

## **The complaint**

Mr C complains that HSBC UK Bank Plc won't reimburse funds he lost as a result of being a victim of fraud.

## **What happened**

As the circumstances of this complaint are well known to both parties, I have summarised them briefly below.

Mr C contacted an individual on a social media platform as they were advertising the sale of a digger that he was interested in purchasing. Both parties agreed a price of £4,000 for the digger, and £350 for its delivery.

The seller provided their HSBC bank account details to Mr C, and he carried out the payment of £4,350 from his account—held with a third-party bank—on 31 May 2023.

The delivery date for the digger passed and so Mr C attempted to contact the seller in order to find out where his item was: on several occasions. No response was ever given to Mr C, and it was at this point he realised he'd been the victim of fraud.

Mr C complained to the third-party bank from which he transferred the funds and was reimbursed £2,175 (50%) of the funds lost.

He also made a complaint to HSBC, the bank that received his funds, as he felt it should reimburse him the remaining loss. But HSBC looked into Mr C's complaint and concluded it had made no error. It therefore decided to offer no reimbursement.

Mr C remained unhappy with HSBC's response, so he brought it to our service for an independent review. An Investigator considered the evidence provided by both parties but concluded HSBC hadn't made an error in the circumstances of this complaint. In summary, they said that:

- HSBC had opened the account in line with its internal compliance procedures and completed relevant due diligence checks.
- He found no suspicious or unusual activity on the account that should have warranted earlier intervention on the account by HSBC.
- HSBC took the appropriate steps once it had been notified of the fraud, and was unable to prevent Mr C's loss as the funds had been removed prior to this point.

Mr C didn't agree with the Investigator's view. He felt that HSBC were still responsible for allowing the perpetrator to open the account and use it to commit crime.

As Mr C didn't agree with the Investigator's assessment, the matter has now been passed to me for a final decision.

## **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.

Regulated firms, such as HSBC, are required to conduct their business with due skill, care and diligence (FCA Principle for Businesses 2) and to comply with legal and regulatory requirements.

Those requirements include maintaining proportionate and risk sensitive policies and procedures to identify, assess and manage money laundering risks – for example through customer due diligence measures and ongoing monitoring of the business relationship, such as scrutinising transactions.

And given the increase in sophisticated fraud in recent years, as a matter of good industry practice at the time I think firms should reasonably have had measures in place to detect suspicious transactions or activities that might indicate fraud or financial abuse (something also recognised by the Banking Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice').

I'm satisfied that this good practice requirement meant not just looking out for situations where a customer might be the victim of fraud, but also situations where the customer might be the perpetrator of fraud or money laundering.

HSBC is also a voluntary signatory to the Contingent Reimbursement Model (the CRM Code). Under the Code, beneficiary banks must consider their obligations when certain authorised push payments (APP) are made to it. Those considerations are as follows:

### *"CRM Code: Payment Journey – Receiving Firm*

*SF2 - Receiving Firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams. This should include procedures to prevent, detect and respond to the receipt of funds from APP scams. Where the receiving Firm identifies funds where there are concerns that they may be the proceeds of an APP scam, it should freeze the funds and respond in a timely manner.*

#### *Prevention*

*SF2(1) - Firms must take reasonable steps to prevent accounts being opened for criminal purposes.*

#### *Detection*

*SF2(3) - Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds.*

#### *Response*

*SF2(4) - Following notification of concerns about an account or funds at a receiving Firm, the receiving Firm should respond in accordance with the procedures set out in the Best Practice Standards."*

Having taken into account all the above considerations against the evidence and testimony provided by both parties, I have concluded the following:

## **Account set-up**

HSBC has provided our service with all the information it relied upon when setting up the beneficiary account. As this contains third-party information, I'm unable to disclose specific details about the account to Mr C. I can however assure him that I've considered all the evidence carefully and am satisfied HSBC carried out sufficient checks to verify the identity of the applicant prior to agreeing to open the account.

I see nothing within the application itself, or the supporting documentation, that ought to have caused HSBC concern about the applicant. I therefore find that all necessary steps were taken by HSBC at the account opening stage.

### **Account activity**

I've also considered if the beneficiary account ought to have caused HSBC concerns from its operation. But having looked at the transactions carried out up to the point Mr C's payment entered the account, I'm satisfied there was no activity that would have stood out as suspicious or concerning in nature, to the extent HSBC ought to have intervened.

I can also see that prior to Mr C raising concerns with his bank—and that information being passed to HSBC—there were no fraud reports made to HSBC about the beneficiary account. So, I don't find that HSBC were put on notice about the account holder's conduct until this report.

Overall, I'm satisfied HSBC didn't miss an opportunity to detect any fraudulent activity sooner.

### **Recovery**

HSBC was notified by Mr C's bank of the fraud on 8 June 2023. I can see HSBC took immediate action on the beneficiaries' account. Unfortunately, by the time HSBC had been notified, none of Mr C's funds remained in the account. So, it had no way of recovering or returning them to Mr C.

Mr C has made comment post view that HSBC should claim the loss from their insurance and pay him back. I am unsure as to what insurance Mr C is referring to, but it's my role to assess whether HSBC has breached any of the considerations I've given above. And as is evident in my assessment, I find that it has not. As such. It would be unreasonable to direct HSBC to reimburse Mr C any of his loss.

I realise this will come as a disappointment to Mr C, and I am sorry he's been the victim of a callous crime. But I can only hold HSBC responsible for his loss where it has made an error. And in this case, I don't find it has.

### **My final decision**

For the reasons I've given above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 11 June 2024.

Stephen Westlake  
**Ombudsman**