DRN-4452051

The complaint

A company which I will refer to as 'H' complains that HSBC UK Bank Plc wouldn't reimburse the money which they lost due to an authorised push payment scam. They say that HSBC allowed a fraudster to open an account with it and then use the account for fraudulent purposes.

What happened

The background to the complaint is known to both parties and so I won't repeat it at length here.

Briefly, in early 2020, unknown to H, a fraudster intercepted an email exchange between H and their supplier. They responded, as if from the supplier, to a previous query from H and then advised H that they had changed their bank account details.

Following this, H made a payment of £42,965.20 to the account the fraudster provided, which was with HSBC. The scam came to light a week later when the supplier contacted H for payment. H contacted their bank who in turn contacted HSBC. Unfortunately, HSBC was only able to recover a very small amount.

H complained to HSBC who did not uphold their complaint. The bank said that it didn't do anything wrong and that it attempted to recover all the money it could, on being advised of the scam.

One of our investigators reviewed the complaint and were of the view that it should be upheld. They said, in summary:

- At the time the recipient's account was opened, there wasn't anything suspicious that should have alerted HSBC to the fact that the account would later be used for fraudulent purposes.

- However, the receipt from H and the outgoing payments soon after, were unusual to the normal account activity. So, HSBC should have intervened at least when a large payment went out of the account. Had it done so and contacted its customer to gain an understanding, their customer wouldn't have been able to give a reasonable explanation and the fraud would have come to light. HSBC missed an opportunity here to help H avoid their financial loss. So, it is fair that the bank compensates them.

H accepted investigator's opinion, but HSBC did not. In the main it said:

- The account activities surrounding the receipt of H's payment were not unusual for the bank to have intervened.

- Even if the bank had intervened and contacted its customer to question some outgoing payments, the focus would have been to ensure that its customer wasn't at risk of

financial harm from fraud. And even if at that the time the bank questioned their customer about the incoming payment, it is quite possible their customer would have been able to provide reasonable explanation to it.

- The fact that its customer did not respond to the bank when it tried to contact them at a later stage isn't a reliable indicator of what would have happened before. This is because at that time there would have been an incentive to give the bank a convincing story. That incentive would no longer have been there when the balance had been depleted.

- H should assume some responsibility for their actions. When the fraudster advised change to the bank account, H could have called their supplier to confirm the bank details. In addition, in the email from the fraudster there were 'warning signs' such as poor grammar and an implausible reason for the payment details to change. That is something H ought to have noted. Therefore, at the very least, H should equally share the loss.

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.

HSBC says that from a legal perspective they owe no duty of care to a third party (like H) with whom they have no contractual relationship. I take on board the point HSBC makes, but whilst I must take the law into consideration, my role as an Ombudsman is to ultimately decide a complaint based on what I think is fair and reasonable in all the circumstances.

HSBC has an ongoing obligation to be alert to various risks in relation to accounts with it. Specifically, I'm mindful that it:

- must conduct their business with due skill, care and diligence;
- has a longstanding regulatory duty "*to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime*" (SYSC 3.2.6R of the Financial Conduct Authority Handbook);
- must fairly and reasonably been monitoring accounts and any payments made or received to counter various risks including anti-money laundering and preventing fraud and scams. At the material time, those requirements included maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage risk, e.g. through customer due-diligence measures and the ongoing monitoring of the business relationship including through the scrutiny of transactions undertaken throughout the course of the relationship;
- must have systems in place to look out for unusual transactions or other signs that might indicate risk of fraud. This is particularly so given the increase in sophisticated fraud and scams in recent years.

The SYSC guidance I've referenced above is about systems and processes for the monitoring of accounts. But that monitoring has a purpose, and that is to be alert to and to react to various risks including concerns of fraud, scams and the misappropriation of funds.

It is a matter for HSBC as to how it chooses to configure its fraud detection systems and strike a balance between allowing its customers to transact business and questioning transactions to confirm they are legitimate.

However, where it is alleged that it didn't do enough to prevent a loss which resulted from an authorised push payment fraud, I will look into the circumstances of the case and based on what I have seen, decide whether in that case HSBC could have fairly and reasonably done more.

The bank has provided relevant information to our service to allow us to investigate this. I am limited as to how much information I can share because it relates to a third-party account. But I'd like to assure H that I've carefully reviewed everything before reaching my decision.

Having reviewed the submissions, I agree with the investigator that HSBC could have done more here, for the reasons they have explained.

As I understand it, the recipient's account was a personal account and was opened in November 2019. Thus, it was a newly opened account. Since opening, there were a couple of small receipts into the account and small outgoing payments. These were very low value international payments and were made despite the charges forming a sizeable proportion of the payment amount (between 10% to 20%), which in my view was somewhat unusual. Such transactions could be indicative of a fraudster testing the system.

Then an unusually large payment of about £43,000 (from H) arrives. Soon after, the customer attempted to transfer most of it abroad, through a single payment.

Given all this, I agree with the investigator that there was enough going on here that ought to have prompted HSBC to take a closer look at what was happening, at least when the large payment was made out of the account, if not earlier.

It may be, to start with, the bank's objective would have been to look out for unusual transaction going out of the account in order to protect its customer from possibility of fraud. But that would have given the bank an opportunity to look more closely at what was going on.

Had it done so, it would have noticed all that I have mentioned above. Further, had HSBC carried out proper checks at that point in time, it would have also noticed that in relation to the incoming payment, the payee's name on the payment instruction was completely different to that of its customer's. An incoming payment with a beneficiary name mismatch is something commonly seen with the movement of the proceeds of a fraud or scam. Indeed, at the time this transaction occurred, the Payments Systems regulator had already proposed Confirmation of Payee check as an important tool to help prevent such APP scams. And a quick internet search would have revealed that the named payee is a large international firm.

I think all of this was enough to have given the bank sufficient cause for concern, and enough to have prompted a further investigation.

I acknowledge that it is difficult to know for certain what would have happened had the bank intervened and questioned its customer about the source of incoming payments. However, on balance, I am not persuaded that its customer would have been able to convince the bank about the receipt of an unusually large payment intended for a large international courier firm.

Generally, when there are concerns about a payment, banks do tend to thoroughly investigate the matter. And had HSBC done so, I think it would have, during this time received the scam notification from the remitting bank.

Thus, I think the bank missed an opportunity here to help prevent the financial loss to H. Therefore, it is only fair that it compensates H for the loss it would not have suffered but for the bank's failure.

Did H act reasonably in the circumstances?

For completeness, I've also considered whether H should bear some responsibility for their loss due to any contributory negligence.

As I understand it, it was the supplier's email which was hacked and as such the email address from which H received the emails weren't suspicious. The fraudster's email came from genuine email address of the supplier and H wasn't aware of what had happened.

Further, the email was part of a chain of emails between H and the genuine supplier. Just prior to the fraudster's intervention, the supplier sent H a statement of account and H asked the supplier to provide a copy of a specific invoice (which presumably was mentioned in the statement of account along with other invoices). The fraudster was able to provide a copy of the requested invoice (which would only have been available to the supplier) and along with that advised change of bank account. In the circumstances, I think it is reasonable for H to believe that they were dealing with their supplier and the instructions came from them.

I have considered the contents of that email and I am not persuaded that the wordings were so odd that ought to have made H suspicious.

I agree that it would have helped had H called its supplier to verify the account details but given what I have said above, I don't think H acted unreasonably by proceeding to make the payment as instructed. In the circumstances, I can't fairly conclude that they should share the loss with the bank as proposed by it.

Putting things right

The payment made to the fraudster was £42,965.20. As I said, the bank ought to have intervened at least when the large payment was made out of the account and that would have led to the subsequent loss being prevented. From what I can see this was the first payment after receipt of H's funds. So, I consider that the bank should reimburse H its entire loss.

However, of this, I understand that £1.54 was recovered and that it was returned to H. If so, the loss to H works out to £42,963.66.

This means HSBC should reimburse £42,963.66 to H. It should also pay interest on this sum. The funds were lost from a business current account, which earned little interest. But the relevant question is the opportunity cost of the lost funds to H. In this case, I cannot be certain about the cost to H of being deprived of the money because it might have used the funds in a variety of ways. It is however clear to see that this was a large sum of money, and the loss has had a big impact on the company. In the circumstances, without any compelling reason to depart from our usual approach, I consider it fair and reasonable that HSBC pays H simple interest at 8% p.a. on the £42,963.66, and that the interest be paid from the date the bank was notified of the scam to the date of settlement.

My final decision

My final decision is that I uphold the complaint. In full and final settlement of it, HSBC UK Bank Plc should pay £42,963.66 to H together with simple interest at 8% p.a. Interest should be paid from the date the bank was notified of the scam to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask H to accept or reject my decision before 1 March 2024.

Raj Varadarajan
Ombudsman