trading as Chase) should now put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms D to accept or reject my decision before 6 January 2025.

Sophie Mitchell
Ombudsman