DRN-4208247

The complaint

Mr and Mrs J complain that HSBC UK Bank Plc (trading as First Direct) won't reimburse the money they've lost to a scam.

What's happened?

Mr and Mrs J fell victim to an email interception scam whilst purchasing a new home in 2022.

On 22 July 2022, contracts were exchanged. On that day, Mr J spoke to the couples' solicitor and was told that he would shortly receive a copy of the mortgage redemption certificate, completion statements and instructions for paying the balance due of £38,864.53, via email. A couple of hours later, Mr J received the email he was expecting. The balance was paid from Mr and Mrs J's joint account via faster payment to the account details quoted in the email on 23 July 2022.

At that time, Mr J didn't know that his email account had been hacked by a fraudster, who had intercepted the solicitor's email and changed the account details quoted in the balance payment instructions to their own before sending it onto him from an email address which was very similar to the solicitor's.

Mr and Mrs J say they didn't have any suspicions about the email Mr J received because:

- The 'From' field displayed the solicitor's name.
- It followed the solicitor's writing style and tone.
- They were expecting to receive it after Mr J's telephone conversation with the solicitor earlier that day.
- They had no idea that this type of fraud was possible.
- They thought the solicitor had exclusive access to the authentic documents attached to the email.
- A small payment had been made to a different account previously, but they thought it entirely plausible that a solicitor would have a separate account for completion of sales/purchases.

The fraud came to light when the solicitor advised that the balance payment hadn't been received.

Mr and Mrs J raised a fraud claim with HSBC. The bank recovered £13.29 from the receiving account, and returned it to them, but it declined to reimburse their remaining loss under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code'). HSBC said that it gave Mr and Mrs J an effective warning when the payment was instructed, but they didn't carry out sufficient due diligence before making the payment.

Mr and Mrs J referred a complaint about HSBC to this Service. They said that:

- They weren't rushing to make the payment, but the warning HSBC gave them wasn't effective – it didn't give any insight into the relevant fraud risk, it just flagged issues that weren't applicable to their situation.

- They checked they'd entered the receiving account details correctly after receiving HSBC's warning.

- They had no reason to doubt the authenticity of the email Mr J received.

- They weren't aware of how email interception scams work at the time.

What did our investigator say?

In summary, our investigator didn't agree that HSBC had provided Mr and Mrs J with an effective warning, and she thought that they had a reasonable basis for belief when they made the payment. She recommended that HSBC reimburse Mr and Mrs J's full financial loss and pay interest at a rate of 8% per annum from the date the payment was made.

In responding to our investigator, HSBC maintained that it had given Mr and Mrs J an effective warning, but they failed to follow its advice. The bank said that if they had done so, its warning would have had a material effect on preventing the scam. HSBC acknowledged that its warning didn't specifically focus on a single scam risk but said it's unrealistic to expect it to, and that alone doesn't make the warning less impactful. The bank pointed out that the warning told Mr and Mrs J what to do if they'd been contacted by email and advised them to check any change in payment details.

This case has now 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.

HSBC is a signatory of the CRM Code, which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr and Mrs J have fallen victim to, in all but a limited number of circumstances. HSBC has argued that two of the exceptions apply in this case. It says that Mr and Mrs J ignored an effective warning it gave during the payment journey, and they made the payment without a reasonable basis for belief that the payee was the person they were expecting to pay, the payment was for genuine goods or services and/or the person or business they were transacting with was legitimate.

Effective warning

The CRM Code says:

SF1(2)(e) *As a minimum, Effective Warnings should meet the following criteria*

(i) *Understandable – in plain language, intelligible and meaningful to the Customer*

(ii) *Clear – in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's* [Financial Conduct Authority] *Principles for Businesses*

(iii) *Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;*

(iv) *Timely – given at points in the Payment Journey most likely to have an impact on the Customer's decision-making;*

(v) *Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*

HSBC says it gave Mr and Mrs J the following warning during the payment journey:

"Caution – this could be a scam

WARNING** – if someone has told you to mislead us about the reason for your payment and/or choose the wrong payment type, **stop, this is a scam.

Fraudsters may advertise on social media, online marketplaces and on websites that seem legitimate but have been set up to carry out fraud. They can also pretend to be a genuine business, access your emails or invoices and ask you to make payment to a different account.

What you need to do before making the payment:

- ***stop and think** – does this seem right? Is the offer for a limited time or too good to be true?*
- ***if you are contacted by email** check the content and address, does it have any grammatical errors or unusual changes in font or format? Was it sent from the company you expected? Is the sender's email address different, even by just one character?*
- ***check any changes** like payment details by contacting the person or company using a phone number you've checked is genuine*
- ***beware of false websites and reviews** and thoroughly research the seller online using trusted sources before sending any money*
- ***don't make the payment** if you're asked to pay by bank transfer rather than using a more secure way e.g. credit or debit card, which gives you more protection against fraud*
- ***if you are paying for a high value item** like a car, make sure you physically see it before making a payment.*

*Visit our **Fraud Centre** for more information on what you should check before making payments.*

IMPORTANT

***By choosing to continue, you agree you've read this warning you're happy to proceed and that we may not be able to recover your payment if it's sent to a fraudster's account. If you have any doubts or concerns at all, please stop immediately.**"*

HSBC says that, within its fraud centre, there is information on different types of scams and

how to spot the signs and stay safe. This includes a section on email interception scams.

I've considered the warning and, overall, I'm not satisfied it can reasonably be said that the requirements of the effective warning exception were met. The warning isn't specific to the APP scam risk here – it covers off several different scam risks – and I don't think it's impactful enough to affect a customer's decision making in a manner whereby the likelihood of an email interception scam succeeding is reduced.

It's clear to me that HSBC's warning attempts to prevent email interception scams. It says that fraudsters can access your emails and invoices and ask you to make a payment to a different account. It also advises on what to do before making a payment if you are contacted by email, and to check any changes in payment details by telephone. But I don't think the warning goes far enough to make the risk really obvious to customers. It doesn't bring to life what this type of scam looks like, nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be. For example – it doesn't explain that fraudster's emails appear to come from a familiar person or business, that fraudulent emails are usually received when a payment request is expected or that fraudster's emails can look the same or very similar to the person's they're impersonating.

I'm not persuaded that a reasonable person would fully understand the risk in an email interception scam from the warning HSBC gave.

The circumstances of this scam made the warning even less effective. Mr J had been successfully communicating with the solicitor for some time before the fraudulent email was received. Mr and Mrs J were at the last stage in the process of purchasing a new home and everything had gone smoothly so far – including when they made a prior small payment to the solicitor. Mr J received an email he was expecting to receive on the same day as he spoke to the solicitor on the telephone. The email displayed the solicitor's name in the 'From' field, it followed the solicitor's writing style and tone, and it attached authentic documents relating to the house purchase. To Mr J, everything looked the same as it had always done, and nothing stood out as suspicious. From what I've seen, I don't think Mr J appreciated the risk that the email may have come from a fraudster. This is supported by his testimony. If HSBC had really brought to life what a scam of this nature looks like, then I think that would've been important information in the context of this scam that would've affected Mr and Mrs J's decision making and led them to take additional steps to protect their assets.

Reasonable basis for belief

From what I've seen, I'm satisfied that Mr and Mrs J had a reasonable basis for belief in this case. They've said that nothing about the email stood out to them as suspicious, and I can understand why. I don't think it's unreasonable in the circumstances, particularly as HSBC didn't give them an effective warning which adequately explained the fraud risk.

The email:

- Was received a couple of hours after Mr J's telephone conversation with the solicitor in which he was told to expect it.

- Displayed the solicitor's name in the 'From' field and was sent from an email address which was only one character different from the solicitor's genuine email address – making the fraud difficult to detect.

- Followed the solicitor's writing style and tone (some of the content was copied directly from the solicitor's genuine email).

- Attached the mortgage redemption certificate and completion statements, and I think this is very persuasive. Mr and Mrs J have explained that they thought the solicitor had exclusive access to those authentic documents, and I think this is a reasonable assumption.

I appreciate that HSBC's warning explains that fraudsters can access your emails and invoices and ask you to make a payment to a different account and advises on what to do before making a payment if you are contacted by email, and to check any changes in payment details by telephone. And that Mr and Mrs J didn't follow HSBC's advice. They've explained that they weren't rushing to make the payment, but they didn't think the warning flagged issues that were relevant to their situation. They did check they'd entered the receiving account details correctly but otherwise; they didn't understand the fraud risk.

As I've set out above, I don't think the warning goes far enough to make the risk really obvious to customers. It doesn't bring to life what this type of scam looks like, nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be. I don't think it's unreasonable that Mr and Mrs J didn't follow HSBC's advice and/or take additional steps to protect their assets in absence of a specific and impactful fraud warning that gave them a good understanding of the risk, and in light of the persuasiveness of the fraudster's email in the surrounding context.

I also appreciate that Mr and Mrs J were instructed to pay a different account to the one they'd paid previously. But I think their assumption about the reason for this was reasonable.

Overall, the fraud was sophisticated, and I can understand why it went undetected by Mr and Mrs J.

Conclusions

Considering everything, I'm persuaded that HSBC should've reimbursed all the money Mr and Mrs J lost to this scam under the CRM Code. I'm not satisfied that any of the permitted exceptions to reimbursement apply in the circumstances of this case.

In addition, I think that HSBC ought reasonably to have done more to prevent this scam. It's common ground that Mr and Mrs J 'authorised' the payment under the Payment Services Regulations, and HSBC had an obligation to follow their payment instruction. 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 HSBC 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 banks 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.

It doesn't appear that the payment Mr and Mrs J made triggered HSBC's fraud detection systems, and I think it ought to have. The payment was high value, it was for significantly

more than any other recent payments out of Mr and Mrs J's account, and it went to a new payee. I think it stands out as unusual and out of character, and it's reasonable to expect HSBC to have asked Mr and Mrs J some questions about it before it was processed.

Even if the possibility of financial harm from fraud was identified, I can see that HSBC didn't contact Mr and Mrs J to ask them further questions about the payment or advise them of the scam risk, as I think it ought to have. If it had done so, I think it's likely that the bank would've recognised the risk of email interception, as it did in a telephone conversation between the parties after the payment had been made during which the discrepancy between the solicitor's and fraudster's email addresses was uncovered, and the scam would've unravelled without the payment being made.

The relevance of this finding is that HSBC ought to have prevented Mr and Mrs J's loss, so the bank should pay interest from the date of loss rather than the date it decided not to refund them under the CRM Code.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct HSBC UK Bank Plc to:

- Reimburse Mr and Mrs J's full financial loss (deducting the £13.29 recovered from the receiving account) within 28 days of receiving notification of their acceptance of my final decision; plus

- Pay 8% simple interest per year on that sum from the date the payment was made to the date of settlement.

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

Kyley Hanson
Ombudsman