

## **The complaint**

P complains that State Bank Of India (UK) Limited (SBI) is refusing to refund the amount it lost as the result of a scam.

P is being represented by a third party. To keep things simple, I will refer to P throughout my decision.

## **What happened**

P was established as a property investment business with the aim of generating an additional income for its owner.

After researching for some time P decided on an investment property and instructed a mortgage broker. In turn the mortgage broker instructed a solicitor firm (A) to process the purchase of the property.

P was appointed a point of contact at A and due to other commitments communication between the two was mostly via email. The email address for A appeared legitimate and P dealt with multiple people at A making it feel safe it was dealing with a real business.

On 12 January 2023 P received an email that appeared to be from their contact at A. The email instructed P to pay a deposit for the property on 13 January 2023. This payment had been discussed previously with A, so the email and request did not come as a surprise to P. P responded asking for a breakdown of the payment and A provided this. The information provided to P was in line with what it was expecting.

Having spoken to SBI over the phone P had become aware that online payments were limited to £25,000 per day and it was agreed that P would attend the local branch to process the payment.

On attending the branch P was taken to a private room where they were required to fill in a form providing information about the payment. When SBI asked P if they knew the person that had provided the payee's bank details, they explained the details had been provided by A. Following this meeting SBI processed a payment of £88,949.88 as instructed by P.

Unfortunately, the email P received in relation to making the deposit payment and the account details had been sent by a scammer posing as A. The payment had therefore been made into the scammer's account.

P explained the situation to SBI, but SBI refused to refund the amount that had been lost.

Our Investigator considered P's complaint and thought it should be upheld in part. SBI disagreed, so this 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.

It has not been disputed that P has fallen victim to a cruel scam. The evidence provided by both P and SBI sets out what happened. What is in dispute is whether SBI should refund the money P lost due to the scam.

I have considered whether the payment in question should be refunded to P under the Contingent Reimbursement Model (CRM) code. The CRM code was setup to give added protection from authorised push payment scams, however the CRM code has been set up on a voluntary basis and as SBI has not subscribed to it I am satisfied it wouldn't apply in this scenario.

*Should SBI have reasonably prevented the payment P made?*

It has been accepted that P authorised the payments that were made from its account with SBI, albeit on the scammer's instruction. So, the starting point here is that P is responsible.

However, banks and other Payment Services Providers (PSPs) do have a duty to protect against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering.

The question here is whether SBI should have been aware of the scam and stepped into question P in more detail about the payment that was being made. And if it had questioned P, would it have been able to prevent the scam taking place.

Among other things SBI has told us that P had asked it about buy to let mortgages years before this payment was made. It considers P to be experienced in this type of transaction and that the details of the receiving bank were provided to P with enough time for P to check the details were legitimate before processing the payment.

SBI has also told us that P was likely to have seen a cybercrime warning when downloading an app used by A and I can see that again on emails that were received from A that there was a warning in the footer of the email. The warning was about "cybercrime" and explained its customers should call it immediately to verify information before sending funds, all transfer instructions should be verified by phone directly with its office, and that bank details would not be sent by email.

I haven't seen enough to suggest that P had lots of experience in this type of transaction but accept this may not have been the only time P had made a payment in relation to a property purchase. In any event, P had been in communication with A via email on a regular basis before the payment was made and the warning in the footer of the emails was not specific to P, but instead put on what appears to be the bottom of every email sent from A after its sign off. Therefore, I don't think this would have been an effective warning when it came to P accepting the payment instruction via the method of email. As neither of the warnings SBI has pointed to appear to have been prominent when the instructions were received by P, I don't think it would be fair for me to say SBI did not have some responsibility for the payment when it was processed.

SBI has accepted that the reason for the payment was clear that it was for mortgage purposes, and I can see from the evidence provided, that it did require P to complete a form before the payment was made. The form shows that P was happy with the payment that was being made. However, like our Investigator has already said I don't think SBI went far enough.

Considering the size of the payment that was being made and SBI's advanced knowledge of

this type of crime I would have expected it to at least have asked P some basic questions about the payment and how the payment details were sent to P.

If SBI had intervened as I think it should have, I think it would likely have found that P had received the payment instruction and account details via email and have seen that the payment being requested wasn't being made to A as would be expected, but instead to a completely different business name "*Oppizle construction Ltd*".

I think this information would have caused SBI concerns, and it would likely have warned P about potential fraud, prompting P to at least check with A via telephone before proceeding. I think this would have uncovered the scam and prevented the loss. So, SBI is responsible for P's loss.

*Did P contribute to the loss?*

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances, I do think it would be fair to reduce compensation on the basis that P should share blame for what happened. P did have the payment details provided by the scammer before making the payment and even asked for a breakdown of what the payment covered. Yet the payment request was in the name of another beneficiary. I think this should have caused P concerns, and this should have prompted them to call A and question this. Had P contacted A by telephone to confirm the bank details were correct the scam would also have been uncovered preventing the loss.

### **Putting things right**

To put things right I require State Bank Of India (UK) Limited to refund P the amount lost as a result of the scam less 50%. State Bank Of India (UK) Limited should add 8% simple interest per year to the amount it pays P from the date of loss to the date it makes the payment (less any lawfully deductible tax).

### **My final decision**

I uphold this complaint and require State Bank Of India (UK) Limited to put things right by doing what I've outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask P to accept or reject my decision before 19 April 2024.

Terry Woodham  
**Ombudsman**