Before the Arbiter for Financial Services

Case ASF 053/2026

NS

('Complainant')

Vs

HSBC Bank Malta plc

Reg. No. C 3177

('Service Provider' or 'HSBC' or 'Bank')

Sitting of 06 November 2026

Complaint

This is a complaint[1] concerning a fraudulent payment made from the account of Complainant to third parties from her account held with the Service Provider.

The Arbiter is dealing with several such complaints, which while differing on certain details, contain many things in common:

1. The payment will be for an amount generally under €5,000 so that it does not get blocked for exceeding the daily limit of payments agreed between the Bank and a retail customer.

2. The fraudster manages to penetrate the means of communication normally used between the Bank and the customer, usually by SMS or e-mail.

[1] Pages (p.) 1 - 6 and attachments p. 7 - 37

3. The fraudster includes a link in his message and invites the customer to click on the link to make a 'validation' or 're-authentication' of his account.

4. Despite several warnings issued by the banks and the Regulator not to click on such links as banks do not send links in their messages, and that the customer should communicate with the bank only through the official App and/or Website through the credentials that the bank gives to customers, the customer inattentively clicks on the link.

5. Thereafter the fraudster somehow manages to penetrate the customer's account and make a transfer of money generally on a 'same day' basis that goes to the fraudster's account, usually to a bank account in Ireland or a Baltic country from where it is almost impossible to make an effective recall of funds once the customer reports to his bank that he/she has been defrauded.

6. As a result, discord develops between the bank and the customer as to who is responsible for bearing the burden of fraudulent payment. The customer claims that the bank did not protect him when they allowed a communication channel normally used between the bank and the customer to be penetrated by the fraudster and that the bank should have noticed that it was a fraudulent payment because the customer generally does not have a history of such payments. The bank maintains that the responsibility lies entirely with the customer because through gross negligence he has given the fraudster access to his account's secret credentials and thus facilitated the fraud.

In this particular case, the following are the relevant details:

1. On 26 October 2025 at 09:23, the Complainant received the fraudulent message on the mobile by SMS where she usually receives notifications from HSBC. It stated that there was a new pending transfer on her account and if

it was not authorised, she was invited to press a (fraudulent) link or call the normal customer service number of the Bank[2].

2. As the Complainant felt that this was a genuine message from HSBC, she clicked on the link contained in the SMS and gained access to a website which she thought was that of HSBC because it seemed identical.

3. Once on the website, the Bank holds she must have inputted her credentials including secret codes and One Time Password (OTP) which enabled the fraudster to log into her real internet banking at 10:34[3]. Complainant denies giving or inputting such confidential data.

4. She then received a further fraudulent communication of the false website inviting her to press an icon 'Cancel Transfer' purporting she was thus cancelling a payment of €2,500 to Joseph Borg.[4] After pressing to cancel the transaction, she was directed to generate and input an OTP.

5. Soon after inputting the OTP, she received a message from HSBC at 10:37 confirming a payment of €9,000 subject matter of this complaint[5]. HSBC timeline shows the payment was executed at 10:37[6].

6. She contacted HSBC to report the fraud at 11:01[7], blocked her account and made a report to the police at 12:11 hours[8].

   NOTE: times in the evidence are on UTC standard but here local times are being indicated.

7. This payment was done through SEPA Instant Payments to a beneficiary named MEHMET ALI GENGEC[9].

[2] P. 25
[3] P. 85
[4] P. 29
[5] P. 25
[6] P. 85
[7] P. 89
[8] P. 21
[9] P. 158

8. No details about any attempt to recall were provided. However, as this was an Instant Payment, it is unlikely that any recall attempt, if made, would have been successful.

9. Complainant seeks a refund of the remaining balance of €7,200, as HSBC have already made a refund of €1,800 on an ex gratia basis.[10]

The Complainant submitted that the Service Provider let her down because:

> ***"I believe HSBC failed in its duty of care by not providing adequate protection against a sophisticated fraud and by placing the full responsibility for the loss entirely on me.***
>
> ***The fraudulent communication originated from HSBC's official SMS messaging number, the same channel through which I normally receive genuine bank notifications. This significantly reduced my ability, as a customer, to recognise the message as fraudulent and created a legitimate sense of trust.***
>
> ***In addition, the one-time passcode (OTP) was requested in misleading context, as I reasonably believed it was required to cancel a transaction rather than to authorise a high-value instant transfer.***
>
> ***The transfer of approximately €9000 was highly unusual and inconsistent with my normal account activity, yet no effective safeguards or enhanced verification measures were applied before the funds were irreversibly transferred.***
>
> ***For these reasons, I believe HSBC's decision to classify the transaction as fully authorised and to deny full reimbursement is unfair and disproportionate.*** [11]***"***

[10] P. 4; p.42
[11] P. 4

Service Provider's Reply

Having considered in its entirety, the Service Provider's reply,[12]

Where the Service Provider explained and submitted the following:

> ***"The Respondent respectfully submits that the Complaint submitted by (Complainant) is unfounded and ought to be rejected on account of the following reasons:***
>
> 1. ***The Complainant had the global sum of €9,000 debited from her Savings account bearing number 0x6-xxxxxx-0x0 allegedly without her authorisation after she accessed a malicious link impersonating HSBC and inserted her credentials, thus facilitating the fraud.***
>
>   ***The Complainant called on same Bank to take action so as to remedy the fraud perpetrated on the Complainant.***
>
> 2. ***It is submitted that the Complainant manifested gross negligence on her part, when she disclosed personal banking credentials despite the Bank's repeated calls for customers to refrain from parting with one's credentials. It was solely as a result of this disclosure, that access to her accounts was rendered possible and the fraud accomplished.***
>
> 3. ***It goes without saying that each account holder is responsible for safeguarding, and barring disclosure of, one's own bank security credentials. This is also a contractual obligation the customer undertakes with the Bank; under the General Terms and Conditions of Savings and Current accounts, Section A.4 'Checking it is you and keeping your account secure', it is made clear that customers "*must be very careful to keep…. security details private and not let anyone get access to any devices you use to make payments.*" That is, customers are responsible for safeguarding their personalised***

[12] P. 41 - 42 with attachments P. 43 - 79

security credentials and must not disclose them to third parties (Doc 1).

The Bank reiterates that customers are repeatedly warned never to share OTPs, PINs, passwords, or security devices with third parties. The disclosure of such credentials is bound to invite occasion for loss.

4. ***It is pertinent to note that the Bank regularly issues fraud awareness communications to its customers. Between 17 and 22 September 2025, (that is to say, only month before the incident) the Bank sent the customer an email containing information on fraud awareness, explicitly stating that the Bank would never ask customers to share PINs, banking passwords, or security codes so that it is no defence on the Complainant's part that the Bank did not reach out to customers to supply them with adequate warnings. The Bank also regularly disseminates fraud awareness information through its website and social media channels. (Doc 2).***

5. ***The Bank was fully compliant with the law and its obligations; the smishing attack is not an event the Bank can prevent – the Arbiter has already determined that. The Bank's role and obligation is to issue adequate warnings to customers in order that customers are reminded of their obligation to not disclose. As premised above, this obligation on the Bank's part was met in full.***

6. ***The complaint itself filed with the Arbiter evidences that (Complainant) is capable of understanding information provided to him and capable of making independent decisions.***

7. ***The Bank, strictly on a without prejudice basis, already remitted to (Complainant), the sum of €1,800 which corresponds to 20% of the value of the transaction in question (as confirmed by the Complainant in Section D of the Complaint Form).***

That, in view of the above considerations, the Bank respectfully submits that the complaint's claim is unjustified in fact and at law and that consequently all

Complainant's demands are to be rejected with costs to be borne by the said Complainant.[13]***"***

The Hearings

A **first hearing**[14] was held on 08 June 2026 for the evidence of the Complainant where she largely repeated her case as above explained.

On cross-examination, she insisted she disclosed only one OTP, that which she generated to purportedly cancel the payment of €2,500 to Joseph Borg and instead it was used to authorise the fraudulent payment subject of this complaint.

On being pressed by the Bank that she must have disclosed another OTP that permitted the fraudster to get access to her account through internet banking, the Complainant insisted that, as far as she can remember, she only opened an OTP once[15].

Second hearing

A further hearing was held on 10 September 2026 for the evidence of HSBC[16].

Kenneth Attard explained (making reference to a schedule attached to their email dated 07 September 2026[17]):

> ***"So, this is what happened on the 26th of October 2025.***
>
> ***I explain that the lines highlighted in yellow are activities belonging to the fraudsters, while the white lines are activities done by Complainant.***
>
> ***It is clearly seen that all her activity was on mobile. The first line shows that she pressed the Generate Security Code and the Transaction Verification to generate the OTP. And she inserted them in the fake website after she had clicked on the link.***

[13] P. 41 - 42
[14] P. 80 - 83
[15] P. 82 - 83
[16] P. 86 - 90
[17] P. 84 - 85

At that very same time, the fraudster took the OTP and, on a browser, he entered it on the real website, the website of HSBC, and logged in.

On the third line, she was prompted to cancel the payment because that is what she had recalled, and she got a pop-up. There, she generated another OTP on her mobile with the last five digits of the fraudulent IBAN, and also the number of the amount. The fraudster took again the OTP, put it on a browser and, at that point in time, the transfer was made.

The exact sequence of events is clearly visible.

The Arbiter understands that there were two inputs of confidential data. Two OTPs: the first one to gain access to the site and the second one to authorise the payment.

I say, yes, exactly. In fact, it is clearly seen that the second time the OTP was generated was for the Payment to New Beneficiary- International (Me to Not Me). This OTP was generated with the last 5 digits of the IBAN and the number of the amount which, in this case, was €9,000.

And that code could only have been generated by (Complainant). In fact, it can be seen that it was generated on a mobile.[18]***"***

On being cross-examined, Kenneth Attard stated:

"Asked when I mention the mobile browser whether I am referring to the mobile browser or I am referring to the App, I say that the mobile is the Mobile App which (Complainant) was using, while the browser is the fraudster putting in on the real website.

It is said that from the logs that I shared, it can be seen that in the first line there is MT DSP Mobile.

Asked whether this refers to the App, I say, yes.

[18] P. 86 - 87

It is said that logging in the App does not require any User ID or OTP code since (Complainant) can access the App using Facial ID.

I say, yes, but you still generate the OTP even if you access it with the face ID. You cannot log in without generating an OTP because then you get the OTP and you put it on the browser. It is impossible for the fraudster to have logged in without an OTP.

It is said that when you log in using the app, you have three different options. You can enter into your account using the face ID. You can enter by the PIN, and then you have the third option on the bottom page where you can select the OTP. And OTP codes are really different between the login OTP, the transaction OTP.

I say that (Complainant), in order to be able to generate the OTP, had to press on Generate Security Code and then choose Transaction Verification. Once she had done that, she would either have inputted a PIN or her biometric, whatever, and the OTP is generated. Once the OTP is generated, it was displayed and she entered it on the fake website, and the fraudster took it from there and inserted it on the browser. It is very clear how it was done: Mobile, Browser, Mobile, Browser, Mobile, Browser, exactly in sequence.

So, she generated when there is Mobile and put it on the fake website. The fraudster took it away, put it on the real genuine HSBC website, logging in her name. Then she generated the second time; the fraudster again took it from the fake website, put it on the genuine website and made the transfer.

It cannot be clearer than what we can see on screen.

(Complainant)says that she is 100% sure that what she used was one unique OTP code to cancel the transaction of €2.5K. She always accesses it using the Mobile App, using the face ID and does not put any code or username or password.

I am asked why I stated that Complainant used two OTPs when in the logs, one can only see one statement stating that the OTP and password were successful while there is no other OTP for the other Payment New Beneficiary International (Me to Not Me).

I say that the first line, at 09:25, is where she generated the first OTP.

At 09:34, the fraudster entered that OTP into the browser.

At 09:35, where there is Authentication Successful, is when she generated the OTP and the fraudster then entered this OTP. It is practically impossible to log in without the generation of OTP.

I confirm that it is absolutely impossible and there is no cause for a discrepancy between the sequence of events and the log I submitted.[19]***"***

It was explained that the quoted times are UTC and local times should be increased by one hour.

On being questioned, the Bank's legal representative explained that as explained by the Arbiter in his decisions, the Bank has no means to control spoofing. He also confirmed that evidence of warnings to clients not to press links were attached to their official reply, but direct SMS messages were only sent after the date of the event of this complaint.

The Arbiter requested the Bank to submit copies of the Complainant's accounts with HSBC for a whole year before the event[20]. From examination, the Arbiter could trace only one SEPA transfer to a third party for €5,056.61 on 12 March 2025[21] which the Complainant explained was a payment to a local notary in respect of purchase of property financed through an HSBC loan[22].

[19] P. 87 - 88
[20] P. 92 - 158
[21] P. 149
[22] P. 160

Final Submissions

In their final submissions, the parties largely repeated what had been revealed in the complaint, the reply and the evidence during the hearings.

Consultation of the Malta Communications Authority

For the Arbiter to understand the technological intricacies on how a fraudster can impersonate the Bank to defraud clients, he invited the Malta Communications Authority (MCA) security expert for consultation.

It was explained that this type of fraud, technically known as *Spoofing* and *Smishing* or collectively as *Social Engineering Scams,* does not allow the bank to take any precaution (other than effective warnings for customers to be careful) so that the fraudster cannot use this communication channel to defraud customers.

Analysis and consideration

The Arbiter is of the opinion that for the sake of transparency and consistency, to arrive at a fair decision on such complaints, it would be appropriate to publish a framework model on how to apportion the responsibility for fraud between the bank concerned and the defrauded customer by taking into account factors that may be particular to each case.

To this end, the Arbiter is attaching to this decision a framework model that he published to be used to reach a decision on how to apportion the consequences of fraud. The model also contains several recommendations for banks to further strengthen consumer protection against increasingly capable and creative fraudsters.

But the Arbiter feels the need to strongly emphasise that while it is true that banks do not have a means of prohibiting *spoofing/smishing* in the channels of communication they use with customers, they are not doing enough to sufficiently warn customers to be careful; not to click on links contained in these messages even though it appears to be coming from the bank concerned on the medium that the bank normally uses to send messages to customers.

It is not enough to make continuous announcements on their website. It is not enough to issue warnings on mass media or social media. The consumer is busy with daily problems, and it cannot be claimed that by making a notice on the website, in the traditional media or TV, or on the bank's Facebook page, the consumer is sufficiently informed. In serious cases of such fraud, it is necessary for banks to use direct communication with the customer by SMS or email. This aspect is one of the factors included in the framework model.

On the other hand, the Arbiter understands that should the client err by clicking on a link that he has been warned not to as it could be fraudulent, this does not automatically fall into the category of gross negligence according to law. The European Court of Justice (CJEU) in the case of Wind Tre and Vodafone Italia[23] makes reference that it would not be negligent in a gross grade if it happens even to an average consumer who is reasonably informed and attentive. The Arbiter sees complaints from complainants who easily fall into this category.

After all, PSD 2 makes it clear that the consumer must give his consent to the specific payment, and it is not enough that there is general consent as contained in any Terms of Business Agreement. Banks therefore need to have a sufficiently robust payment system so that payment is not processed unless it is specifically authorised by the customer. Banks cannot escape responsibility if they leave holes in their systems whereby the fraudster can, without further involvement of the customer, make a specific authorisation of the payment in favour of the fraudster. This fact is also included in the model.

The model also considers any applicable particular circumstances of the case. There may be circumstances where the fraud message looks less suspicious. Circumstances where the customer is in negotiations for a bank loan or the customer is abroad and is carrying out transactions that are not customarily carried out by them, thus, reducing the customer's suspicion that the message received may be fraudulent.

[23] Decision 13 September 2018 C-54/17

The model also considers whether the Complainant is familiar with the bank's online payment to third party systems by having made any similar (genuine) payment in the previous 12 months. This also helps to form an opinion on whether the monitoring of payments system which the Bank is bound to make (as explained in the model) is effective.[24] [25]

Decision

The Arbiter shall decide, as provided for in Article 19(3)(b), by reference to what he considers to be equitable, fair and reasonable in the circumstances and substantive merits of the case.

When the Arbiter applies the model proposed for this particular case, it arrives at this decision:

[24] (EU) 2018/389 of 27 November 2017 RTS supplement PSD2 EU 2015/2366 Articles 2(1) and 2(2)
[25] PSD 2 EU 2015/2366 Article 68(2).

	Percentage of claim allocated to Service Provider	**Percentage of claim allocated to Complainant**
Complainant who has shown gross negligence	0%	100%
Reduction because they receive fraud message on the channel normally used by the Bank	50%	(50%)
Increase because the Complainant cooperated fully in making the complained payment	(30%)	30%
Increase because they had received a direct warning from the Bank in the last 3 months	0%	0%
Sub-total	20%	80%
Reduction to special circumstances	20%	(20%)
Reduction for absence of similar genuine, monthly payments in the last 12 months[26]	0%	0%
FINAL TOTAL	**40%**	**60%**

[26] P. 149

Therefore, according to the framework model, the Complainant should bear 60% of the loss and the other 40% should be borne by HSBC.

The model finds that the Complainant continued to cooperate with the fraudster by disclosing her credentials, believing she was cancelling rather than authorising a payment. Although Complainant said she did not remember inputting OTP twice, the probabilities are that she did, otherwise the fraudster would not have both accessed her internet banking and then, authorised the payment for which two distinct OTP's were necessary.

The model partially excuses the Complainant as she had not received a direct warning from HSBC about these fraudulent schemes in the months before this case and thus offers her 20% compensation.

The Arbiter finds the warning given about the introduction of Instant Payments as insufficiently forceful and direct and it was lost on page 8 of a 10-page circular[27]. In the Technical Note attached to this decision, the Arbiter had urged banks to send direct SMS on a quarterly basis to their customers reminding them not to press on links even if they appear on the same channel used by banks for normal communications. HSBC admit they started doing so only after this event had happened.

The Arbiter's model further switches another 20% responsibility on to the Bank as he considers that there are special circumstances which justify the allocation. In fact, the Arbiter feels that special circumstances explained below should increase the allocation to 40% for these reasons:

1. Customer had untypical payments limit of €25,000 on the day of the incident.[28] The maximum payment observed in the statement was €5,056 to a local notary. In the circular to announce the benefits of Instant Payments, HSBC should have informed their customers to revisit their payments limit as

[27] P. 70 - 79
[28] P. 91

whilst the system had technical benefits, it also had exposure to risks especially for clients holding high payments limits.

HSBC should have informed clients that they have the facility to modify their instant payments transfer limits at any time and at their sole discretion[29].

2. The Bank's monitoring system was not sensitive enough for the abnormality of such foreign third-party payment for an untypically high amount in the days after the introduction of Instant Payments.

3. Whilst the model penalises Complainant 30% for continuing to co-operate with the fraudster to authorise the payment, the Arbiter sees a case for reducing her gross negligence allocation considering that the Complainant believed she was stopping rather than authorising a payment.

Taking the above into account the Arbiter's final allocation of responsibility is as follows:

[29] Article 5a(6) of regulation EU 260/212 as inserted by the Instant Payment Regulation EU 2024/886

	Percentage of claim allocated to Service Provider	**Percentage of claim allocated to Complainant**
Complainant who has shown gross negligence	0%	100%
Reduction because they receive fraud message on the channel normally used by the Bank	50%	(50%)
Increase because the Complainant cooperated fully in making the complained payment	(30%)	30%
Increase because they had received a direct warning from the Bank in the last 3 months	0%	0%
Sub-total	20%	80%
Reduction to special circumstances	40%	(40%)
Reduction for absence of similar genuine-monthly payments in the last 12 months	0%	0%
FINAL TOTAL	**60%**	**40%**

Thus, in terms of Article 26(3)(c)(iv) of Cap. 555 of the Laws of Malta, the Arbiter is ordering HSBC Bank Malta p.l.c. to pay the Complainant the sum of five thousand, four hundred euro (€5,400) being 60% of the fraud payment of €9,000. This amount is inclusive of the ex gratia payment of €1,800 already effected, thus, a residual payment of €3,600 is applicable.

Payment must be made within five working days of the date of the decision. Otherwise, interest at 2.65%[30] starts to run from the expiry of the five days to the date of effective payment.

Since responsibility has been allocated between the parties, each party is to carry its own expenses.

Alfred Mifsud
Arbiter for Financial Services

<u>Information Note related to the Arbiter's decision</u>

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

[30] Equivalent to the Main Refinancing Operations (MRO) interest rate fixed by the European Central Bank.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.