DRN-4641026

The complaint

Mr A complains that HSBC UK Bank Plc placed a block on his credit card due to suspected fraud. He's unhappy with HSBC's handling of this matter, including their fraud procedures, and the impact this had on him while he was abroad. Mr A wants to be compensated for this.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

HSBC contacted Mr A by text message on 14 October 2023 providing a fraud alert. They asked Mr A to log on to his mobile banking app to verify an attempted transaction. HSBC explained that, to protect Mr A, they may temporarily block the card until he responds.

HSBC sent Mr A another fraud alert text message, about an hour later, which explained they needed him to verify recent transactions. And that Mr A would shortly receive a message – from another number – with directions on how to respond. HSBC reiterated that they may decline the card until they receive a response.

HSBC sent the further text message to Mr A, which said:

> *"HSBC Fraud Alert: Possible unauthorised transactions on card ending [XXXX], If YOU have attempted to make all these transactions reply Y, if NOT reply N. 0.00USD 14-Oct-2023 12:18 PM AMAZON.COM; 200.00USD 13-Oct-2023 11:22PM CIVILIAN HOTEL"*

Mr A has explained that, as the messages were from unknown numbers, he thought they were phishing attempts from a fraudster. He did however receive a push notification on the HSBC mobile banking app asking whether he recognised a $0.00 Amazon transaction. As he didn't, Mr A selected 'no'.

HSBC placed a block on Mr A's credit card, preventing him from making any transactions. Mr A contacted HSBC via their mobile banking chat but they explained to him that he would have to call their telephone banking team.

Mr A says he tried to contact HSBC on several telephone numbers that he'd been provided but the calls wouldn't connect. But, after receiving a voicemail with a pre-recorded message from HSBC, he did speak with them on Monday 16 October 2023 about the disputed transaction and the block placed on his account – as he wanted to know how it could be removed so that he could use his credit card while abroad.

HSBC explained to Mr A that, as he didn't recognise the $0.00 Amazon transaction, they would need to cancel the card and order a new one to his UK address. Or alternatively, as Mr A said he needed to be able to use his credit card while abroad, he could contact them to have the block temporarily removed each time he wanted to make a purchase. Mr A was unhappy with the options put forward by HSBC. He thought having to call HSBC on each occasion he wanted to make a purchase wasn't practical; and sending a new credit card to

his UK address wouldn't be helpful while he was abroad. He said HSBC were leaving him stranded without the ability to access his finances or make payments. Mr A raised a complaint.

HSBC rejected the complaint. In short, they said:

- A transaction for £0 was attempted by Amazon which breached their security parameters – thereby prompting a temporary block on the credit card until they could speak with Mr A. And they sent a notification to Mr A via mobile banking asking him to confirm the transaction was genuine – to which he replied 'N'.
- When they spoke with Mr A, he confirmed he didn't recognise the transaction and so the block remained in place.
- They acknowledged this was inconvenient and frustrating for Mr A - and apologised for this. But they explained a fraudster will on occasion test a card with a £0 transaction to check its authenticity before processing further transactions for larger amounts. And so, if a customer doesn't recognise a transaction, it is safer to cancel and re-issue the card.
- They did offer to keep the block in place, rather than cancel the card, thereby allowing Mr A to contact them when he needed to make a payment. Although they appreciated Mr A wasn't happy with this solution, they'd followed their correct process.
- Mr A's card had since been cancelled with a new one issued.
- Although Mr A complained that his calls to HSBC were unanswered, their fraud detection team is open seven days a week, 24 hours a day. As well as their Premier Team being open seven days per week between 8am and 8pm. They'd had no reported issues with calls being unanswered over the period Mr A tried to contact them.

Mr A remained dissatisfied and highlighted further concerns. These included:

- How did HSBC try to contact him as he hadn't received any calls on his personal number?
- He received text messages from HSBC while abroad from unknown numbers that included a link to Amazon.com and asked him to call them urgently. He struggled to understand how HSBC believes sending text messages from random numbers is a secure method of informing customers. And he questioned how he could've identified these as legitimate requests opposed to phishing attempts?
- Similarly, how could he have differentiated between whether the pre-recorded message he received on a voicemail came from HSBC or a fraudster?
- How could anyone recognise a transaction for a zero value in a different currency? With the limited information he had he could only say he didn't recognise it.
- He contacted HSBC via the live chat function but he was told they couldn't help – and that he would have to speak with the fraud team. Unfortunately, any attempt to contact HSBC failed (and he provided details of the telephone numbers he tried). In the meantime, he was left in a foreign country with no access to his finances or way of contacting HSBC about the matter.
- When he did speak with HSBC, he wasn't given any additional information to have allowed him to understand whether it was a legitimate transaction.
- The systems HSBC use to inform customers about any potential alerts are underwhelming and of a poor standard, and he questions why the Amazon transaction was flagged to begin with.
- He'd experienced a similar issue with HSBC a year prior.

HSBC's position didn't change. In short, they added:

- They attempted to call Mr A on the number they hold, with the line ringing for a few seconds before going to a busy tone.
- They were sorry Mr A felt the attempts to contact him by text message appeared to be phishing – but they use this method of contact to try and resolve fraud checks efficiently.
- They apologised for any issues Mr A had attempting to contact them. They explained that, from the numbers he provided, the first was the correct number for calling overseas to speak to their fraud detection team. The second is for customers calling within the UK. And the third is for their telephone banking team when calling from overseas – available seven days per week between 8am and 8pm UK time. They'd experienced no issues with the lines for customers calling.
- When a transaction is processed by a retailer they have minimal information available. Therefore, if a customer doesn't recognise it, they will cancel the card as a security measure – which is done to protect customers and HSBC.

Mr A remained unhappy, reiterating that he hadn't received any calls or voicemails from HSBC. And that HSBC's actions are made to protect themselves, not cardholders. Further, Mr A said HSBC still hadn't established whether the zero-dollar transaction was fraudulent or not. But, nonetheless, HSBC don't seem concerned that a potentially insignificant issue has left a customer in a difficult position – with him having to use other cards to make transactions while abroad.

The complaint was referred to the Financial Ombudsman but our Investigator didn't think HSBC had to do anything further. She said HSBC acted reasonably, and in line with the terms of Mr A's account, by putting the block in place – which was a security measure for both Mr A and HSBC. And that leaving the card unblocked would've left it open to possible unauthorised use.

Our Investigator noted that Mr A said HSBC's proposal for him to call them to temporarily remove the block wasn't feasible. But, in the circumstances, she didn't think there was any other alternative given that removing the block would pose a security risk. And although Mr A had said he was left without access to his finances, he'd confirmed he was able to use other debit and credit cards he had with him – so, while these may have offered different exchange rates, Mr A still had access to funds while abroad as well as a credit card that provided protection under section 75 of the Consumer Credit Act.

In respect of HSBC's fraud processes, our Investigator explained that it isn't uncommon for fraud alerts to be sent by text message. And although she understood Mr A's concerns about them being possible phishing attempts, she thought HSBC's messages were clear about the potential fraudulent transactions. And that their explanation as to why it was flagged by their security system was reasonable. Our Investigator acknowledged Mr A's frustration at trying to resolve the situation while abroad, but she explained that HSBC had to make sure they were speaking to the genuine account holder and so it was reasonable for HSBC to ask Mr A to contact them. And although Mr A says he didn't receive any missed calls from HSBC, the phone number they hold for him matches what Mr A provided the Financial Ombudsman.

Mr A disagreed and so the matter has been passed to me to decide. In short, Mr A has added:

- HSBC's actions weren't a protective measure for him as the card issuer has full liability for fraudulent purchases made with a credit card.
- His request for compensation is due to the extremely poor service provided by HSBC and it has nothing to do with the mitigation he took to take care of himself. He

could've been left with no access to any other form of cash, credit or debit facilities and HSBC would've acted in the same way.
- The methods used by HSBC to inform customers about potential fraud are the same of those used by fraudsters – that being text messages received from an unknown number.
- He didn't read the text messages in the order HSBC sent them – as he read the third message, asking him to reply 'Y' or 'N', first. And this message appeared like a phishing attempt particularly as the text 'Amazon.com' had a clickable link. How therefore is it ok for one of the largest banking groups in world to fight fraud in 2024 by sending customers asynchronous messages from 'HSBC Fraud' and random numbers?
- The messages from HSBC also refer to two transactions, one very identifiable whereas how is it possible for someone to identify a $0 transaction? And he questions what this transaction was for, was it a pre-authorisation check by Amazon who hold his card on file? If HSBC is asking him to recognise the transaction, with the consequences of blocking his card, they should at least help him to make an informed decision – but here, they couldn't explain what triggered it including how it was attempted or in what country/time zone.
- He was essentially asked to recognise a transaction of no value at one of the biggest merchants in the world, which he shops at every other day. He did say he didn't recognise it but he could've easily said he did considering it was of zero value. He was asked to make an informed decision without any context about the transaction, while being unable to speak to anyone because the fraud team was gone for the weekend while his card was blocked.
- There is no evidence nor explanation as to whether there was any fraudulent activity.

Before I go on to explain the reasons I've reached, I want to clarify that I'm only looking at the circumstances of this complaint here. And so, while Mr A has referred to previous experiences of his card being blocked by HSBC, including another complaint decided by the Financial Ombudsman last year, this won't form part of my 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.

I appreciate Mr A was inconvenienced because of the block placed on his credit account by HSBC due to suspected fraud, particularly given this happened while he was abroad. I'm aware Mr A has made a number of points for my consideration in support of his complaint. I've given careful consideration to all the evidence provided. And so, I'd like to reassure Mr A that if I don't mention a particular point, it's not because I haven't considered it, but I've focussed instead on what I believe to be important to the outcome of this complaint. Having done so, and while I know this won't be the outcome Mr A is hoping for, I don't think HSBC acted unfairly for similar reasons to our Investigator. I'll explain why.

HSBC is expected to have systems in place to counter various risks such as preventing fraud and scams. To do this, HSBC should look to identify unusual transactions, or other signs, that their customers are at risk of fraud. And carry out additional checks before processing payments, or declining them altogether, to prevent the possibility of financial harm from fraud.

HSBC's terms and conditions also say:

> ***"5. Can we refuse to authorise a transaction or suspend your right to use the account?***
>
> *5.1 There are times when we might refuse to authorise a transaction, cancel or suspend use of the account or refuse to replace or reissue a card. This could be where we reasonably consider it's necessary for any of the reasons set out below.*
>
> *(c) We suspect fraudulent or unauthorised use of the account.*
>
> *(d) We believe we have to so we can keep the account or card secure."*

I'm therefore satisfied that, where there is reason for HSBC to suspect fraudulent or unauthorised use of the account and/or they believe it necessary to keep the account or card secure, HSBC can suspend (block) use of the account. And so, I've considered whether it was reasonable for them to do so here.

HSBC's systems identified two possible unauthorised transactions on Mr A's account. And so, I think it was reasonable for HSBC to block Mr A's account until he responded to confirm whether they were legitimate or not. Mr A recognised one of the transactions but the other he did not – that being a $0.00 transaction to Amazon.com, which he confirmed to HSBC via their mobile banking app after receiving a notification. Given Mr A confirmed that he didn't recognise the transaction, there was a risk his account was being used for fraudulent purposes. Because of this, I think it was reasonable – as per the account terms - for HSBC to maintain the block to prevent this from happening until they spoke with him further.

When Mr A did speak with HSBC, he confirmed that he didn't recognise the transaction. Mr A has questioned how anyone could identify a transaction of a zero value. And that beyond knowing its value and that it was being made to a merchant he regularly used, he wasn't given any further information about it. While I appreciate Mr A had limited information about the transaction, I don't think I can hold HSBC responsible for that. This is because they would've simply received the request for payment from the merchant and so, they wouldn't have known what it was for – although HSBC did try to explain that, often, zero value transactions are used as a pre-authorisation check. And that these types of pre-authorisation checks are sometimes used by fraudsters to check its authenticity before processing further transactions for larger amounts.

Given the payment was also made to Amazon.com, it's reasonable to conclude that it was made with the card details entered online – and so, it wouldn't have been a chip and pin transaction. Nevertheless, I think it was for Mr A – and not HSBC – to know whether he had made the transaction or not. And it's unclear to me what, if anything, HSBC could've provided to Mr A for him to have had a better understanding as to whether he recognised it as a legitimate transaction or not. This is because, as Mr A has explained he is a customer of Amazon, he ought to have known whether he'd agreed to a payment or pre-authorisation check for goods or services from them. And if he didn't, Mr A could've – if he wished - contacted Amazon to have queried whether there was a payment on his account and, if so, what it was for. I therefore don't think it is fair or reasonable to hold HSBC responsible for Mr A not recognising a payment on his credit card.

As HSBC explained, pre-authorisation checks are sometimes used by fraudsters to check its authenticity before processing further transactions for larger amounts. And so, given Mr A didn't recognise the transaction, it was reasonable for HSBC to conclude Mr A's credit card might have been compromised. I therefore think it was reasonable for HSBC to explain to Mr A that they would need to cancel his card and re-order a new one to prevent potential fraudulent use. The issuing of a new card to Mr A's UK address however meant that he

wouldn't have access to his credit facilities while abroad. And so, I think HSBC proposed a reasonable solution in the circumstances by providing Mr A with the option of not cancelling the card, keeping the block in place but allowing him to contact them to have it temporarily removed when he wanted to make a purchase. By doing this, and keeping the block in place, it allowed Mr A access to his credit facility – albeit with limitations – and ensured the account/card remained secure which, as per the account terms, HSBC is allowed.

I'm aware Mr A has questioned the practicality of this proposal – as it would've been inconvenient for him to call on every occasion he wanted to purchase something and, if in a location he didn't have a phone signal, not possible at all. While I appreciate the challenges this proposal would've had on Mr A, I wouldn't expect HSBC to remove a block on a credit card in situations whereby it would expose it to possible fraudulent use. And so, I don't think it was unreasonable for HSBC to give this as an option for Mr A in the circumstances – as it allowed him access to his credit facilities whilst keeping the account secure.

At which point, I understand Mr A has argued that HSBC's actions were for their own benefit, protecting themselves, and not him as the cardholder. This is because, had there been fraudulent purchases made on the credit card, Mr A says HSBC would've been fully liable for them. While I've noted Mr A's point here, there are circumstances in which cardholders can be held liable for transactions they haven't authorised themselves. But irrespective of that, it's not unreasonable for HSBC to protect themselves from fraud either – and the account terms allow them to suspend a customer's account to do just that.

Mr A has pointed out that the actions HSBC took could've left him stranded abroad without access to cash or debit/credit card facilities. But that wasn't the case here as Mr A has confirmed he did have access to other banking facilities which he successfully used. I note Mr A's claims this was due to his own actions in mitigating the situation he found himself in. But I can't consider something that didn't happen. And if Mr A had been in the position whereby the HSBC credit card was his only method of accessing funds while abroad, he could've explained this to HSBC for their consideration. In any event, HSBC offered Mr A a way of being able to use the credit card – that being to call them when he wanted to make a transaction. So, even if Mr A had been in the situation he's suggested, he would've still been able to make purchases or withdraw cash on his credit card if required.

I understand Mr A is dissatisfied with the systems and processes HSBC has in place when handling fraud, particularly in respect of how they notify customers of potentially fraudulent transactions. This is because the communication he received by text message and a voicemail came from unknown numbers and he says it was indistinguishable from phishing attempts used by fraudsters. Although I appreciate Mr A's views on this, it's not the role of the Financial Ombudsman to tell financial firms how to operate. That said, it's not uncommon for banks to contact their customers by way of text message when fraud is suspected. Naturally, customers should think carefully about the communication they receive and whether it is genuine or not – which, fortunately, in this case it was. So, while I'm understanding of Mr A's concerns, I can't see there has been any impact as a result here – particularly as Mr A also received a notification via the mobile banking app, which is considered a secure method of communication, about the potential fraud. This therefore would've given him greater reassurance it wasn't a phishing attempt.

I've also considered the difficulties Mr A has referred to in communicating with HSBC. He's said the telephone numbers he tried to contact HSBC on didn't connect, and that he never received calls from them as they claimed. Although Mr A has provided evidence showing his attempts to contact HSBC, it's unclear why these were unsuccessful. HSBC has confirmed they didn't have any reported issues with their phone lines at the time and, of the three numbers Mr A confirmed he tried, two of these were open 24/7 – one of which was the

correct number for customers calling when overseas. So, although I don't dispute Mr A had difficulties trying to contact HSBC, I can't reasonably conclude HSBC was responsible for that.

It's similarly unclear as to why Mr A says he didn't receive the attempted calls from HSBC. The telephone number HSBC hold on file matches that which Mr A provided the Financial Ombudsman. And I'm satisfied HSBC held Mr A's correct telephone number as he received their text messages. It's therefore difficult for me to know whether HSBC is responsible for this issue either. In any event, I can see that when HSBC explained to Mr A that they'd tried to call him, he explained his preferred method of communication was email. So, I don't think he was inherently disadvantaged by this issue.

I realise Mr A had a poor experience because of the block HSBC placed on his credit card due to the suspected fraud. I'm sympathetic to the impact dealing with this matter had on him while in another country, as well as when he returned. I also appreciate that Mr A has said that it remains unclear as whether the transaction was indeed fraudulent or not. Mr A could however contact Amazon further about this if he wants confirmation – as they should be able to tell him whether they attempted to make such a payment on his account. But even if turns out not to be fraudulent, HSBC had reason to believe it was and this suspicion was supported by Mr A's inability to recognise the transaction. And, for the reasons I've explained, I consider HSBC acted reasonably – and in line with the terms of Mr A's account – by putting the block in place on his account. It follows that I won't be directing HSBC to take any further action here.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 2 April 2024.

Daniel O'Dell
Ombudsman