DRN-4806730

The complaint

Mrs P is unhappy J.P. Morgan Europe Limited ("Chase") won't refund the money she lost as a result of a third-party scam.

What happened

I'm not going to cover all the points raised in detail. The view of 14 December 2023 covered the details of Mrs P's testimony. But briefly in April 2023 Mrs P fell victim to a cryptocurrency scam. She was contacted by a third-party purporting to be a 'trader' - I will refer to as N. Between 3 May 2023 and 8 June 2023, Mrs P made the following transactions to genuine cryptocurrency providers (referred to as C and X).

Date	Payee	Debit	Credit
3/5/23	C	£5	
4/5/23	C	£5,000	
5/5/23	F		£4,872.52
9/5/23	X	£1,000	
9/5/23	X	£14,000	
10/5/23	F		£33
25/5/23	X	£7,000	
29/5/23	X	£7,000	
31/5/23	X	£7,000	
5/6/23	P		£782.94
8/6/23	X	£7,414	

Chase said it held all but the two smallest payments for further checks before processing them. It says it provided warnings when it spoke to Mrs P over the phone. It said, despite the warnings, Mrs P continued with the payments, so it isn't liable for her loss. Chase says it managed to return £5,688.46 of Mrs P's funds to her.

Our investigator upheld the complaint from the second transaction for £5,000 onwards. However, she felt it fair that Mrs P should share in the responsibility for her losses – so she recommended Chase refund 50% of the transactions from 4 May 2023 along with interest. Mrs P accepted the investigator's recommendations. Chase didn't agree. It didn't think it could have done more during the calls and considers even if it had done more - there was in sufficient evidence Mrs P would have been honest about the reasons for the payment.

I issued my provisional decision on 10 May 2024 explaining why I was reaching the same outcome as the investigator but my proposals for redress took into account the returns Mrs P had received as part of this scam.
Both parties accepted my provisional decision. Chase asked me to confirm whether its figures for redress were correct.

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.

Chase has asked me to confirm whether its refund calculations are correct. My decision sets out a formulaic calculation. The reason for this is because Chase holds all the relevant data (and interest is payable to the date of settlement which is unknown). That said it appears to have followed the formula I set out - except it hasn't added 8% simple interest to the amount it is proposing to refund - which it will need to do.

As neither party has provided any further evidence or arguments regarding the merits of this case for consideration, I see no reason to depart from the conclusions set out in my provisional decision. For completeness, I have set this out below.

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 Mrs P authorised the scam payments. It is also not in dispute that Mrs P was duped by the scammer into instructing the bank to transfer money to a cryptocurrency account and ultimately on from there into the scammer's account. The scammer deceived her into thinking she was making a legitimate cryptocurrency investment for further trading.

As I understand it, payments to the cryptocurrency provider were used to purchase genuine cryptocurrency which was then placed with a cryptocurrency exchange in a wallet in Mrs P's name and from there it was moved for further trading with N on a fake trading platform. So, although Mrs P did not intend the money to go to the scammer, under the Payment Services Regulations 2017, and the terms and conditions of her account, she is presumed liable for the loss in the first instance.

I appreciate the loss did not occur directly from Mrs P'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.

Should Chase have fairly and reasonably made further enquiries before it processed Mrs P's payments and would that have prevented the loss?

What can be considered unusual or uncharacteristic usually requires reference to common activity on an account, but the account had only been opened a few weeks before the transactions in question. That said, I think the first transaction was unremarkable, and I don't think that there was enough suspicion about the transaction that I would've expected Chase to intervene. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. It will be impossible to prevent all fraud without a significant number of genuine payments being delayed considerably and inconveniently. To the bank, they appeared genuinely authorised payments.

But by the second transaction, I think the bank ought to have been concerned. A new account had been opened a few weeks earlier with the purpose of 'everyday spending'. The payment for £5,000 to a known cryptocurrency provider was a payment instruction that Chase ought to have realised warranted additional checks before it simply processed it without question.

And Chase did in fact provide a warning as part of the online process. Mrs P selected 'Investments and cryptocurrencies' as the reason for the payment. The corresponding warning suggested to do research and to seek independent advice. It warned not to continue if someone has control of your account. And it directed the customer to the warnings section of the Financial Conduct Authority (FCA) website and instructed the consumer to check that the firm is genuine. Although the warning had some good aspects – it doesn't bring to life what cryptocurrency scams look like or highlight key features such as being contacted by fake trading companies and fake trading platforms.

But after Mrs P completed the online process - Chase was still sufficiently concerned that it stopped the payment and went on to speak with Mrs P over the telephone before processing it. Accordingly, it's just a question of whether it did enough.

It seems, as a financial services professional, Chase was aware at the time that fraudsters use genuine firms offering cryptocurrency as a way of defrauding customers and that these scams often involve money passing through more than one account. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022.

It may have appeared at face value to have been a legitimate payment to a legitimate organisation. But even though the money appeared to be going somewhere safe or on (as it did) to the consumer's own wallet, I don't think the conversation should have stopped there. Based on the industry warnings at the time, I think Chase ought to have had a good enough understanding of how these scams work – including that consumers often move money to buy genuine cryptocurrency before moving it on again to a fraudster.

Looking at the transcript for the call on 4 May 2023 and all the calls that followed, I do accept aspects of the calls are quite good. And Chase continued to intervene and ask questions on each occasion Mrs P made a significantly sized payment. Chase did ask Mrs P questions and it warned her that the crypto marketplace is a target for fraud and scams. It also asked if she'd done research and how she'd heard about the opportunity.

But I don't think the conversations went far enough. There were red flags that I think Chase could have picked up on and probed Mrs P further on - rather than limiting itself to a script. Of course, the questions regarding whether she was in control of her accounts or whether anyone had access to them wasn't the real issue here. Neither was the payment itself to the genuine cryptocurrency provider. In fact, Mrs P did ask the call handler "how can scammers use C (the genuine cryptocurrency)?"

So I think Chase could have explained how scammers use genuine cryptocurrency to make payments to what appears to be genuine trading platforms but are fake and that scam 'trading' firms can manipulate software to distort prices and returns and trick people into buying non-existent currency. I think this would likely have resonated with the exact situation Mrs P found herself in.

During the call on 31 May 2023 Mrs P mentions a "trading platform" and explains "every day I have to discuss what I'm going to buy". The call handler simply moves to the next question on the script without exploring what Mrs P is telling him/her. This was another opportunity to highlight a key feature of cryptocurrency scams – i.e. fake trading platforms.

During some of the calls Mrs P mentions her 'broker' – this being the real issue here. So I think Chase could have picked up on this information and asked open questions such as the name of the broker and where she'd heard about the opportunity. Some further digging might reasonably have revealed there was a warning on the FCA website about N published on 4 April 2023. I think this information would have been concerning.

During one call Mrs P did explain she'd seen the opportunity on the internet – but this isn't explored any further. With further questioning about how she'd come across the broker would likely have revealed that she'd seen an advert on a social media site endorsed by a celebrity. I think this would have given Chase cause for concern. I appreciate in the last call Chase did warn "be wary of adverts online' and "be suspicious if you are contacted out of the blue". But this was lost in part of a script which it seems Mrs P was becoming increasingly frustrated with.

I think Chase missed an opportunity much earlier on to engage with what Mrs P was telling it. In my view the signs were there, and it had the opportunity to fully expose the scam through better probing and by asking more open questions and highlighting some of the key features I've mentioned above.

I think this would have caused sufficient doubt in Mrs P's mind not to proceed with the payments. In other words, if Chase had carried out further or better questioning in line with the bank's duty of care, it seems probable that Mrs P would have become credulous about the scam in time and stopped the £5,000 payment (and any subsequent payments) in its tracks. The fraud would have failed; and Mrs P would not have lost the £5,000 or the transactions that followed.

Chase has suggested that there's no evidence that Mrs P would have been honest (and so I take it it means - better questioning wouldn't have made a difference). This is certainly not the sense I get from the transcripts of the calls. On the contrary, the overall sense is one of Mrs P describing events as she was led to believe they were at the time.

Should Mrs P share in the responsibility for her loss?

I've thought carefully about what Chase's obligations were, as set out above. But another key issue is whether Mrs P acted reasonably taking into account all the circumstances of the scam. So, I have also considered whether Mrs P should share in the responsibility for her losses. I won't go into detail here as Mrs P accepted the investigator's conclusions but for completeness I agree – broadly for the same reasons.

It seems N called Mrs P out of the blue (although I accept, she may have had some earlier contact with this or a similar organisation earlier that year).

Mrs P was encouraged to take out loans and some of the reasoning given (including an insurance policy for a risk-free investment) ought to have been a cause for concern. I note early on in the chat with the scammer – it seems a loan was cancelled because of concerns her husband had. So I think the deal warranted closer scrutiny.

And although I don't think the warnings Chase provided went far enough, the online warning did refer to the FCA warning list with a link. I think given the extent of Chase's ongoing concerns and some of the points it raised with Mrs P – ought reasonably to have led Mrs P to researching N more closely. Even a basic internet search of N brings up the FCA warning on N – which was posted before Mrs P transferred her money. This information was concerning and would likely have led to Mrs P discovering this was a scam.

On that basis, I think it's reasonable for Mrs P to share the responsibility with Chase and reduce the refund on the payments by 50%.

Putting things right

To put things right for Mrs P J.P. Morgan Europe Limited ("Chase") must

- Reimburse 50% of Mrs P's loss
- Mrs P's loss = transactions from 4 May 2023 to 8 June 2023 inclusive less the credits in the table above along with any funds Chase recovered (I understand this to be £5,688.46)
- As Mrs P has been deprived of the use of this money - pay interest on the net loss calculated at 8% simple per year from the date the transactions were made to the date of settlement.

If Chase considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Mrs P how much it has taken off. It should also give her a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

My final decision is that I uphold this complaint in part, and I require J.P. Morgan Europe Limited ("Chase") to put thing right for Mrs P as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs P to accept or reject my decision before 18 June 2024.

Kathryn Milne
Ombudsman