Before the Arbiter for Financial Services

Case ASF 010/2024

ZG

('Complainant')

Vs

Bank of Valletta p.l.c.

Reg. No. C 2833

('Service Provider' or 'BOV')

Sitting of 18 July 2024

This is a complaint concerning a fraudulent payment made on behalf of the 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 email.

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 7 November 2023, the Complainant received the fraudulent message on the mobile by SMS where she usually receives notifications from BOV.

2. As the Complainant felt that this was a genuine message from BOV, she clicked on the link contained in the SMS and gained access to a website which she thought was that of BOV because it seemed identical. At the time, she was travelling in Vienna and was concerned that failure to unblock her account by pressing the link would not allow a debit to card account for an accommodation booking made on *booking.com*

3. She went step by step with all the instructions given to her by the fraudster and thus entered the details to make a payment of €3,456.

4. This was done to the fraudster's bank account in Ireland and the fraudster had placed instructions to make the payment 'same day'.[1]

5. The payment included false name (Samantha cloke) and address of the beneficiary (15 pitkali Attard ASD 6732) as well as false reason for payment (For family xmas presents xx) in order to reduce the risk of the payment being blocked by the Bank's transaction monitoring systems.[2] [3]

6. Soon after completing what she thought was a re-validation to unblock her account, she received from BOV an alert message informing her of a debit charge to her account for €3,456.

7. She tried to contact BOV on the number indicated in the message but could not make contact before 3 hours later. By then, it was too late to stop the transaction. In the meantime, she attempted to communicate with the Bank via email.[4]

8. The Bank maintains that following log-in at 10:14 hours, the payment was duly authorised as a same day transfer by 10:17, and log-out was effected at 10:22.[5] Furthermore, the Service Provider maintains that as the payment was categorised as **immediate same day,** it could not be stopped once properly authorised. The SMS from the Bank with confirmation of the payment was reportedly received by the Complainant at 10:57 hours.[6]

9. A recall[7] was made by BOV on same day at 14:10 hours both to recipient bank (Revolut) and intermediary bank (UNCRITMMXXX _ Unicredit) but this was unsuccessful except for a refund of €2.07 received on 12 December 2023

[1] Page (p) 24
[2] P. 18 - The SEPA system moves strictly according to IBAN number and, so far, does not connect to the name and address of the beneficiary as stated in the transfer.
[3] P. 24
[4] P. 13
[5] P. 41
[6] P. 3
[7] P. 91

10. The case was reported to the police in Vienna for further investigation of the fraud.[8]

11. Complainant seeks a refund of €3,485.93 being amount scammed of €3,456 less recovery of €2.07 plus €32 charges. Following filing of complaint, Complainant was charged a further €50 being charges by Unicredit for the recall.[9]

The Complainant submitted that the Service Provider let her down for three reasons, being:

1. That it is obvious that BOV does not provide sufficient internet or online security to its clients;
2. That customer service was not available in case of an emergency; and
3. That there was incompetence in the handling of her complaint.

Having considered, in its entirety, the Service Provider's reply, including attachments,[10]

Where the Service Provider explained and submitted the following:

1. *Whereas in her complaint Ms. ZG ("the complainant") states that "on 7.11.2023 I received an SMS from 'BOV Mobile' asking me to verify the mobile signature of my debit cards. ... I followed the link as provided in the SMS and all given instructions.[11]" She then explains that she received an SMS from BOV informing her that her account was debited with 3456 EUR and she realised that she had fallen for a scam. Therefore, she is expecting the Bank to refund her the amount she lost as she states that the transaction was caused by "BOV's obvious lack and negligence of Internet/online security-proof."[12] The Bank submits that this claim is*

[8] P. 20 -22
[9] P. 97; 104
[10] P. 33 - 40 with attachments P. 41 - 93.
[11] Fol. 003 of the complaint.
[12] Fol. 003 of the complaint.

unfounded as will be explained throughout this reply and throughout the proceedings.

2. *Whereas the complainant attached the details of the transaction in question, bearing reference number 2331110037017000-1623518972. According to the Bank's records, this transaction was duly authorised on the 7th of November 2023 at 10:17.*[13] *As part of the Bank's security system which is in line with the Payment Services Directive 2 (PSD 2), there are various levels of authentication to ensure that the transaction was carried out by the complainant, from credentials and systems registered in her name. In fact, this transaction had no indication that it was fraudulent.*

3. *Whereas article 40(1) of Directive 1 of the Central Bank of Malta (which Directive is based on the PSD2) provides that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. As explained, the Bank received legitimate instructions from credentials associated with the complainant and therefore has no obligation to refund the complainant.*

4. *Whereas the Bank implemented the necessary measures to ensure that its systems are secure and in line with the PSD 2 which provides the following on 'strong customer authentication':*

   *"**strong customer authentication'** means an authentication based on the use of two or more elements categorised as **knowledge (something only the user knows), possession (something only the user possesses)** and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;"*[14]

5. *Whereas apart from strong customer authentication, the Bank implements also a system of 'dynamic linking' as outlined in the*

[13] 'DOC.A': Records of the internet banking of the complainant regarding the transaction in question.
[14] Article 4(30) of PSD2.

Commission Delegated Regulation (EU) 2018/389, which supplements the PSD 2. Article 5 provides the following:

"*Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:*

a) the ***payer is made aware of the amount of the payment*** *transaction and of the payee;*

b) the ***authentication code generated is specific*** *to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;*

c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to ***the identity of the payee agreed to by the payer****;*

d) any change to the amount or the payee results in the invalidation of the authentication code generated."

6. *Whereas the complainant was not only aware of the amount of the transaction, but also inputted it herself in her token which is whether her BOV app or the physical internet banking key (this is the element of possession of strong customer authentication). Besides this, she also inputted the lasts digits of the lBAN number of the recipient, and this satisfies the element outlined in article 5(c) above mentioned. Upon entering these details, a code would have been generated which needs to be used to approve the transaction.*

7. *Therefore, it is completely incorrect and unfounded for the complainant to say that "BOV does not provide sufficient internet/online security to its clients."*[15] *This due to the fact that the Bank adheres to the above-mentioned Directive and Regulation and implements the process of strong customer authentication and dynamic linking to ensure that a*

[15] Fol. 003 of the complaint.

customer is completely informed of what he is doing, that is, approving a payment.

8. *Whereas this payment was approved by the confidential details of the complainant with the use of her token. The Bank had no control over this transfer because it was completely in the control of the complainant without the Bank's intervention. Once the Bank receives legitimate instructions for a "third party payment" from the adequate channels, the Bank implemented them, as it is reasonably expected that the only person who has access to such confidential details and systems is the person with whom they are associated. In fact, this is outlined in the terms and conditions of the Internet Banking system (attached and marked as **'DOC.B'**) which provide the following:*

   "You authorise us to act on any instruction that we receive through the Channels which has been, or reasonably appears to have been, sent by you and which, where applicable, has been sent using your Security Number/s or BOV Mobile PIN or biometric data."[16]

   *"All payments, instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your Boy Secure key security number or numbers ("Security Number/s"), or input your BOV Mobile PIN ("BOV Mobile PIN"), or input your biometric data, are deemed as **binding** on you."*[17]

9. *Whereas in fact, every token used to generate codes in order to approve a payment has a certificate associated with it. In fact, the certificate number associated with the token with which the payment in question was approved is the same one associated with the token of Ms ZG which she has previously used to make other payments which she is not contesting the legitimacy of. This can be seen from the document attached and marked as **'DOC.C'**.*

10. *Whereas besides the fact that the payment was duly authorised, there is also the fact that the transaction amount was within the limit imposed*

[16] DOC.B: 'BOV 24x7 Services – Important Information and Terms and Conditions of Use' Page 5.
[17] *Ibid*., Page 4

for these kinds of transactions. With respect to the transaction in question in this arbitration, which is a 'third-party transaction' the limit is five thousand euro, as can be seen in the highlighted section in the document attached and marked as ***'DOC.D'*** *(this document is accessible from the Bank's website.) Therefore, there were no suspicious signs for the Bank with respect to this transaction. One should also note that the PSD 2 does not oblige the Bank to impose any limit on transactions. It only stipulates that if there is the possibility to put in place spending limits, the customers should be informed of this.*[18]

11. *Moreover, the above-mentioned Commission Regulation provides that the Bank can decide to not apply strong customer authentication for transactions which are considered to have a low level of risk.*[19] *Therefore, one can conclude that when a transaction is considered to be of a higher risk, (because for example it is not of an amount normally done by the customer), the Bank should implement the use of strong customer authentication, which was in fact done in this case.*

12. *Whereas without prejudice to the above, if the complainant is alleging that this transaction was not authorised by her and has evidence of this, then the Bank is still not obliged to refund her since even if she did not have the intention to approve a payment, she still followed the necessary steps to approve it. In this respect the Bank refers to article 45 of Directive 1 of the Central Bank of Malta, particularly to the article entitled* ***'Obligations of the payment service user in relation to payment instruments and personalised security credentials'*** *which provides the following:*

> *45. (1) The payment service user entitled to use a payment instrument shall:*
>
> *a)* ***use the payment instrument in accordance with the terms governing the issue*** *and use of the payment instrument, which must be objective, non-discriminatory and proportionate;*

[18] Article 28(2) of Directive 1 of the Central Bank of Malta which reflects article 52(2) of the PSD 2.
[19] Article 18 of Regulation (EU) 2018/389

(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, ***take all reasonable steps to keep its personalised security credentials safe****.*

13. *Whereas article 50(1) of the Directive provides:*

The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or ***gross negligence****.*

14. *Whereas if the complainant is alleging that the transaction was not authorised by her, this means that she generated the necessary codes for the payment to be approved and passed them on to a third party. In order to generate such a code, she had to insert the amount of the transaction and the last 5 digits of the recipients' IBAN. This fact should have raised suspicion within the complainant since if she had no intention of approving a payment, then it would have been reasonable for her to take action and ask herself why she was being asked to input an 'amount' and a 'payee code' which she accessed from a section entitled 'transaction signing'.*[20] *She could have confirmed this doubt with the Bank who would have immediately informed her that the SMS was not genuine.*

15. *The fact that she provided all these details and followed all the necessary steps, goes against the terms and conditions of the internet banking service which provides the following:*

"You must take all the reasonable precautions to prevent the loss, theft or fraudulent use of the BOV Securekey, the Security Number/s, the BOV Securekey PIN, and/or the BOV Mobile Application, the BOV Mobile Authentication Software, biometric data, the BOV Mobile PIN, as applicable. You undertake not to record your BOV Securekey PIN and/or BOV Mobile PIN in any easily recognizable form and to keep said PINs separate from the BOV Securekey and/or the mobile device. You must make every effort to prevent the BOV Securekey, the Security Number/s, the BOV Securekey PIN and/or the BOV Mobile Application, the BOV

[20] DOC.E – Demonstration of screen used for approval of transaction

Mobile Authentication Software, the BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party."[21]

16. Whereas as a voluntary user of the internet banking service, the complainant knows or ought to have known that this service can only be accessed from the Banks' website or from the BOV Mobile App. Whereas the Bank never before requested the complainant (or any other *customer) to access her internet Banking from a link in an SMS, because it has the adequate systems for this service to be accessed. In fact, the Bank warns customers to be careful what information they disclose, particularly on links. In fact, in May 2014, the published 'Tips for Safer Mobile Banking" which amongst other provide the following:*

    - *"Watch what you send: never disclose, either via text, email, or through a website, any personal information such as account numbers, passwords, or personal info that could be used by unscrupulous persons to gain unauthorised access to your bank accounts.*

    - *Do not trust links or attachments that originate from people you do not know. If a person you do know has sent you a link or attachment, check with them that it is legitimate before opening it."*

17. *Whereas as can be seen from this extract, the Bank warns customers to be careful and confirm if a link is genuine, even if they know the person who sent it to them, and this to avoid incidents of fraud.*

18. *Whereas the abovementioned warning is part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. The abovementioned document and others similar to it are easily accessible from the Banks' website and every customer should have an interest of keeping themselves informed and updated on the terms and conditions which regulate a service they voluntarily subscribed to, something which is reasonably expected from all consumers.*

19. *Whereas in May 2023 the Bank published a page entitled 'Spot the Scam: Bank impersonation Scams' which explains that scammers may use a*

[21] DOC.B: 'BOV 24x7 Services – Important Information and Terms and Conditions of Use' Page 7.

technique called 'Spoofing' where "scammers manipulate caller ID or email addresses, so they appear to be from reputable companies such as banks. It can be tough to identify and misleading because it makes people think they are communicating with a trustworthy source. Ask yourself what a bank will NEVER ask you for over the phone."[22] *It also explains what personal details such scam may ask for which indicates that the communication is not genuine. As will be explained throughout the proceedings, the Bank cannot control such incidents of spoofing.*

20. *Whereas the link received by the complainant had indications that it was not the genuine link of the Bank since the URL was BovSupport.com. This fact could have raised suspicion in the complainant which would have led her to use more caution before accessing the link, providing confidential details on it and following instructions provided by this website.*

21. *Whereas in May 2021, the Bank also published on its website a page entitled 'Warning: Scam Alerts' which informs customers that:*

*"**Bank of Valletta does NOT send text messages or messages via social media asking customers to unlock suspended or blocked accounts or provide personal or financial information**."*

22. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams.* ***'DOC.H1'*** *shows a comprehensive list of the posts made by the Bank on social media in the previous 6 months. Moreover, the Bank coordinated TV appearances where Bank employees explained what SMS spoofing is and how to identify it. These programmes aired on the 10th of April 2023, 27th of April 2023 and September 2023. The Bank also published multiple newspaper articles, on various media as can be seen from the attached list marked as* ***'DOC.H2'****.*

23. *Whereas besides information provided by the Bank, there are various entities which make educational campaigns in order to raise awareness concerning fraud which may be directed to consumers of financial services. These include the Malta Financial Services Authority who*

[22] DOC.G: 'Spot the Scam: Bank Impersonation Scams'

provide information on how a person can identify a system where a payment is to be made. Of particular relevance is the page 'The MFSA's Guide to Secure Online Banking'[23] which provides the following:

- *"Use the genuine internet website of the bank. Never access the bank's website through links contained in emails or SMS, unless you are sure of the identity of the sender. It is always best to access the bank's website by* ***typing in the web address, as provided by the bank, directly in the browser****.*
- *Follow the* ***information and guidelines provided by your bank*** *on how to use digital banking services.*
- *Take the necessary time to* ***read the terms and conditions provided by your bank****.*
- *Ensure that you always* ***protect all personal details*** *such as card details, passwords, and other confidential data to access the bank's online platform or mobile app.*

24. *Whereas despite all these warnings, the complainant still carried out all the necessary actions for the payment to be approved and therefore, she breached the terms and conditions of the Internet banking service and this against the above-mentioned article 45(1) of the Directive.*

25. *Besides this, she also acted against article 45(2) of the Directive because she did not take all the reasonable steps to keep her personalised security credentials safe. It is reasonably expected that a consumer is aware of the terms which regulate the contractual relationship by which they are bound and adhered to.*

26. *Therefore, any alleged fraud which occurred due to the participation of the complainant who provided confidential details on a fraudulent website and followed instructions provided by this website. All this contributed to her gross negligence.*

[23] https://www.mfsa.mt/publication/the-mfsas-guide-to-secure-online-banking/

Timeline of Events

27. *Whereas the payment was approved on the 7th of November 2023 at 10:17. This kind of payment is processed immediately as can be clearly seen in the terms and conditions marked as* ***'DOC.B',*** *particularly in the section entitled 'Cancelling or changing a payment instruction' which provides 'If you ask us to make a payment immediately, we cannot change it or cancel the payment instruction because we start processing it when we receive it." The Bank submits that this clause is in conformity with article 80 of the Payment Services Directive 2, entitled 'Irrevocability of a payment order'.*

28. *Therefore, when the complainant called the Bank on the 7th of November at 13:25, the Bank blocked her internet banking and cards. The Bank also made a recall request to the intermediary and beneficiary banks, which request is made through a digital, internal system between Banks. This request was made at 14:10 on the 7th of November to the beneficiary bank and to the correspondent bank. Multiple reminders were also sent by BOV as can be seen from* ***'DOC.I'****.*

29. *Whereas when the complainant called, the customer service representative informed her of the charges associated with the recall of funds and also that there is no guarantee that the recall will be successful, and the complainant consented. He also informed her of the charges associated with the issuing of new cards since her previous ones were blocked. The complainant consented to both these charges.*

30. *The outcome of the recall process depends completely on the bank where the funds were received since they would have their internal procedures and rules and BOV has no control over other banks and therefore cannot dictate how long they take to answer the recall request or what kind of answer they give.*

31. *Therefore, the Bank respectfully submits that it did its utmost to recover the funds and give them to the complainant. In fact, a minimal amount of*

€2.07 was recovered and credited to the complainant's account as she explains herself.[24]

32. *Finally, the Bank submits that it implements measures to ensure that its internet banking systems are secure (in line with EU law). The Bank also makes on a continuous basis, various warnings on scams which may be directed towards its customers. However, this is all futile if customers choose to ignore the terms and conditions of service and any warnings made by the Bank. Thus, the customer cannot expect the Bank to take responsibility for her actions which show gross negligence.*

Conclusion

33. *For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and law.*

34. *Chapter 555 of the Laws of Malta vests the Honourable Arbiter with the authority to decide a case on the basis, inter alia, of the Complainant's legitimate expectations and what he deems fair and equitable in the circumstances of the case. The Bank very respectfully submits that such element of fairness and a customer's legitimate expectations are founded and pivot on a balance between rights and obligations whereby a customer most certainly has rights but also an inherent interest and obligation to faithfully abide with all terms, conditions as well as guidelines issued by the Bank, as these are ultimately intended to serve and protect the customer.*

35. *The Bank reserves the right to bring oral and documentary evidence in order to substantiate the defences raised in this reply, as well as to make submissions both verbally and in writing pursuant to the provisions of Chapter 555 of the Laws of Malta.*

36. *The Bank reserves all rights/actions pertaining to it at law, and respectfully requests the Arbiter to reject and dismiss the complaint's claims."*

[24] Fol.003 of the complaint.

The hearings

Two hearings were held on 22 April 2024[25] and 10 June 2024.[26]

The parties maintained, in their testimonies and submissions, their positions as explained in the Complaint and in BOV's reply.

The Complainant blaming the BOV for allowing the fraudster to penetrate the SMS channel which the Bank normally uses to communicate with her and for not noticing that the payment was a fraud.

"It was not visible to me; I did not notice that I was actually making any payments because all I was asked for was to put in codes, to generate codes."[27]

"I immediately called Customer Care at 11:05 and I did not go through Customer Care until 13:25. In the meantime, I sent an email to BOVCustomerCare.com at 11:05 … And, finally, at 13:25, I managed to go through to Customer Care who then told me that it was too late to stop this payment or to get anything back."[28]

"Obviously, since my cards and my internet banking were stopped, Customer Service at BOV Branch Naxxar reactivated my internet account and for that I received a password which was actually sent to the same message trail in which I received the initial BOV link which was fraudulent.

And this is really when I thought how can I distinguish when I receive a password on the same SMS thread which I had to put into my Mobile App since this is so similar to what happened before? And I actually told the Customer Care Officer that I am not going to insert this link which I received with this password in my Mobile App because what will happen if this is wrong again? She assured me that it was not, but since I won't really be able to distinguish anymore, I asked her to do that for me." [29]

When asked by the Arbiter whether she had made online payments to third parties using the BOV App before this incident, the Complainant confirmed that

[25] P. 94 - 96
[26] P. 102 - 107
[27] P. 94
[28] P. 95
[29] P. 95 - 96

she had done so recently twice before as, normally, she used to make internet online payments using her computer and the hardware token (key) for such payments. In fact, she thought that reactivation as per fraudulent message was needed because she started using the App for online payments.

On being cross-examined, the Complainant stated:

"***Asked whether the bank before 7 November (before I received the fraudulent SMS) ever sent me a SMS with a link in it, I say that I don't think so, I don't remember.***

Asked whether the bank ever asked me via SMS to verify my mobile signatures, I say, no, they never asked me but, as I said last time, I did not use my BOV mobile very much prior to 7 November. There were only a few transactions prior to this message so, for me, there was this connection.

Asked whether before 7 November, BOV ever asked me to access my BOV Mobile App through a link in a SMS, I say, no.

Being referred to the last sitting where I said that I inputted certain numbers and codes, I am being asked where I inputted these. I say that I received an application when I was pressing the link which did not look similar to the Mobile App where there was an instruction to insert something and generate a code which then I had to insert it into a new page which was opened by this link application.

Asked whether I used my Mobile BOV App in this process, whether I accessed the App itself or not, I say, no.

I am asked whether I put any information on the App. I say that I opened the link and a page appeared where I had to give in something, but it was not asking me to open my BOV Mobile App. No, I did not use my App through this process.

Asked whether I am familiar with the terms and conditions of the Internet banking service and whether I read them, I say that I don't know whether I ever read them all in detail. No, probably not.

It is being said that in my complaint, I mentioned that I did a police report regarding this case. Asked whether I ever followed it up with the police, I say that I was not contacted yet by the police. I followed it up with the Arbiter.

I never opened a police report against Bank of Valletta or anything. I mean, I was here in Vienna against the transaction so and they were telling me that there are so many of such complaints that it is very likely that I would not be contacted to follow this up."[30]

BOV presented their proof through the evidence of Michael Gatt, Executive in the Payments Section. Mr Gatt explained that, in accordance with the timeline attached[31] to the Bank's reply to the Arbiter, the payment was authorised through the 2-factor authentication by Complainant herself as only she could have been in possession of the One-Time-Password to access her account and the Authorisation Code to authorise the payment.

Furthermore, Doc. C attached to the Bank's reply,[32] confirms that the same App on the same mobile (token reference number ending 6276) was used to authorise the transaction as was done when authorising normal payments in prior days (12, 16 and 29 October 2023).

Final submissions

In her final submissions,[33] the Complainant re-emphasised that

"*The SMS channels of BOV are not properly secured, otherwise it would not have been possible for the hackers to use the communication SMS channels usually used by BOV for their genuine messages. This became very clear when I received my password to reactivate my online banking on this same SMS channel. Hence, BOV is liable for not securing their communication channels from such attacks*."

She also confirmed that she had not received any direct warnings from BOV about fraudulent smishing attcks that can be sent on BOV's own channels.

BOV made final submissions which[34] repeated many of the arguments already raised particularly emphasising that the payment had been authorised by the Complainant with the 2-factor authentication.

[30] P. 102 - 103
[31] P. 41
[32] P. 52
[33] P. 109 - 110
[34] P. 112 - 118

BOV claims that it fully complied with the law as provided by PSD 2[35] and Banking Directive 1[36] issued by the Central Bank of Malta.

BOV maintained that it had a robust payments system, fully in line with the two factor authentication provisions of PSD 2. Once payment was fully authenticated by the Complainant there was necessarily gross negligence on her part which made her fully responsible for the consequences of the fraud she incurred.

The Bank also disputed Complainant's claim that '*it was not obvious to me that I am authorising a transaction'*.

They maintain that Complainant, in her evidence, confirmed she had made similar transactions before. She confirmed making two payments through the App shortly before the fraud payment event.

'Moreover, Ms ZG had clear indications that she was approving a transaction since throughout the process she had to access a section entitled 'Transaction Signing', where she would see a section entitled 'Amount' and another section entitled 'Payee Code' as shown in DOC.E attached with the Bank's reply. These sections and wording are visible both on the hardware token and on the software token, thus irrespective of whether a customer uses the physical internet banking key (hardware token) or the BOV Mobile app (software token) to approve a payment, the information shown is the same. These words all clearly indicate that a transaction is being authorised. The fact that she followed the instructions when seeing these words and when she did not have the intention to make a payment, contributes to her gross negligence. This especially in view of the fact that the SMS did not refer to any transaction.

Respectfully, the Bank submits that Ms ZG only mentions the SMS and is neglecting to acknowledge the additional actions which she performed which greatly contributed to the fraud. Had she simply clicked on the link or entered her log in details on the website, the payment would not have been approved. The payment was approved because she actively participated in the approval when she had multiple indications to realise what she was doing.

[35] Directive (EU) 2015/2366 commonly referred to as PSD 2meant to safeguard the consumer (PSU) from having responsibility for payments which are not properly authorised.
[36] Directive 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which is modelled on the requisites of Directive (EU) 2015/2366.

Bank's response to the reported transaction

Whereas Ms ZG states that "BOV support was not available in this critical situation". As explained in the Bank's reply to the initial complaint, the Bank took immediate action and made the recall request on the same day, within less than an hour from when Ms ZG called to report. At this point, this was all the Bank could do, since the payment had already been duly authorised. BOV has no control on the actions or decisions of other banks.'[37]

Reference was also made to the fact that the Malta Communications Authority (see next section) had confirmed that the BOV had no means of preventing any fraudster from personifying the Bank and using the SMS normally used by the Bank to give notifications to its customers.

Consultation of the Malta Communications Authority

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

From the consultation meeting, it emerged 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 (otherwise 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.

[37] P. 117

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 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 the fact that the client errs 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[38] makes a 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.

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

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.

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 duty bound to make (as explained in the model) is effective.[39] [40]

Decision

The Arbiter shall decide as provided for in Article 19(3)(b) by reference to what he considers to be fair and reasonable fairness 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:

[39] (EU) 2018/389 of 27 November 2019 RTS supplement PSD2 EU 2015/2366 Articles 2(1) and 2(2)
[40] PSD 2 EU 2015/2366 Item 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	0%	0%
FINAL TOTAL	40%	60%

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

The model finds that the fact that the Complainant continued to cooperate with the fraudster by completing the amount and last 5 figures in the Signatures of the App, and then inserting the generated authorisation code specifically for the payment, as well as the fact that she had made online third-party payments in the previous 12 months, increases the Complainant's dose of negligence.

The model partially excuses the Complainant as she did not receive a direct warning from BOV about these fraudulent schemes in the months before this case and, thus, offers it 20% compensation.

The Arbiter further switches another 20% responsibility on to the Bank as he considers that there are special circumstances in that the Complainant was travelling, had a problem in contacting telephonically the Customer Service of the Bank, and was in panic by the possibility of missing due payments to Booking.com if her account remained blocked.

Thus, in terms of Article 26(3)(c)(iv) of Cap. 555 of the Laws of Malta, the Arbiter is ordering Bank of Valletta p.l.c. to pay the Complainant the sum of one thousand, three hundred and eighty-two Euros and forty cents (€1,382.40) being 40% of fraud payment of € 3,456. The Arbiter is disregarding the small recovery of €2.07 as this goes against the recall charges involved.

Payment must be made within five working days of the date of the decision. Otherwise, interest at 4.25%[41] starts to run from the expiry of the five days to the date of effective payment.[42]

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

Alfred Mifsud
Arbiter for Financial Services

[41] Equivalent to the Main Refinancing Operations (MRO) interest rate fixed by the European Central Bank.
[42] If this decision is appealed and the appeal confirms this decision, interest would apply from the date of this decision.

Information Note related to the Arbiter's Decision

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 20 (twenty) 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.

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 15 (fifteen) 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 on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.