DRN-5341460

The complaint

Mr B complains that J.P. Morgan Europe Limited trading as Chase ('Chase') hasn't refunded the money he lost as the result of an authorised push payment ('APP') bank impersonation scam.

What happened

The circumstances of the complaint are well-known to both parties. So, I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

On 29 March 2024, Mr B sent a £25,000 faster payment from his Chase account to a third party. At the time, Mr B thought he was following the instructions of a Chase employee. However, unbeknownst to him at the time, Mr B was actually speaking to a scammer who was impersonating a Chase employee.

After realising he'd been the victim of an APP scam, Mr B reported the situation to Chase. Unfortunately, Chase couldn't recover all the money from the beneficiary bank, but £10,063.92 was recovered and returned to Mr B on 15 May 2024.

Chase considered whether it needed to reimburse Mr B's outstanding loss of £14,936.08 but decided it didn't need to. Chase argued that Mr B had spoken to Chase, prior to the scam payment being released but hadn't given accurate answers, which prevented Chase from identifying the scam. It considered Mr B was responsible for his outstanding loss and not Chase.

Unhappy with Chase's response, Mr B referred a complaint to this service. Our Investigator considered the complaint and upheld it. In summary they said Mr B's outstanding loss ought to have been refunded in full under the terms and conditions of his Chase account. They also considered interest should be added at 8% simple per annum on that amount, from the date of the scam payment until the date of settlement.

Mr B accepted our Investigator's opinion, but Chase didn't. Chase agreed it could've done more to stop the scam but thought Mr B had been given appropriate warnings (both verbally and in writing) about bank impersonation scams prior to the payment being released. Chase also reiterated that Mr B had given inaccurate answers when Chase questioned him about the scam payment. Chase offered to reimburse 50% of the scam payment, plus interest.

Mr B declined Chase's offer and so, as an informal agreement couldn't be reached, the complaint has been passed to me to decide.

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.

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

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account.

It's not in dispute that Mr B made the scam payment. So, the payment was authorised and under the Payment Services Regulations, the starting position here is that Mr B is responsible for the payment (and the subsequent loss) despite the payment being made as the result of a scam.

However, that isn't the end of the story. The terms and conditions of Mr B's account with Chase (at the time the scam payment was made) say that where a payment is made as a result of an APP scam, Chase will refund the payment *unless* the customer should've known they were being tricked by a fraudster. There's been no suggestion made that Mr B wasn't the victim of an APP scam. So, I've gone on to consider if Chase could fairly refuse to refund Mr B because he ought to have known that he was falling victim to an APP scam.

Prior to making the scam payment from Chase, Mr B had received a phone call from someone impersonating another of his banking providers, which I'll refer to as 'A'. During that call, Mr B was told that there was suspicious activity on his credit card with A. He was advised that his phone might have been hacked through logging on to a publicly available WIFI connection. Mr B had recently been abroad and accessed WIFI at the airport and so Mr B thought it was plausible that his phone had been compromised.

Mr B gave details of some of his other accounts (including his Chase account) so the caller could investigate if those accounts were compromised and if so, take action to protect them. The caller advised Mr B that he may receive calls from his other banking providers and he was provided with a security code which the callers would quote to confirm the call was legitimate.

Mr B then received a call from someone impersonating another of his banking providers, which I'll refer to as 'B'. The caller quoted the security code, which reassured Mr B that the call was genuine. The caller said suspicious activity had been detected on his account with B. Mr B was told that his debit card would be cancelled and a new one would be issued to prevent further fraudulent activity on his account.

Shortly afterwards, Mr B received a call from someone impersonating Chase. Again, the caller gave Mr B the security code. The caller explained that someone had tried to make a £19,000 transaction using Mr B's Chase account. Mr B was driving at the time of the call and the signal repeatedly cut out, resulting in the call being terminated. However, when Mr B arrived home, the person impersonating Chase called him again, this time on his landline. The caller said they had managed to stop the unauthorised transaction for £19,000 but they said further action was needed to protect Mr B's funds.

Mr B was told Chase's fraud team, based in America, were suspected of being involved in fraudulent activity. To stop his funds being stolen, Mr B was told he needed to create a new "*encrypted*" account with Chase, which members of Chase's fraud team wouldn't be able to access. The caller guided Mr B through the application process and was able to confirm what questions Mr B would be asked and at what stage of the application. Mr B says this knowledge of Chase's application process helped reassure him that he was speaking to a genuine employee of Chase.

Once the new account had been opened, Mr B was told to move his funds to a "*system generated account name"* with B. Mr B understood that B would then forward the funds to his newly opened account with Chase and by doing so, this would prevent any fraudsters from being able to trace where his funds had gone and stop them from being stolen.

Mr B was reminded that Chase's fraud team were suspected of behaving fraudulently. So, Mr B was told to say, if questioned, that he was paying a builder for home improvements and not to disclose his conversation about the alleged fraudulent activity on his Chase account. Believing the caller to be a genuine Chase employee who had Mr B's best interests in mind, Mr B followed the advice on the understanding that he was protecting his money.

In these circumstances, I'm persuaded this was a sophisticated and well planned out scam. Mr B was in a state of shock and panic created by the scammers and the scammers carefully established plausibility over several phone calls. They also established an element of fear and distrust of Chase's genuine fraud department, to the extent that Mr B thought any intervention could be from someone attempting to defraud him. Mr B also recalls the scammers he spoke to were professional, calm and reassuring, taking time to build Mr B's trust. As a result, I'm not satisfied that Mr B ought to have known he was being scammed at the time he initiated the £25,000 payment.

I appreciate that after setting up the payment, it was stopped by Chase and held for a fraud check. Mr B was initially provided with a written warning about bank impersonation scams. Some of the information in the warning was relevant (i.e., he'd been called by someone claiming to be from Chase) but other information wasn't relevant (i.e., he wasn't using remote screen share software). Also, the warning didn't go into detail about how bank impersonation scams work in practice and so I don't think that warning reasonably ought to have prompted Mr B into realising he was being scammed.

Mr B then spoke to a Chase advisor verbally and was asked some questions about the payment. Mr B did give inaccurate answers to Chase during that call, as instructed by the scammer (whom he thought was a Chase employee). Chase gave some bank impersonation scam education to Mr B. Some of that education was relevant (i.e., the scammer had told Mr B not to be truthful with Chase) but again Chase linked these types of scams very strongly to the use of remote access software, which wasn't relevant in Mr B's circumstances, so I can understand why this didn't resonate with Mr B at the time.

Mr B told the advisor that none of the bank impersonation scam red flags applied in his circumstances and that he was paying a local builder for home improvements. At this point, Chase's questions shifted to scams involving rogue traders and invoice interception scams. So, the remaining questions and education weren't relevant to Mr B's circumstances.

Overall, I'm not satisfied that Mr B ought to have known that he was falling victim to an APP scam at the time of the payment, despite the written and verbal warnings Chase gave him about bank impersonation scams. As a result, I think Chase reasonably ought to have refunded him under the terms and conditions of the account and Chase should now reimburse Mr B's outstanding loss.

Our Investigator thought Chase could've done more when it spoke to Mr B about the scam payment and that if it had, the scam could've been prevented. As a result, our Investigator said Chase should pay interest on the refund she'd recommended, from the date of payment until the date of settlement. In its response, Chase agreed the intervention could've been better and as part of its offer to reimburse 50% of Mr B's loss, it agreed to pay interest as recommended by our Investigator. As there appears to be an agreement between the parties that interest should run from the date of payment, I see no reason to depart from our Investigator's findings on that point.

I appreciate Mr B feels Chase could've acted with more urgency once he reported the scam. Chase hasn't provided evidence of the time it contacted the beneficiary bank. So, I can't be certain there hasn't been a failing by Chase in not reporting the scam as quickly as it reasonably should've done. However, as I think Chase ought to reimburse the outstanding loss and pay interest on the refund from the date of the payment, any potential failings won't have been to Mr B's detriment and so I don't think Chase needs to do anything further in response to this complaint point.

Putting things right

To resolve the complaint, Chase should:

- refund Mr B's outstanding loss of £14,936.08; and
- pay interest on the refund, at 8% simple per annum, from the date of the payment until the date of settlement.

My final decision

For the reasons explained above, my final decision is that I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 17 December 2025.

Liam Davies
Ombudsman