Before the Arbiter for Financial Services

Case ASF 188/2024

DK

(Complainant)

vs

Bank of Valletta p.l.c. (C-2833)

('BOV' or 'Bank' or 'Service Provider')

Sitting of 7 March 2025

This is a complaint[1] concerning a fraudulent payment made on behalf of the Complainant to third parties from his 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.
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.

[1] Pages (p.) 1 – 6 and attachments p. 7 - 28

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 18 July 2024, the Complainant received the fraudulent message on the mobile by SMS where he usually receives notifications from BOV.

2. As the Complainant felt that this was a genuine message from BOV, he clicked on the link contained in the SMS and disclosed the confidential information granting access to his account. Shortly after, he received a message on same BOV SMS channel warning him that there was a card verification transaction with Deliveroo UK, but no payment was yet being affected. The SMS invited him to contact BOV as the card verification was not authorised.

3. Soon after, there was an attempt to make a payment of €750 to Western Union but he contacted the Bank's helpline in time to deactivate his online banking. He was informed that no payment had been made. The Bank representative informed him that the Bank never sends links with its SMS messages and that a new card will be sent by mail. As he admitted disclosing his secret codes after he pressed the fraudulent link, he was informed to visit a branch of the bank in order to reactivate his online banking.[2]

4. The next day on 19 July 2024, his online banking was restored after two visits to a BOV branch. Shortly after, he received a call on the Bank's number asking if his online access problem was resolved and he confirmed that everything was fine.

5. Less than one hour later, he received another call on same number from somebody called James pretending to be from BOV informing him that for security purposes, they needed to change his USER ID (which had already been changed in the morning when he visited the branch). This call was followed up by other calls supposedly to start the process to change the USER ID. Complainant admits that, in hindsight, it is clear that these calls were fraudulent as scammers were persisting in their attempts which had failed the previous day.

6. Believing that he was speaking to the Bank, the Complainant proceeded to follow the instructions given by the fraudsters until he was informed that the process to change his USER ID had been successfully completed at about 15:51 on 19 July 2024. At this point, Complainant claims he lost access to his online banking.

7. A fraudulent payment for GBP 1,300 (equivalent to €1,573.85) was taken from his account on Monday 22 July 2024, payable to a beneficiary Vera o Connell to a UK IBAN. The beneficiary declared a Malta address and shows the purpose of the payment as purchase of 3 months dog watching services. The payment was done on a same day priority basis.[3]

[2] P. 112
[3] P. 104

8. Complainant claims he only received an SMS alert about this payment on 24 July 2024. He immediately went to file a police report.[4] Subsequently, he went to BOV branch to report the fraudulent payment. A recall of funds procedure was initiated but was unsuccessful as the payment had been processed 2 days earlier on an urgent same day basis.

9. Complainant seeks a refund of €818.92 being 50% of the amount scammed plus €32 charges.

Having considered, in its entirety, the Service Provider's reply, including attachments,[5] where they state:

A. 'Timeline of Events

1. *Whereas ("the complainant") states that "I was the victim of a fraudster who was able to extract funds from my account."[6] Whereas according to the Bank's records, the events which led to this incident were the following:*

2. ***18/07/2024 at 17:53**: he received an SMS from BOV Mobile saying "BOV-BOV Card has been blocked please phone us at 21440823 or remove the block from your BOV mobile app at https://ebanking-bovuser.com."[7]*

3. ***18/07/2024 at 19:55**: he received an SMS from BOV Mobile stating "BOV-Attempt to transact EUR 750 on BOV Card at https://westernunion.com/mt".[8]*

4. ***18/07/2024 at 19:59**: He called the Bank's customer service center to inform them regarding the 2 above-mentioned SMS's he received. The Customer Service representative informed him that the first message was a scam message and informed him that the Bank does not send SMSs with links. Moreover, **she informed him that the Bank never asks customers for their USER ID or card details.** The representative authenticated Complainant and proceeded to stop his card. She also confirmed that the last transaction he made was genuine and no fraudulent transactions were affected. Complainant informed the customer service representative that on the link*

[4] P. 107 - 110
[5] P. 34-43 with attachments P. 44 - 97.
[6] P. 3
[7] P. 16
[8] *Ibid.*

he clicked on the initial message, he provided his USER ID and thus the representative informed him that this needed to blocked as well. She also informed him that he would not have access to his card or internet or mobile banking. She informed him he has to wait for his new card and with respect to the internet and mobile banking, she informed him that he needed to visit a branch to reactive them.

5. ***19/07/2024**: Complainant's software token was re-activated at 15:49:01. Each token, whether a software token (the BOV Mobile app) or the hardware token (the physical key), has a unique certificate number associate with it. Upon re-activation of the token, a new software token serial number was generated, which was 'FEB7322355'.*

6. ***24/07/2024 at 9:18**: Complainant called the Bank's Customer Service Centre and stated that he received an SMS saying "BOV ALERT – A payment for EUR 1573.85 has been issued from A/C No. ending 9111, ref.2420401031449000. If not in conformity contact 21312020 immediately." The representative informed him that a payment had been affected via internet banking to Wise payments. She also informed him that the transfer had occurred using his USER ID and his log-in one time password. He then stated that on Saturday afternoon he received a call from a BOV number who told him to change his USER ID. However, he also stated that when he went to the branch, he was informed that it is not possible to change his USER ID. He also stated that when he received the call in the afternoon, he provided his log-in one time password. He then mentioned that it is possible that he did not give the one-time password but a signature. The representative informed him that the signature section is used to approve payments.*

B. <u>Approval of the Payment</u>

7. *Whereas the complainant attached the details of the transaction in question, bearing transaction reference number 2420401031449000. According to the Bank's records, this transaction was duly authorised on the 22nd of July 2024 at 8:44.[9] 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*

[9] DOC.A: Log showing the internet banking session when payment was approved.

complainant, from credentials and systems registered in his name. in fact, this transaction had no indication that it was fraudulent.

8. *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.*

9. *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;*[10]

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

[10] Article 4(30) of PSD2

*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."

11. *Whereas the complainant was not only aware of the amount of the transaction, but also inputted it himself in his token which is either the BOV app or the physical internet banking key (this is the element of possession of strong customer authentication). Besides this, he also inputted the last 5 digits of the IBAN number of the recipient, and this satisfies the element outlined in article 5(c) abovementioned. Upon entering these details, a code would have been generated which needs to be used to approve the transaction. The customer accesses this section from the section entitled 'Transaction Signing', 'Signature 2' and then sees a section entitled 'Amount' and another entitled 'Payee Code'. This can be seen from the document attached as '**DOC.B**' (which is easily accessible on the Bank's website). These phrases all clearly indicate that one is approving a transaction.*

12. *Whereas this payment was approved by the confidential details of the complainant with the use of his 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 systems (attached and marked as '**DOC.C**') 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."[11]

"All payments, instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your BOV Securekey 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."*[12]

13. *Whereas in fact, every token used to generate codes 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 the same one which was associated with his token which was re-activated a few days earlier, which was FEB7322355.*

14. *Whereas besides the fact that the payment was duly authorised, there is also the fact that the transaction amount was within the limit imposed 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.*[13]

15. *Moreover, the abovementioned 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.*[14] *Therefore, one can conclude that when a transaction is considered to be of a higher risk,*

[11] DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 5.
[12] *Ibid,* page 4.
[13] Article 28(2) of Directive 1 of the Central Bank of Malta which reflects article 52(2) of the PSD 2.
[14] Article 18 of Regulation (EU) 2018/389.

(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 for this transaction and all other transactions so that the Bank ensures that it implements the highest level of security possible (Even if a transaction is considered to be low-risk).

16. *Whereas without prejudice to the above, if the complainant is alleging that this transaction was not authorised by him and has evidence of this, then the Bank is still not obliged to refund him since even if he did not have the intention to approve a payment, he 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;*

    *(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**.*

17. *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**.*

18. *Whereas if the complainant is alleging that the transaction was not authorised by him, this means that he 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, he 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 he had no intention of approving a payment,*

then it would have been reasonable for him to take action and ask why he was being asked to input an 'amount'.

19. *The fact that he 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 an 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 Secure Number/s, the BOV Securekey PIN and/or the BOV Mobile Application, the BOV Mobile Authentication Software the BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party."*[15]

20. *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. 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'*[16] *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 bank accounts.*

[15] DOC.C 'BOV 24X7 Services – Important Information and Terms and Conditions of Use Page 7
[16] DOC.E 'BOV Mobile Banking – Tips for Safer Mobile Banking'.

- *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."*

21. *Whereas the above-mentioned 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.*

22. *Whereas in May 2023 the Bank published a page entitled 'Spot the Scam: Bank impersonation Scams' which explains that scammers may use a 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."*[17] *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.*

23. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams. '**DOK. G1**' shows a comprehensive list of the posts made by the Bank on social media in the months preceding the incident of the complainant. Moreover, the Bank coordinated TV appearances where Bank employees explained what 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.G2**'.*

[17] DOC.F 'Spot the Scam: Bank impersonation Scams'

24. *Whereas besides communication on social media, in November 2023 the Bank also launched a scheme of sending SMS's directly to its customers in order to inform them of ongoing scams which may be directed at them. In fact, prior to this incident, the Bank had sent Mr. Micallef the following SMS's:*

    10/11/2023 – "SPOT THE SCAM. Please be vigilant. BOV never sends links by SMS. DO NOT click on any links and do not provide personal information, passwords, or card details."

    06/02/2024 – "SPOT THE SCAM. BOV will NEVER send you an sms/email with weblinks that ask you to provide card details, PIN, verification codes or on-line banking passwords."

    25/04/2024 – "SPOT THE SCAM. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests."

25. *Whereas besides these SMS's, Mr. Micallef had been informed by the Customer Service representative* ***on the 18th of July 2024 that the Bank never asks for card details or the USER ID****. Moreover, the call he received asked him to follow the instructions in order to change his USER ID. However, as he explained himself in the call to the Customer Service Representative on the 24th of July, the same morning he had received the call, he had gone to the branch where he was informed that the USER ID cannot be changed. Therefore, all this should have raised suspicion in Mr. Micallef that the call was not genuine.*

26. *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 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'[18] which provides the following:*

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

- *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.*

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

28. *Besides this, he also acted against article 45(2) of the Directive because he did not take all the reasonable steps to keep his 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 adhere to.*

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

C. <u>Bank's actions upon reporting of the fraud</u>

30. *Whereas the payment was approved on the 22nd of July 2024 at 8:44. This kind of payment is processed immediately as can be clearly seen in the terms and conditions marked as '****DOC.C****', 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'.

31. *Therefore, when the complainant called the Bank on the 24th of July 2024 at 9:18am, the representative blocked the internet banking of the complainant. The same day, Bank also made a recall request to the correspondent and beneficiary banks, which request is made through a digital, internal system between Banks.*

32. *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 king of answer they give.*

33. *Therefore, the Bank respectfully submits that it did its utmost to recover the funds and when it received a reply from the foreign bank, it informed Mr. Micallef accordingly and urged him to follow up the matter with the police who are the appropriate entity vested with the power to investigate and persecute fraudsters. (**'DOC.H'**).*

34. *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 his actions which show gross negligence.*

D. Conclusion

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

36. *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.

37. *The Bank reserves the right to bring oral and documentary evidence in order to substantiate the defenses 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.*

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

With expenses."

The hearings

At the first hearing on 14 January 2025, the Complainant gave this evidence:

"***What originally happened was that I received SMS with regards to a scam and at the time I was at work. I was a bit confused, all over the place, and I ended up falling for an engineered scam by SMS.***

That being said, at the time I had phoned BOV instantly to stop my card. At the time, they were really helpful, they stopped my card straight away. I did not lose any money. But the only problem was that during this call when I asked what happens with regards to my user ID, given that this was given during the scam, the reply by the person on the telephone said, 'Then go to the bank tomorrow and they'll tell you what to do.'

So, at this point, I was already a bit confused with regard to this point about the user ID. I went to the bank the next day and this was sort of sorted because my BOV online was reinstated. But, on the day, I also received an SMS by BOV stating that today we will be receiving a call from BOV. I did receive a phone call from a number of BOV and I told them that I already went to the bank. Case closed.

But about an hour later, I received another phone call from the number of the Customer Care of BOV, at which point, the person on the phone, who had an

English accent, (I think his name was James), who told me, 'We need to change the User ID. I'm going to get in contact with my manager; I will phone you again later.'

So, now, in retrospect, I know that he is the scammer. He phoned me again, let's say an hour or two after, and he was guiding me through the process to change my user ID. And, again, in this respect, this was the scam, but I was unaware at the time; I made mistakes on my end. That is what caused the transfer to happen. That being said, after this took place, I did not have access to my BOV online services.

The last time I met with BOV, I asked how this happened, and the reply I got was that the services were all working fine and that it could have been my Internet connection. I don't think this the information I asked for. I wanted to know why I was denied access, not the system in general. And I can assure you, over the course of four days, I had access to Internet, and I still don't know if my account was closed from BOV's end without my authorisation or if it was because of something else. But I was told, when I went to the bank after the scam happened, that I needed to authorise the account being closed and I never authorised this. So, I just want more clarification with regard to this point because saying the Internet did not work is not the case.

The point which I want to focus on the most as well was that as soon as I received the SMS asking me whether this transfer was fraudulent, I phoned within two minutes. I even paid money for a recall of funds, and they sent that the funds had already moved. But why send the SMS when it's too late? The bank told me that they have no obligation to send the SMS. But if you're going to send an SMS, why send it when it's too late as opposed to sending me even an email receipt on the day of the transfer saying this transfer was made, etc.

As I didn't have access to my BOV online as well as not receiving this SMS in good time, I couldn't contact the bank sooner to sort out the problem when it would have been possible to be sorted out."[19]

[19] P. 98 - 99

On being cross-examined, Complainant stated:

"***Asked what information I provided to the person who was allegedly calling from the bank, I say that I can't remember exactly the information. I mean, whatever they asked me, unfortunately I was compliant. I thought it was from the customer service. At the time, I thought it was from a verified source, given it was from BOV's number. I am sorry I can't tell as this was six months ago; I don't remember exactly what I gave and what I didn't give.***

Asked whether I just provided information or whether I used the BOV mobile app in the process, I say, yes. I had to give a Signature 2. I understand that this was a mistake.

So, I just decided I had to give a Signature 2. At the time, I was confused. I thought it was the Signature 1, which is needed to do an incoming transfer, and I thought this guy is helping me change my user ID Signature 2 for these types of details. Again, I know this was a mistake.

I say that I am talking about the second attempt.

On the first attempt, no money was taken. BOV were very helpful at that instance because my card was blocked instantly. So, there were no problems.

Unfortunately, they phoned again; given they had some of my information, they continued to use it and, ultimately, it worked, unfortunately.

Asked to confirm whether the bank had sent me SMSes warning me to be aware of such scams in the months preceding the scam, I say, yes, they had sent but I do not recall how long it has been since I last received an SMS. I know that I received one a week after this happened as well, so I don't know if there is a general time.

And I don't know how long the interval was between receiving an SMS and this happening.

It is being said that the service provider listed three SMSes on page 8 of their reply. Asked to confirm whether I received these SMSes on those dates: 10 November 2023; 6 February 2024 and 25 April 2024.

I can confirm that I received the one sent on 25th of April. I say, yes, I did receive these SMSes. Again, I don't claim that I have not made any mistakes.

Asked when I called on the 18th of July to report the first incident whether I remember that the person who spoke to me told me that the bank never asks me for the User ID and that it never sends me links and SMSes after I reported the first scam, I say that I do not think that this information was given to me on the 18th. I'm going to be honest.

Again, like I mentioned, when I asked a question regarding the user ID, she told me to go to the bank and they'll tell me what to do, which was quite an unambiguous answer. It left me a bit confused; I made a mistake when the guy told me that I need to change my User ID, I wasn't sure.

It is being said that in that conversation of the 18th of July, I was informed by the bank representatives that the bank never asked customers for the User ID, which is basically the same as it was in the previous SMS.

Asked to confirm whether she gave me this information, I say, I'm sorry but I do not remember. Again, it was six months ago.

Asked whether I am familiar with the bank's terms and conditions regarding Internet banking, I say, I guess so because I use the bank's service.

Asked whether I made a police report regarding this incident, I say, yes, I made a police report instantly. In fact, BOV told me to go to the police and I had already made the police report.

Asked whether I received any updates from the police, I say, so far, no."[20]

At the second hearing on 4 February 2025, Michael Gatt was presented to give evidence by BOV. He stated:

"***I have been employed by the bank for almost thirty years and for the last fifteen years within the Electronic Banking Section.***

I say that to process the transaction, first of all, one has to have access to the mobile, so the mobile must be unlocked using biometrics – fingerprint, Face ID.

[20] P. 100 - 102

Then, one has to access the BOV Signatures; has to go to the Transaction Signing, choose Signature 2, enter the amount and the Payee Code. Then you enter your PIN, get a Challenge Token and at that point the transaction will be processed.

Without all these steps, even if you miss one of them, the transaction will not be processed.

The User ID or Login ID will only give you access to view the accounts. A transaction cannot be processed using only the Login ID or the User ID. It is impossible.

I say that, according to our logs, the complainant followed all the aforementioned steps to authorise the transactions."[21]

On being cross-examined, Michael Gatt replied:

"***The complainant says that according to the steps, he inputted an amount in a transaction that he did not do personally and he is confused by this.***

I say that when one signs, when one is in the process of signing a transaction, there is a specific field, it's called 'Amount'. So, someone must have entered that amount, the amount is specific.

It is being said that the complainant definitely did not do this, and asked whether it is possible that the amount was placed by another device."[22]

At this point, the Arbiter clarified that once a fraudster penetrates the Complainant's account, he creates the payment order, but what Mr Gatt is referring to is that this payment order needed an activation code to be executed.

The activation code is from Signature 2. Once you go on Signature 2, you are given a panel which shows 'Amount' and the last five digits of an IBAN number and then, you have to input the activation code before the payment can be affected.

The Complainant opted not to cross-examine the evidence by Michael Gatt.

[21] P. 113
[22] P. 114

The Arbiter then asked the Complainant to explain again the timeline of 19 July 2024. Complainant replied:

"***Yes. On the 19th, in the morning, I went to the bank. I went to Bormla bank. I had to go twice. Yes, on the 19th by 12:00, I was set up, I was alright; and I received the phone call from the fraudster after this, in the afternoon, and then I lost the connection again.***

The Arbiter asks the bank whether they have any evidence or explanation of why the complainant lost the connection on Friday afternoon."[23]

Michael Gatt replied:

"***We checked our records and we had no issues with our mobile banking and if the complainant's account was blocked, then he couldn't have logged in on the 22nd to authorise the transaction. Once an account, a token is blocked, then you have to go personally to the bank to unlock it.***

If it was locked, on the 22nd he would not have even logged in."[24]

Dr Luana Vella representing the Bank further explained:

"***During the last sitting, the complainant mentioned that he entered certain details in Signature 2. If his device was not working, he could not have access to Signature 2***."[25]

Complainant replied:

"***The transaction taking place on the 22nd, to me, does not make sense because I received the phone call from the fraudster on the 19th in the afternoon; when I gave Signature 2 it definitely was not on Monday 22nd, so if a transaction took place, my authorisation was given on Friday, the 19th. It definitely was not given on the 22nd. So, if the transaction took a few days to go through, I don't know. From my end, though, I definitely did not enter anything on the 22nd of July because all this took place on the 19th. I should have the phone log. I'm pretty sure I sent the phone log, and I received the phone call from the***

[23] P. 116
[24] *Ibid*.
[25] *Ibid*.

fraudster on the 19th. So, if I gave access, it was during this phone call on the 19th, definitely not on the 22nd.

The Arbiter states that he notes the complainant's case and he knows that Bank of Valletta presented a log which shows that the transaction payment was affected on the 22nd.

The Arbiter has to decide which one carries more weight. The Arbiter asks Mr Gatt whether the bank has any record that in this process there was an attempt or of any registration of a new device."[26]

Mr Gatt replied:

"***I can check but from the records, no. The difference in the serial number of the token was because on the 19th everything was stopped for the complainant, and a new activation code was sent and that will change the serial number of the token. That happened before the transaction, after, no.***

I think we can check if the complainant had performed some transactions after the 22nd and 99.99%, it would be the same serial token that was used before since only he can request a change or has to change his mobile.

The Arbiter asks whether the Bank's records show that a new device was registered, not just the activation code.

No."[27]

The Arbiter requested submission of evidence that subsequent genuine transactions were made with the same token which was used to make the fraudulent transaction.

The Arbiter also requested confirmation of the time and date the SMS alert about the fraudulent payment was sent to Complainant. The Arbiter knows that there is no regulatory obligation to send these alerts, if an alert is sent, it is not sent two days after.

[26] P. 116 -117
[27] P. 117

Final submissions

In their final submissions, the parties have reiterated their positions as already explained in the Complaint, the Reply and evidence given during hearing.

The BOV submitted, as requested:

> Evidence that the SMS notification of the fraudulent payment was submitted on 22 July 2024 at 09:12:02, i.e., less than half an hour after the transaction was executed at 08:44.[28] [29]

They explained they cannot submit evidence that the token used to authorise the fraudulent payment was also used for genuine transactions as the token identifier number changes every time the USER ID changes. The USER ID was changed on 19 July when the first unsuccessful fraud attempt was reported and before the second successful fraud attempt was executed and was changed again on 24 July after the fraudulent transaction was reported. In between, no transactions occurred other than the fraudulent payment subject of this Complaint.[30]

Consultation of the Malta Communications Authority

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

From the minutes of the consultation meeting,[31] it emerges 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

[28] P. 45; 127; 129
[29] Complainant contends that he received 2 days later but furnished no evidence in this regard.
[30] P. 123 – 124, point 7
[31] P. 76 -77; 78 - 84

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 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[32] 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.

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

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.

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. [33] [34]

Final analysis

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:

[33] (EU) 2018/389 of 27 November 2019 RTS supplement PSD2 EU 2015/2366 Articles 2(1) and 2(2)
[34] 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	(20%)	20%
Sub-total	0%	100%
Reduction to special circumstances	0%	(0%)
Reduction for absence of similar genuine, monthly payments in the last 12 months	20%	(20%)
FINAL TOTAL	**20%**	**80%**

Therefore, according to the framework model, the Complainant should bear 80% of the weight and the other 20% will be borne by BOV.

The model finds 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, thus, increasing the Complainant's dose of negligence.

This particularly so when in the phone conversation with the Bank's customer service centre on 18 July 2024, the Complainant was specifically informed that BOV never sends any links with its SMS messages to customers.[35]

BOV has proven to the Arbiter's satisfaction that the fraudulent payment was effectively authorised by the Complainant on 22 July 2024 using the new token reference allocated to him after the first fraudulent attempt had failed and the Bank had to change the USER ID which was disclosed to the fraudster during the failed first attempt.

The model offers no relief to the Complainant for failure of a direct warning from BOV about these fraudulent schemes in the months before this case. It has been confirmed that 3 such direct SMS warnings were sent to Complainant by BOV on 10.11.2023, 06/02/2024 and 25.04.2024 (apart from the verbal warning on 18.07.2024 referred to above).

The Arbiter does not see any special circumstances which may inspire a reduction of the negligence involved in authorising the payment being complained of. On the contrary, there were special circumstances which could apply against the Complainant when he not only ignored multiple warnings not to press any links on SMS messages purporting to be sent by BOV, but also in not suspecting that the calls were fraudulent when he accepted to co-operate to change his USER ID which he had just changed during a branch visit earlier the same day.

The Complainant had ample opportunity to understand that a change in USER ID was only possible through a physical visit to a branch of the Bank.

[35] P. 112

Furthermore, there were other inconsistencies in the evidence provided by the Complainant especially regarding his contention that he did not co-operate with the fraudster on the 22 July when the payment was made and arguing he had done so only on the 19th. BOV explained that the code authorising the payment would remain valid only for seconds and for a one-time use.[36]

The Arbiter is however conceding a 20% relief of the responsibility for reason that no evidence was provided that Complainant was familiar with the online payments to third-party system operated by BOV.

Decision

For reasons above explained, and 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 three hundred and fourteen euros and seventy-seven cents (€314.77) being 20% of the fraud payment of € 1,573.85.

Payment must be made within five working days of the date of the decision. Otherwise, interest at 2.90%[37] starts to run from the expiry of the five days to the date of effective payment.[38]

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

Alfred Mifsud
Arbiter for Financial Services

[36] P. 126, para. 19
[37] Equivalent to the Main Refinancing Operations (MRO) interest rate fixed by the European Central Bank.
[38] If this decision is appealed, and the appeal confirms this decision, interest would apply from the date of this 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 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.

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 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.