DRN-4045216

The complaint

T, a limited company, has complained Starling Bank Limited won't refund money they lost from their account as the result of a scam.

T are represented in their complaint by Mr W.

What happened

Mr W holds both a personal and business account (in the name of T) with Starling. The personal account is the subject of a separate complaint.

In 2022 Mr W received a call from someone stating they were from his bank, Starling. He was told a payment he'd made thinking it was genuine had been increased by fraudsters and that his phone had been compromised by spyware.

Mr W was immediately reassured that the call came from his actual bank as the person he was talking too seemed calm and thorough. At the same time he was extremely concerned about losing any money from his account. He was told he'd need to take action to ensure his money was kept safe. Mr W was working outside (as T) and was distracted by the noise and the stress of what was happening.

Mr W then followed the instructions he was given to authorise four transactions. At the same time Mr W was being told who was actually trying to compromise him – a cryptocurrency company (who I'll call B). He understood that the payments to B would enable Starling to trace the payments and provide evidence against B, who Mr W believed were the scammers.

After Mr W was unable to get Starling back on the call using the number that had called him, Mr W realised something was wrong. He got in touch with Starling and asked them to refund T's account. They told him they wouldn't do so as they'd authorised the payments, not exercised sufficient caution and these payments weren't subject to the Contingent Reimbursement Model code for authorised push payments.

Mr W brought T's complaint to the ombudsman service.

Our investigator noted Starling had provided no warnings to Mr W despite these transactions being of a high value and out of character for T's account use.

She asked Starling to refund the payment made from T's account, along with 8% simple interest for the time period T was without his money.

Starling disagreed with this outcome. They felt Mr W should be at least partially liable for the transaction as he'd not sufficiently challenged the person on the phone. They've asked an ombudsman to review the complaint.

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 outcome as our investigator. I'll explain why.

There's no dispute that T (well, Mr W) made and authorised the payment. Mr W knew the reasons why he was being asked to make the card payments. At the stages he was making the payment, he believed he was taking urgent action to keep T's money safe and assist Starling. He believed once this had been done, he'd be able to get T's money back as he'd been reassured there was a bank insurance scheme to protect his money.

I don't dispute T was scammed but under the Payment Services Regulations 2017, I'm satisfied the transaction was authorised.

It's also accepted that Starling has an obligation to follow T's instructions. So in the first instance T is presumed liable for their loss. But that's not the end of the story.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider that Starling should:

- have been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.

- 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 (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which financial institutions 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 its customers from the possibility of financial harm.

Mr W fell victim to a sophisticated scam. Unfortunately safe account scams – which is what this was – are not massively unusual. Mr W realises how this happened as he responded to a fake message supposedly from the NHS. This allowed fraudsters to know Mr W had accounts with Starling and meant they could tailor their approach to him and make it believable.

I know Starling have said they'd have expected Mr W to undertake some checks to ensure who was calling him was genuine. I disagree. I don't think this takes into account the stress that can be caused by these types of calls, and the panic they're meant to engender in the people who receive them. Particularly when I take into account Mr W's personal circumstances.

The fraudster was also able to explain in detail how Mr W should make the payment and direct him to the relevant aspects within Starling's app which helped to gain his trust.

Starling has confirmed they do have mechanisms in place to check unusual transactions, but Mr W wasn't doing anything sufficiently unusual to trigger any warnings.

However I find this surprising. Mr W by making a transfer from T's account to his personal account, then a further payment from T's account emptied this account. T's account held a substantial balance before the scam. This should have been sufficient for Starling to have

taken action as these activities strike me as unusual.

I have taken into account that Mr W was presented with a warning stating that Starling would never contact him and ask him to use the specific screens. However by this time Mr W was convinced he was talking to his genuine bank so didn't see anything wrong in doing what he did.

There's no record of any similar card payments on T's account within the preceding six months. Any larger value payments from that account were set up as regular online transactions. I don't believe any argument that this reflects T's normal payment behaviour would stack up.

For these reasons I believe Starling should have undertaken additional steps to intervene at the time the payment of £4,900 was successfully authorised. Financial institutions are able to block card payments, and this is the step I'd have expected Starling to have taken here. This would have brought what was happening to an end as I'm sure if T's card had been blocked, the fraudsters would have come off of the phone immediately.

As I say, safe account scams are not unusual. All banks are aware of how these operate. The use of a card to send payments to a money transfer service or as here, a cryptocurrency company, is particularly prevalent. This limits banks' ability to send messages which can be done when customers are making online transactions.

Putting things right

As I believe any intervention Starling should have made would have changed what happened here, I am going to ask them to refund the disputed payment Mr W made from T's account. They will also need to add 8% simple interest to that amount. The money Mr W transferred from T's account to his personal account is covered by the resolution to the other complaint in Mr W's name.

This has had a massive impact on Mr W, shattering his confidence and impacting his ability over the last year to participate in important family events. I'm really sorry that this is so. Unfortunately this complaint is set up in the name of T and there is no provision to provide additional compensation to business entities for distress.

My final decision

For the reasons given, my final decision is to instruct Starling Bank Limited to:

- Refund £4,900 to T;
- Add 8% simple interest from 18 February 2022 to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 2 October 2023.

Sandra Quinn
Ombudsman