

Mr D and Ms J are seeking to recover £8,000 from TSB Bank plc ("TSB"), which was stolen from their account as a result of a third-party scam.

TSB says it is not liable for the loss because Mr D unwittingly authorised the payment — and it could not reasonably have intervened or done more than it did to try to recoup the money from the receiving bank.

my findings

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 have concluded that the complaint should be upheld for the following reasons:

It is not disputed that Mr D authorised the scam payment of £8,000. He was in the process of paying a deposit for some building work that was due to start on his home. On 16 April 2018, following a request for his builder to confirm his account details, Mr D received an email which provided what looked like the account details he'd asked for. The email appeared in a chain of others that Mr D had been responding to and appeared to come from the building firm he had been in contact with.

On the same day, Mr D transferred the money as per the instructions he was sent. He did so via his online banking where he firstly transferred the funds from his savings account to his current account. He then set up a new payee using the details he'd been provided with in the email and transferred the money out of his account.

When Mr D spoke with his builder a few days later, he was asked again to transfer the initial payment so the work could start. Mr D was surprised by this, he thought he'd already transferred the payment. He told his builder he'd already done so and showed him the emails they'd shared. It then came to light that the building firm had not sent the latest emails containing the account details – they were different to the original account details included in the builder's payment proposal that had been sent much earlier. And the £8,000 deposit payment had not been paid into their account.

Mr D had fallen victim to a sophisticated scam - the email Mr D received was from a fraudster who had managed to send a fake email to Mr D – which appeared to be just like genuine ones sent by his builder and which appeared to come from the same email address.

I accept that this was an 'authorised payment' even though Mr D was the victim of a sophisticated scam. He used his security credentials to request the payment online. So, although he did not intend the money to go to the scammers, under the Payment Services Regulations 2017, and the terms and conditions of his account, Mr D and Ms J are presumed liable for the loss in the first instance.

However, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider TSB 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 make 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.
- For branch transactions, those steps may include following the Banking Protocol where appropriate.

TSB initially declined to refund Mr D the £8,000 as it didn't believe it had done anything wrong in carrying out Mr D's instructions to make the payment. It said there was nothing about the payment itself that should've put TSB on notice that Mr D and Ms J might've been at risk of financial harm.

TSB said it isn't unusual for its customers to transfer money from their savings (or other accounts) in order to then pay for a large purchase. And in this case, Mr D had a specific account that he'd been using to save for the proposed building work. It also said that Mr D held a number of accounts with TSB, some of which he'd previously used to make similar high value transactions. So, transferring large amounts wouldn't have stood out as unusual for Mr D - if all of his account activity was taken into consideration.

TSB went on to say that even if the transfer had triggered its fraud monitoring systems and prompted a discussion with Mr D, the scam still wouldn't have been uncovered. Mr D would simply have explained what the payment was for and confirmed it was genuine. TSB wouldn't have known Mr D's builders account details had been changed. And so, TSB could not have prevented the scam. But I don't agree with TSB and I'd like to explain why.

I'm satisfied a payment of £8,000 was unusual for Mr D and uncharacteristic for this particular account - there had been no comparable legitimate payments in recent times. The largest transaction that left this account in the months leading up to the scam, appears to be a monthly mortgage payment which equates to c£2,000, a quarter of the value of the payment now in question. I also don't think it would be reasonable to compare the activity on this account to the activity on Mr D's other accounts. This is the account in question. And even if I were to do so, there doesn't appear to be any comparable legitimate payments from these accounts either - the payment here is twice the value of any payment that left his other accounts too. It's also been made to a new payee. And so I'm satisfied TSB ought fairly and reasonably, and as a matter of good practice, to have done more here - I think it ought to have made enquiries about the purpose of and the circumstances leading up to the payment before it processed it.

TSB has commented that it had an obligation to debit its customer's accounts in line with its customers mandate and by allowing the payment to leave the account here, it was simply following Mr D's payment instruction. I accept there is a balance to be struck between identifying potentially fraudulent payments and minimising disruption to legitimate

payments. But I'm satisfied that if TSB had contacted Mr D in this particular case, the scam would have been revealed and prevented. I'll explain.

Mr D fell victim to a scam which is sadly all too common – "invoice intercept". And it's a type of scam I'm satisfied TSB ought to have been aware of at the time. And I agree with TSB that had it contacted Mr D, he would most likely have told TSB he was intending to pay for some building work he was having completed on his home. But, at this point, being aware of the prevalence of this type of scam and its common characteristics, TSB would've had the opportunity to question him further.

A particularly common feature of this type of scam, is that a customer will receive an email that appears to be from the genuine business they are in contact with. This email will contain either updated payment details or the payment details previously provided will have been subtly changed - unbeknown to the customer, in order to redirect the payment to a fraudulent account.

This is a common scam with very particular characteristics, and I'm satisfied TSB ought fairly and reasonably to have asked Mr D how the payment details had been communicated to him. Mr D would've told the bank they'd been sent to him by his builder, by email. And TSB could've questioned if the account details he'd been provided with were different to those he'd received in the past.

TSB could then have educated Mr D about this type of scam and its key characteristics. Crucially, TSB could have asked him to check before continuing with the transfer - it could've advised Mr D to contact his builder using an established contact number to confirm the account details were correct. Had TSB done so, I'm persuaded that this would likely have produced some doubt in Mr D's mind that the payment details may not be legitimate, and he would've contacted his builder before proceeding with the payment. After all, this was a significant amount of money and Mr D may not have been aware previously that this type of scam was even possible. I'm persuaded that once informed of this, he would have taken some steps to verify the account details provided to him – had Mr D done so, I'm persuaded that the scam would have been prevented and no loss occurred.

In summary, I'm persuaded TSB ought fairly and reasonably to have encouraged Mr D to confirm the account details he'd been sent. His circumstances had all of the hallmarks of a well-known scam. And TSB should have explained the risks of scams involving the interception, altering and hacking of emails which would have prompted further action from him. In other words, if TSB had carried out further or better questioning in line with a bank's duty of care, it seems probable that Mr D would have contacted his builder just to make sure everything was as it should be. At this point, the scam would have come to light. The fraud would have failed; and Mr D and Ms J would not have lost £8,000.

However, by the time the scam came to light, there was only £224.65 left in the beneficiary account – which the receiving bank said it would refund to Mr D and Ms J if TSB raised an indemnity on their behalf. Given that the majority of the funds had already been removed by the time TSB were made aware of the scam, TSB could not recover any more of Mr D and Ms J's funds than those that remained.

In light of my conclusions above, it is not necessary in this case to consider whether the bank also exercised enough care and urgency in trying to recover the stolen funds from the payee bank before they were irretrievably removed by the scammers. But for completeness, I will say that, it would have made no difference because the recipient

banks records show that the scammers withdrew nearly all the money before Mr D had notified TSB of his concerns.

I have also considered whether Mr D should bear some responsibility for his loss. However, it is clear that up to and including the time of authorising the payment, he was still totally in the dark and simply did not appreciate what he was doing – he thought he was making a legitimate payment to a business he had been in regular contact with. I am satisfied there was no contributory negligence on this occasion, Mr D was the unwitting and blameless victim of a clever fraudster. The bank was the professional in financial matters; Mr D was a layperson.

In the circumstances I am satisfied TSB should fairly and reasonably reimburse Mr D and Ms J for the loss suffered without any reduction, together with interest to compensate them for being deprived of the money they lost.

It is not clear if the £224.65 that remained in the receiving account has already been returned to Mr D and Ms J or not. And so TSB will need to take this into account when calculating its offer. I am satisfied that had the fraudster not taken the money from Mr D and Mrs J, they would've used it for its intended purpose, to pay their builder, and so interest should be calculated at a rate of 8% simple per annum.

my final decision

I uphold this complaint against TSB Bank plc and direct it to:

- refund Mr D and Ms J the £8,000 lost as part of the scam – minus the remaining £224.65 if this has already been returned; *and*
- pay interest at a rate of 8% simple per annum from the date the payment left the account to the date of settlement*;

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D and Ms J to accept or reject my decision before 5 February 2021.

Emly Hanley
ombudsman

* TSB may be required by Her Majesty's Revenue & Customs to deduct tax from the interest. If it does, and if Mr D and Ms J request it, TSB should provide them with a certificate showing how much tax has been taken off, so they may reclaim it if appropriate.