DRN-4045997

The complaint

Mr and Mrs W are unhappy that HSBC UK Bank Plc has not refunded them after Mr W was the victim of a safe account scam.

Whilst this complaint concerns a joint account, it was Mr W that fell victim to the scam and is acting on behalf of both account holders in bringing this complaint – so I have only referred to him throughout this decision.

What happened

I'm not going to cover all the points raised in detail. The view of 31 March 2022 covered the detailed timeline of the transactions and the details of Mr W's testimony. But briefly:

On 19 January 2021, Mr W says he received a call from someone who he believed was from HSBC's fraud department. Mr W told us he called the number on the back of his bank card and was given a password to verify the caller – which led him to believe the caller was genuine. The following day (20 January 2021) an attempt to transfer £17,000 via Mr W's online banking was made. However, this was declined, and Mr W was asked to visit one of HSBC's branches. Mr W did so later that day. The branch called the fraud team who spoke with Mr W directly. Mr W told the fraud team the payment was for building works. The block on Mr W's account was lifted and the transaction for £17,000 successfully transferred via online banking the following day (21 January 2021).

On 25 January 2021 a transfer of £25,000 was attempted – but declined. Again, Mr W was asked to visit a branch - which he did later that day and the transfer was completed. He told staff the payment was for his son. Two further attempts to transfer £25,000 were made in the days that followed - but both payments were blocked. Following the last attempted transfer on 28 January 2021, HSBC evoked the Banking Protocol and the police visited Mr W. They reported back to the bank that they had no concerns over the payments Mr W had made for his son and for building works.

On 3 February 2021, Mr W visited a branch and explained to staff he was told to lie to the police and branch staff by the scammer and now realised he had been the victim of a scam. HSBC declined to refund the transactions under the Contingent Reimbursement Model (CRM) Code. It said it gave the consumer an effective warning and Mr W didn't make any additional checks prior to making the payments.

Our investigator did not uphold the complaint as he felt HSBC had done all it could when questioning Mr W about the transactions and Mr W ought to have been concerned about the legitimacy of the transactions he was making.

I issued my provisional decision on 7 March 2023. HSBC hasn't responded. Mr W doesn't agree for a number of reasons and believes he should be fully reimbursed.

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 have considered Mr W's response to my provisional decision.

Many of the points Mr W has raised don't change the outcome here and I don't need to address every single point that's been raised if it is not material to the outcome. No disrespect is intended, and it doesn't follow that the points haven't been considered, simply that I don't need to particularise every point in reaching an outcome I consider to be fair and reasonable in all the circumstances. I've instead concentrated on the issues I think are central to the outcome of this complaint.

First, I want to make it absolutely clear that I am in no way doubting Mr W was a victim of a cruel and callous scam. This is a difficult decision to make; I'm sorry Mr W has lost a considerable amount of money and I can understand why he would like to be compensated for more of his losses. But I'm only considering whether the bank, which had no involvement in the scam itself, should be held responsible for what happened and whether it is fair to hold it responsible for all of Mr W's losses when there were signs that things were not quite right.

Second, it is not a question of me not believing Mr W and I am not saying he has been untruthful. As I mentioned in my provisional decision, where the evidence is incomplete, inconclusive or contradictory (as some of it is here), I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

I don't doubt at the time of the scammer's call(s) Mr W was tricked into believing he was speaking to HSBC. Furthermore, I accept Mr W may have been tricked into believing that he called the number on the back of his card and tricked into believing he had genuinely verified the individual as a representative of HSBC. But as Mr W acknowledges himself, he has always been aware the mobile call history doesn't reflect his version or recollection of the events. And as I have mentioned above – I have to base my conclusions on the evidence and what I think is more likely than not.

It is not for me to get Mr W's phone analysed (or disprove the facts simply because that is not how Mr W recalls the events). I have no doubts that the call history reflects what happened here – albeit this is not how Mr W recalls the events (or was tricked into recalling things differently by the fraudster).

In any event, I don't think the call history changes anything here (so there is no need for me to wait for Mr W to do further research into this matter). I accept Mr W may have been tricked into thinking he had called the genuine HSBC number – indeed this is a common tactic used by fraudsters (and this may have been what happened when the long number combining both the 0345 and 0800 number shows on the call history). The photo labelled 'time of my first call to HSBC' is an incoming call from 0800 not an outgoing call to 0800. I believe this is likely the spoofed 0800 call from the fraudster. The fact remains Mr W did not - at any point - get through to the genuine HSBC or a genuine HSBC employee on 19 January 2021.

I did not say “the initial contact was an incoming call to his mobile not the landline”. I don’t have the evidence in relation to the landline - but in my provisional decision I said:

I accept that Mr W was called by a spoofed number and don’t doubt the possibility that this was initially on his landline.

I apologise if my double negative has caused confusion - but to confirm - I accept there was a possibility Mr W was also called on the landline and I accept that a much longer call may have happened there.

Whilst I am not entirely sure of the relevance of this point, I don’t agree with Mr W that the bank’s email of 8 April 2021 denies the 0800 number was a valid HSBC number. On the contrary, it says:

I understand the call appeared to come from ‘0800….’, which is an HSBC Private Bank phone number. If you’d have researched the number, you’d have known this and questioned why HSBC Private Bank would be contacting you when your account is held with HSBK UK.

And

…you advised you’d dialled a number you’d found on the back of your card, ‘0345…. ’, and spoken to a member of staff who confirmed a password the fraudster had told you. This is not an HSBC phone number and isn't detailed on any HSBC cards. Conducting research on the number confirms this.

I also don’t doubt Mr W had a newly activated card and that there appeared to be suspicious activity on the card. And I understand, and accept, this was the premise on which the scammers call was made. In any event, this point it not material to the outcome of the complaint.

So, I accept Mr W was the victim of a scam and was tricked into thinking the bank had called him. I accept Mr W was tricked into believing he had called the number on the back of his card. At this point, and in the moment of the call, I accept he had a reasonable basis for believing this was a genuine situation. But for the reasons outlined in my provisional decision, I think this changed by the time the transaction was actually made.

With reference to the call and online transfer on 20 January 2021, I accept Mr W may not have been aware of these. It seems the bank had concerns over the voice in the call and the size of transfer being made. I think it’s possible that these attempts were made by the fraudster himself – who by now had access to Mr W’s banking details. It is also possible the online transfer (BP standing for Bill Payment) was made by the fraudster too and that if Mr W didn’t make the transfer himself – he was tricked into providing the information on the key generator to the fraudster – albeit he does now not recall. There is no other plausible explanation.

I appreciate Mr W may have believed (and possibly tricked by the fraudster into believing) that the transfer happened whilst in the branch – but again the evidence does suggest otherwise. The banks internal notes, along with Mr W’s own bank statements reflect the fact this was done the following day – 21 January 2021- by online Bill Payment.

In my provisional decision, I explained how for both transactions, Mr W made it difficult for HSBC to give a tailored and impactful warning (albeit, he believed he was helping the HSBC fraud department by not telling them the true purpose of the transaction). This means it would not be fair for me to say HSBC has failed in its obligation to provide an effective warning. The warnings given during the last two branch visits aren't relevant here – as no transactions took place.

The call that took place during the first branch visit did not warn about rogue traders as Mr W seems to recall – although this was the cover story Mr W gave the fraud team for the purpose of the payment. As I explained in my provisional decision – that call did specifically cover impersonation scams. And I also explained that aspects of the warning were good, for example the caller warns not to transfer funds in response to any suspicious calls asking Mr W to move money. And although, lost in a list of other trusted organisation, the fraud team member asked Mr W if he had received calls from HSBC.

In response to my provisional decision, Mr W says he had no reason to be suspicious. But this is not what was said during the call with the bank when he finally realised he'd been the victim of a scam. As I outlined in my provisional decision, Mr W said there were a lot of things he didn't understand, a lot of things didn't make sense. He acknowledged he was being asked to do 'some stupid things' and that he did 'some stupid things'. He says he knew something wasn't right.

I have noted Mr W's comments regarding the red flags I listed, but it was a combination and accumulation of red flags that I feel ought to have reasonably caused concern. I acknowledge that there could be an explanation behind each of the points I've mentioned, when they are all taken into consideration together and holistically, I think there was enough going on to question and check things further.

Having considered Mr W's further submissions and in the absence of any from HSBC, I see no reason to depart from the conclusions set out in my provisional decision. For completeness, I have set this out below.

HSBC is a signatory of the Lending Standards Board Contingent Reimbursement Model CRM Code (CRM Code) which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. HSBC says one or more of those exceptions applies in this case. The exceptions relevant to this case are:

- The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

- The customer ignored an effective warning in relation to the payment being made.

There are further exceptions within the CRM Code, but they do not apply in this case.

The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

I am also mindful that when Mr W made these payments, HSBC should fairly and reasonably also 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 (among other things). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud. For branch transactions, those steps may include following the Banking Protocol where appropriate.

Did HSBC meet its obligations under the CRM Code and did Mr W ignore an effective warning?

The CRM Code says that Effective Warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions.

The first transfer for £17,000 was actually made on 21 January 2021 (although there was in fact earlier intervention from the bank the previous day which I will come on to later). When considering what happened when the transfer was actually made, I can see HSBC did provide a 'light box warning' before the transaction was processed. Mr W was asked to choose a reason for the payment, and he chose 'paying a bill' rather than 'unexpected request from bank/police/organisation'. While Mr W says he doesn't remember choosing or seeing a warning (in fact, it's not clear to me if the consumer made the online transfer himself or whether the scammer did it on his behalf), HSBC has confirmed the real reason for the transfer (i.e. its 'unexpected request from bank/police/organisation') was an option at the time. But I am also mindful that Mr W was coached by the scammer into choosing a warning that wasn't the real reason.

I haven't repeated the warning that was shown during on the online payment process because Mr W's choice made it very difficult for HSBC to give a tailored and impactful warning. It wouldn't be fair to suggest that HSBC had failed to adhere to an obligation that it was never possible for it to meet. It's also the case that, had its 'unexpected request from bank/police/organisation' warning met the definition of 'Effective' under the CRM Code (that's not a finding I need to make here), it would be irrelevant because Mr W didn't see that particular warning. So, I don't find that HSBC has failed in its obligation to provide an effective warning, but I also can't say Mr W ignored an effective warning either.

Turning to the warnings on the second transfer for £25,000 that was completed in the branch on 26 January 2021, there is some contradictory evidence as to whether a warning was given. The notes relating to the branch visit at 16:08 (page 9 of 33 of HSBC's complaint summary document) indicate in answer to '*select warning msg relayed*' that '*warning not required'* was chosen. I appreciate the later testimony of that member of staff revealed this was a 'clerical error' and in fact questions in relation to 'family and friends' scams were asked, along with more general questioning. But this - and the consumer's responses - are not evidenced. In more recent submissions, HSBC provided the friends and family 'light box warning'. But as I understand it – the second transfer was done in branch and not via online banking – so I'm not sure how relevant this is – unless this was read out to the consumer in branch.

In any event, this was again a scenario where Mr W made it difficult for HSBC to give a tailored and impactful warning (albeit, as with the first payment, he believed he was helping the HSBC fraud department by not telling them the true purpose of the transaction). So for the same reasons as the first transaction - I don't find that HSBC has failed in its obligation to provide an effective warning but I also can't say Mr W ignored an effective warning either.

Warnings during bank intervention on 20 January 2021

HSBC had stopped the payment for £17,000 the day before it was finally transferred. The contemporaneous notes indicate HSBC had concerns over the consumer's voice during a call on 20 January 2021 at 12:42 and asked Mr W to visit the branch. Mr W visited the branch and from there he spoke to the fraud team over the phone with a branch staff member present.

During this call, Mr W was asked what the payment was for and he explained it was for some building works. He confessed he only knew the builder's first name and struggles to pronounce the second name. No further questioning around the building work was explored. This is a common cover story given in scam cases and I think, given the consumer's hesitation over the payee name and purpose of payment, it warranted further exploration. Especially given HSBC's concerns earlier that day with the voice mismatch and the further concerns that were revealed during this call about a failed login attempt – which Mr W confirmed wasn't him.

The fraud team member does go on to ask more generic scam type questions and specifically covers off impersonation scams. So, it seems HSBC had identified the particular scam Mr W was falling victim to. Aspects of the warning are good, for example the caller warns not to transfer funds in response to any suspicious calls asking Mr W to move money. However, I don't think the warning is impactful – as it doesn't ensure that Mr W understood the consequences of continuing with an irrevocable payment. The specifics of 'the bank' and 'HSBC' are lost in a list of other trusted organisations. It doesn't bring to life what scams of this nature look and feel like and could, for example, have pointed out that HSBC's fraud team would never call to ask a customer to transfer money. In any event, the warning is not timely - as the payment is not actually made at this time.

As I've said, there were other concerns during this call - as the fraud department clearly had qualms that someone else has logged on to Mr W's account and the caller does say to the branch staff member there's "*something fishy here"*. I think, given the concerns over a potential impersonation scam and the clear worries that someone else had tried to logon to Mr W's account, that HSBC could have taken further steps here. I think HSBC should have evoked the Banking Protocol at this point.

I've gone on to consider whether an effective warning and evoking the Banking Protocol at this point would have made a difference. I am mindful that when the Banking Protocol was eventually evoked sometime later - on 28 January 2021– it did not initially make a difference. Mr W misled the police and police intervention did not break the spell he was under– so it's difficult to see how an effective warning at this time would have made a difference.

But after a few days (six days to be exact) Mr W seems to have had had time to think things through and went into the branch realising, at that point, he was the victim of a scam. So even if HSBC had given an effective warning and evoked the Banking Protocol on 20 January 2021, I don't think it would have made a difference to the first £17,000 payment. I think Mr W would probably have transferred that payment anyway - in the day or days that followed. So I can't fairly instruct HSBC to refund this payment.

But I think by the time the second payment for £25,000 was made (six days later) – Mr W would have had time to think things through and would probably have realised he was the victim of a scam before the second transaction was completed in branch on 26 January 2021. So, I don't think the second transaction for £25,000 would have been made and should be refunded.

Did Mr W have a reasonable basis of belief or could he have done more to mitigate his losses?

I need to consider not just whether Mr W believed he was sending money under instruction from HSBC's fraud department, but whether it was reasonable for him to do so. I've thought about the steps Mr W took to reassure himself about the legitimacy of the transactions and whether it was reasonable for him to proceed with the payments.
This was clearly a sophisticated scam. Mr W says the original spoofed call was on his landline and he used his mobile to verify the individual calling the number of the back of his bank card. But Mr W's testimony does not quite reflect what I can see on the mobile call history provided.

That history suggests he was called on his mobile from a spoofed HSBC number which matched the number on the back of his bank card. But I don't think the mobile call history shows that *he called* the number on the back of his card to verify the individual. And if he had done – then I think on balance, HSBC would have a record of that call. It is of course possible he did dial the 0800 number on the back of his card from the landline, whilst fraudsters were still on the line and it might have seemed that he'd got through to HSBC – but I don't think he ever got through to the genuine HSBC.

I accept that Mr W was called by a spoofed number and don't doubt the possibility that this was initially on his landline. As I've said, the mobile call history suggests he was called by the number of the back of his bank card on 19 January 2021. The history indicates Mr W then made an outgoing call (possibly tying in with his testimony that he verified the original caller) to a 0345 number. This number is not officially recognised as the bank's and I feel it's likely the number was given to him during the initial call with the scammer - as a way to verify the caller. Of course, this number took him through to a second person involved in the scam - who was able to give a password that the first person would be able to confirm.

So, Mr W was called by a spoofed HSBC number which matched the number on the back of his card, and he believed he had verified the caller by making an independent call. He says he was given a password which the scammer was able to confirm. So, I don't agree with HSBC that '*he didn't do any checks'.* In the moment of a call like this, I think it might have been difficult to start making more extensive checks when what he had seen seemed - at first glance – genuine and verified.

It is also worth noting that whilst HSBC considers Mr W did not do enough checks. There is no standard of care or specific responsibilities placed on customers via the Code, and in any event, the Code does not bind customers. This is something the Lending Standard Board pointed out in its 2022 Review of adherence to Contingent Reimbursement Model Code https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/09/CRM-22-Summary-report-Final-0922.pdf

That said, the transactions in dispute were not made during the initial scam call. Mr W was not under immediate pressure to make the payments. In my view, there was a lot of activity and time for reflection between the call on 19 January 2021 and when the first transfer was actually made on 21 January 2021.

I think there was time in the two days that followed to reflect on what he was being asked to do and there were a number of red flags that ought to have caused Mr W concern about the person he was dealing with and what he was being asked to do.

- Mr W had time to reflect on his mobile call history and check the number he had actually dialed to verify the individual - which did not match the number on the back of his bank card. A quick internet search of the 0345 number does not reveal any links to HSBC or bring up any official bank pages. In fact, the first result does show the number could potentially be connected with a scam.

- I think there was time to question why the fraud department couldn't have made the transfers themselves and why it needed his help.

- The initial payment was blocked and whilst the conversation Mr W subsequently had with HSBC's genuine fraud department on 20 January 2021 doesn't amount to it giving an effective warning, there were points within that call that ought reasonably to have caused Mr W concern. In particular he had had a call from his bank - HSBC and had been asked to transfer money. I think some of these points ought to have resonated with what Mr W was being asked to do by the scammer. He had time to reflect on that conversation too – before the payment was actually made the following day.

- He was asked to share his computer screen with the 'fraud department' and download software so they could take control, but he didn't question why the bank couldn't access all his banking details without the need to take control of his computer. I think this request ought to have caused concern.

By his own admission during the call with the bank on 19 February 2021 - when he realised he'd been scammed - Mr W said there were a lot of things he didn't understand, a lot of things didn't make sense. He acknowledged he was being asked to do 'some stupid things' and that he did 'some stupid things'. He says he knew something wasn't right but kept going back to the fact that he'd spoken to the fraud department. But overall, I don't think that was enough to disregard some of the clearer warning signs here.

I therefore feel it is appropriate to reduce the amount of redress HSBC has to pay the Mr W on the £25,000 transaction by 50%.

Did HSBC do enough to recover Mr and Mrs W's funds?

I've thought about whether HSBC took reasonable steps to recover Mr and Mrs W's funds once it was made aware, Mr W was the victim of a scam.

The scam payments were made on 21 January 2021 and 26 January 2021. According to HSBC notes, Mr W reported the scam to HSBC on 3 February 2021 at 16.40. HSBC has now confirmed it first contacted the beneficiary banks on 19 February 2021 in accordance with its internal note at 17:44 confirming that the beneficiary bank had confirmed no funds remained. The same note suggests an email was sent to the beneficiary bank of the first transaction and it appears the remaining £4 were recovered and returned to the consumer at this time.

So, HSBC did not contact the receiving bank within reasonable time scales. The Best Practice Standards which I understand HSBC is signed up to, says banks should contact the receiving bank 'immediately'. But it contacted the receiving banks over two weeks after Mr W reported the scam.

I have considered whether HSBC's delay in recovery made a difference. But I don't think it does – as the money for both transactions was removed almost immediately (except for the £4 recovered and returned). I understand that Mr W didn't know he was the victim of a scam before 3 February 2021, but the delay means any recovery action would not have been successful at that point.

Putting things right

In order to put things right for Mr and Mrs W, I require HSBC UK Bank Plc to:

Refund 50% of the second transaction (so £12,500) with interest from the date of transfer to the date of settlement.

Interest should be paid at the originating account rate.

It's not clear based on the information HSBC has provided - but I understand Mr W cashed in an ISA to fund the transaction. So, I think fair compensation should reflect the position he would have been in (as closely as possible) had the funds remained there.

Mr W confirmed his ISA has been cashed in and reinvested elsewhere. I assume Mr W will be able to pay the refunded amount back into a Cash ISA elsewhere if he chooses to do so.

My final decision

My final decision is I uphold the complaint in part and require HSBC UK Bank Plc to put things right for Mr and Mrs W as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W and Mrs W to accept or reject my decision before 21 April 2023.

Kathryn Milne
Ombudsman