Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 184/2024

SK u LK

('Ilmentaturi')

Vs

Bank of Valletta p.l.c.

Reg. Nru. C 2833

('Fornitur tas-Servizz' jew 'BOV' jew 'Bank')

Seduta tat-28 ta' Frar 2025

Dan huwa ilment li jirrigwardja pagament frawdolenti li sar għan-nom tal-Ilmentaturi lil terzi mill-kont li għandhom mal-Fornitur tas-Servizz.

L-Arbitru ġew quddiemu diversi ilmenti ta' dan it-tip li filwaqt li jvarjaw fuq ċerti dettalji, fihom ħafna affarijiet komuni bejniethom:

- Il-pagament ikun għal ammont ġeneralment taħt il-€5,000 biex ma jinżammx minħabba li jeċċedi d-*'daily limit'* ta' pagamenti li jkun maqbul bejn il-Bank u klijent tat-tip *'retail'.*
- Il-frodist jirnexxielu jippenetra b'mod frawdolenti l-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *email*.
- Il-frodist jagħti *link* fil-messaġġ tiegħu u jistieden lill-klijent biex jagħfas fuq il-*link* biex jagħmel '*validation'* jew *'re-authentication'* tal-kont tiegħu.

- Minkejja diversi twissijiet maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-bank ma jibgħatx *links* fil-messaġġi tiegħu, u li l-klijent għandu jikkomunika mal-bank biss tramite l-App u/jew il-websajt uffiċjali u dan permezz tal-kredenzjali li l-bank ikun ta lill-klijenti, il-klijent b'nuqqas ta' attenzjoni jagħfas il-*link*.

- Minn hemm 'il quddiem, il-frodist b'xi mod jirnexxielu jippenetra l-kont tal-klijent u jagħmel trasferiment ta' flus, ġeneralment fuq bażi '*same day',* li jmorru fil-kont tal-frodist, ġeneralment f'kont bankarju f'pajjiż barrani minn fejn huwa kważi impossibbli li jsir *recall* effettiv tal-flus ġaladarba l-klijent jirrapporta lill-bank tiegħu li ġie ffrodat. Ħafna drabi l-frodist ikun pront jiġbed jew jittrasferixxi l-flus appena jaslu fil-kont indikat.

- B'riżultat jinħoloq nuqqas ta' ftehim bejn il-bank u l-klijent dwar min hu responsabbli jġorr il-piz tal-pagament frawdolenti. Il-klijent isostni li l-bank ma pproteġihx meta ħalla li kanal ta' komunikazzjoni normalment użat bejn il-bank u l-klijent jiġi ppenetrat mill-frodist, u li l-bank messu nduna li kien pagament frawdolenti għax ġeneralment il-klijent ma jkollux storja ta' pagamenti bħal dawn. Il-bank isostni li l-ħtija hija kollha tal-klijent għaliex permezz ta' traskuraġni grossolana (*gross negligence)* ikun ta aċċess tal-kredenzjali sigrieti tal-kont tiegħu lill-frodist u b'hekk iffaċilita l-frodi.

F'dan il-każ partikolari, dawn huma d-dettalji relevanti:

- Fit-3 ta' Novembru 2023, għall-ħabta tal-11:20, l-Ilmentaturi għafsu fuq *link* li kienet fuq *email* frawdolenti li kienet tidher li ġejja mill-BOV.

- Billi l-Ilmentaturi ħasbu li dan kien messaġġ ġenwin mill-BOV, għafsu l-*link* u daħlu f'websajt li kienet tidher tal-BOV għax dehret identika.

- Imxew pass pass mal-istruzzjonijiet kollha li tahom il-frodist u, permezz t'hekk, jidher li ġie awtorizzat pagament frawdolenti ta' €4,321.[1]

[1] Paġna (p.) 13

- Dan sar f'kont tal-bank tal-frodist fl-Olanda (NL), u l-frodist kien poġġa struzzjonijiet biex il-pagament isir ***'same day priority payment'***.[2]

- B'mod qarrieqi, il-pagament kien jindika li l-benefiċjarju kien jismu **Said zaimi,** u bħala dettalji tal-pagament indika ***"Loan repayment – THANK U SAID".*** Indika li l-indirizz tal-benefiċjarju kien f'Pariġi.[3]

- L-Ilmentaturi jsostnu li ma rċevew l-ebda SMS biex jinnotifikahom fuq il-pagament u kien biss wara li marru jiċċekkjaw il-kont li ntebħu bil-frodi.

- L-Ilmentaturi pront ċemplu lill-BOV iżda damu biex jaqbdu u minħabba f'hekk meta fl-aħħar irrapportaw, il-pagament kien diġà ġie pproċessat peress li kien fuq bażi *same day*.

- Sar *recall* mill-BOV iżda dan ma ġiex aċċettat mill-bank benefiċjarju.[4]

- Il-każ ġie rrapportat lill-pulizija għal aktar investigazzjoni tal-frodi.[5]

L-Ilment[6]

L-Ilmentaturi elenkaw dawn ir-raġunijiet għalfejn iħossu li l-Bank kellu jagħmel tajjeb għat-telf li ġarrbu minħabba l-pagament frawdolenti.

'*On 3rd November 2023, we fell victim to a phishing scam, resulting in a fraudulent payment of €4,321 being made from our Bank of Valletta (BOV) joint account 1290070301 3 to a third party. I (the Complainant) received an email that appeared to be from BOV, stating that the use of my mobile signature had been temporarily restricted. The email provided a link for me to 'self-remove' the restriction. At the time, I was abroad in the United Kingdom, accompanying my husband (the Complainant) for a medical procedure.*

Concerned that our primary bank account could be blocked, I followed the link and entered my credentials. Subsequently, an unauthorised payment of €4,321 was made to a bank account in the Netherlands, with the beneficiary named as 'Said Zami'. I did not receive any SMS notification of the payment and it was only

[2] *Ibid*.
[3] *Ibid*.
[4] P. 166 - 168
[5] P. 44 - 46; P. 42 - 43
[6] P. 1 - 6 u dokumenti annessi p. 7 - 97

when I checked the transactions, I realised a payment was made. Upon realising that this was a fraudulent transaction, I immediately attempted to contact BOV's customer support but faced significant delays. By the time I managed to report the fraud, the bank claimed it was too late to stop the payment, as the funds had already been transferred.

Despite multiple follow-ups and my swift reporting of the incident, BOV failed to recover the stolen funds or take timely action. In their response to my formal complaint, BOV argued that the transaction was executed in accordance with their security protocols and that they were not liable for the loss. The bank did not consider the fact that I had never made such a high outward payment before, and that the transaction should have triggered a more stringent review process given its suspicious nature.

The bank's failure to promptly identify the fraudulent transaction, along with the delays in their response and communication, resulted in the loss of my funds. I have also lodged police reports both in the United Kingdom and Malta (reference numbers NFRC231106274296 and NPS 6/POL/6990/2023) and have waited to see if there would be any developments on that front before escalating this matter further with the Arbiter for Financial Services.

Considering these circumstances, I am seeking a reimbursement of the €4,321 stolen from my account due to the bank's failure to act with due care and diligence in preventing this fraudulent transaction.

Reasons why Bank of Valletta (BOV) has let me down

1. ***Failure to Detect and Block Suspicious Transactions:***

   The fraudulent payment of €4,321 was significantly higher than any other outwards payments made from my account. I had never previously made such a large payment to an external party, especially not to a foreign beneficiary. Despite this, BOV did not identify the transaction as suspicious or take any additional steps to verify its authenticity before allowing it to be processed.

2. ***Delayed and Inadequate Response to the Fraud Report****:*

   When I realised that the fraudulent payment had been made, I immediately attempted to contact BOV's customer support. However, I experienced long wait times and was unable to get through to an agent in a timely manner. This delay hindered any chance of blocking the payment at an early stage or recalling the funds while they were still being processed.

3. ***Lack of Effective Communication and Follow-Up****:*

   Throughout the process, the bank continued to communicate through the same compromised email channel through which I received the fraudulent message, moreover, having to click on a hyperlink to read their messages, which I was wary of. This not only caused confusion and concern but also demonstrated a lack of consideration for secure communication during a critical period. Despite acknowledging the fraud on 6 November 2023, BOV took no further steps to provide direct updates or alert me promptly about the status of the fund recall.

4. ***Ineffective Fund Recovery Efforts:***

   Although BOV claims to have made several attempts to recover the stolen funds through SWIFT messages to the foreign bank, their actions were ultimately unsuccessful. The delays in follow-up indicated a lack of urgency and efficiency in dealing with the matter. The bank's reliance on a series of SWIFT messages, spanning over a month, without effective follow-up actions or alternative measures, suggests a lack of efficiency in fund recall procedures. This delay diminished the likelihood of recovering the funds. Moreover, the bank did not offer any alternative strategies for recovering the funds or supporting me in pursuing legal or financial remedies through the foreign bank.

5. ***Failure to issue Timely Warnings:***

   BOV only issued a public warning about the phishing scam on 13 November 2023 (attached), ten days after the fraudulent payment had already been processed from my bank account. The delay in issuing this warning deprived me and other customers of critical information that

could have prevented the incident. The bank also failed to provide specific, direct warnings to customers via secure channels, which would have alerted me to the risk of such scams.

6. ***Inconsistent Handling of Customer Concerns:***

   BOV continued to chase me to update my account details, despite being informed of my situation abroad and the fact that I had reported the fraud. This inconsistency and lack of coordination between internal teams led to unnecessary stress and confusion during an already difficult time.

7. ***Denial of Refund based on Security Protocols:***

   The bank justifies its denial of refund by stating that the payment was processed through authorised channels. I challenge this assertion based on the fact that the transaction was fraudulent and therefore was not initiated with genuine customer consent. The bank's security mechanism should have identified this, based on the absence of any prior similarly large outbound payments to third parties in foreign countries, in view of us being long-standing customers with a long history of transactions with the bank being our primary banking relationship.

Given these shortcomings, it is evident that BOV did not take adequate steps to protect my account from fraudulent activity, nor did they provide the necessary support and response to mitigate the loss once the fraud was reported.'[7]

Spjegaw ukoll li dak iż-żmien kienu qegħdin jgħixu Londra minħabba raġunijiet mediċi rigward saħħet l-Ilmentatur.

Fil fatt, l-Ilmentatriċi spjegat:

'*On the 3rd of November 2023, I received an email, which looked like it was coming from Bank of Valletta, stating the following:*

"At Bank of Valletta, we prioritize customer security. As part of our security measures, we have temporarily restricted the use of your mobile signature.

You have two options:

[7] P. 7 - 8

- ***You can either visit your nearest branch and reference the number BV155285***
- ***You can self-remove this restriction by following the provided instructions.***

BOV Internet Login"

At the time of receipt, I was accompanying my husband in the United Kingdom for a stem cell transplant after he was diagnosed with leukaemia. My husband had informed the bank in September when Remediation team were chasing via email to update our records, that we were in the United Kingdom for medical reasons with no definite date as to when we were returning back to Malta. Yet the bank still continued communicating with us and chasing to update our details via email. At the time of receipt of the above-mentioned email, my first thought was that the Bank was restricting our ability to make payments, and this being our primary bank, my fear was that we would end up in the United Kingdom without having means of paying through Bank of Valletta, with no date of return to Malta as my husband was still recovering from the procedure. Therefore, I had clicked on the link and followed through to "self-remove the restriction".'[8]

Bħala rimedju, huma talbu li l-Fornitur tas-Servizz jirrifondilhom il-pagament ta' €4,321.

Risposta tal-Fornitur tas-Servizz

Fir-Risposta[9] tagħhom, il-BOV qalu:

'*Respectfully submits:*

1. *Whereas Mr. and Mrs. (''the complainants'') state that "on 3rd November 2023, we fell victim to a phishing scam, resulting in a fraudulent payment of €4,321 being made from our Bank of Valletta (BOV) joint account."*[10]

   They explain that this incident originated from an email received by (the Complainant) appearing to be from BOV informing her that her mobile signature had been temporarily restricted.

[8] P. 10 - 11
[9] P. 104 – 112 u dokumenti annessi p. 113 - 168
[10] P. 7 *of the complaint.*

2. *Whereas the complainants attached the details of the transaction in question, bearing transaction ID 134230248.*[11] *According to the Bank's records, this transaction was duly authorised on the 3rd of November 2023 at 11:27.*[12] *According to the Bank's systems this transaction was duly authorised by credentials and systems associated with (the Complainant). 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 duly authorised. 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 complainants.*

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;*[13]

5. *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:*

[11] P. 13 *of the complaint.*
[12] *DOC.A: Log of transaction.*
[13] *Article 4(30) of PSD2.*

"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 either the BOV app or the physical internet banking key (this is the element of possession of strong customer authentication). Besides this, she also inputted the last 5 digits of the IBAN 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. 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.*

7. *Whereas this payment was approved by the confidential details of (the Complainants) with the use of her token. The Bank had no control over this transfer because it was completely in the control of the customer without*

the Bank's intervention. Once the Bank receives legitimate instructions for a "third party payment" from the adequate channels, the Bank implements 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.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.''*[14]
>
> *"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.''*[15]

8. *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 approved is the same one associated with the token of (the Complainant) 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.D'.***

9. *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.E'*** *(this document is accessible from the Bank's website.)*

[14] *DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 5.*
[15] *Ibid*, *page* 4.

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.[16]

10. *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.*[17] *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 so that the Bank ensures that it implements the highest level of security possible (even if a transaction is considered to be low-risk).*

11. *Whereas without prejudice to the above, if the complainants are alleging that this transaction was not authorised and has evidence of this, then the Bank is still not obliged to refund them since even if (the Complainants) 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;*

*(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.***

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

12. *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**.*

13. *Whereas if the complainants are alleging that the transaction was not authorised by them, this means that (the Complainants) 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 her since if she had no intention of approving a payment, then it would have been reasonable for her to take action and ask why she was being asked to input an 'amount'. She could have confirmed with the Bank whether the email she received was genuine, particularly since the email address (the Complainant) is saying she received the email from was 'signatures@bov.com.arici-abbruch.de via research.net'.*[18]

14. *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 Mobile Authentication Software the*

[18] P. 45 *of the complaint.*

BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party.''[19]

15. *Whereas as a voluntary user of the internet banking service, (the Complainants) know 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 Complainants) (or any other customer) to access their internet Banking from a link in an email, 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'*[20] *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."*

16. *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.*

17. *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.*

[19] *DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 7.*
[20] *DOC.F 'BOV Mobile Banking – Tips for Safer Mobile Banking'.*

18. *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.''*[21] *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.*

19. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams.* ***'DOK. H1'*** *shows a comprehensive list of the posts made by the Bank on social media in the 6 months preceding the incident in question. 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.H2'.***

20. *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'*[22] *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.***

[21] *DOC.G: 'Spot the Scam: Bank impersonation Scams'*
[22] https://www.mfsa.mt/publication/the-mfsas-guide-to-secure-online-banking/

- *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.*

21. *Whereas despite all these warnings, (the Complainants) 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*.

22. *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.*

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

24. *Whereas the Bank makes reference to the claim made by the complainants that there was "inconsistency and lack of coordination between internal teams" because she was asked to update her account details.*[23] *Respectfully, the Bank submits that the request to update her accounts was separate from the incident regarding the payment and the Bank has been carrying out the process of updating its' customers' details over the past few years and this is being done for all customers. Therefore, there is no lack of coordination between the Bank's departments as the complainants are alleging*.

Timeline of Events

[23] P. 8 *of the complaint.*

25. *Whereas the payment was approved on the 3rd of November 2023 at 11:27. 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'*.

26. *Therefore, when the complainant called the Bank on the 3rd of November 2023, the representative blocked the internet banking of (the Complainants) The Bank also made a recall request on the same day to the beneficiary bank and also sent multiple reminders. This communication is done through a digital, internal system between Banks. 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. Eventually, the Bank received a negative reply that the funds could not be returned. An extract of this communication is attached as **'DOC.I'**. The Bank informed (the Complainants) accordingly and suggested that she follows up the matter with the police (**'DOC.J'**).*

27. *Therefore, the Bank followed the correct procedure to recall the funds, and it is thus unjustified for the complainants to say that there was "a lack of efficiency in fund recall procedures" and that "this delay diminished the likelihood of recovering the funds."*[24]

28. *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.*

[24] P. 8 *of the complaint.*

Conclusion

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

30. *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.*

31. *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.*

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

With expenses.'[25]

Seduti

Saru żewġ seduti nhar is-7 ta' Jannar 2025[26] u l-11 ta' Frar 2025.[27]

Fl-ewwel seduta, l-Ilmentatriċi spjegat kif kienu ilhom Londra alloġġjati mill-bidu ta' Ġunju 2023. Waqt li kienu imsefrin, binthom infurmathom li l-BOV riedu jagħmlu aġġornament tal-profil tagħhom iżda dan kien diffiċli li jsir waqt li kienu imsefrin għax *online* ma setgħux jaqbdu.

[25] P. 104 - 112
[26] P. 169 - 172
[27] P. 175 - 180

'Ngħid li meta, mbagħad, irċevejt dik l-email li kienet tidher awtentika tal-bank, għidt mela solvew il-problema u, allura, nistgħu nagħmlu minn hawnhekk. Kien hemm miktub li aħna stajna nagħmluha online jew inkella mmorru l-bank u, għalhekk, dehret ġenwina.

U anke għall-fatt li kien hemm it-2-Factor Authentication, li inti tirċievi numru u trid tiktbu fiha. Allura, dehret serja l-affari, li l-affarijiet qegħdin kif għandhom ikunu għax għalhekk qiegħda 2-Factor Authentication għax inti mhux fuq ħaġa waħda qed tirċievi imma fuq xi ħaġa oħra wkoll.

Ngħid li meta bdejt niffolowja l-instructions ta' din l-email, ma kont qed nagħmel l-ebda pagament. Ma kien hemm imkien li jien qed inħallas xi flus. Fir-risposta tal-bank hemm 'Family/Friend Reason: Loan Repayment, Thank U Said.' Ngħid li jien ma kont qed nagħmel xejn minn dan, ma kont qed inniżżel ammonti ta' flus imkien.

Ngħid li ma kont qed nagħmel pagament ta' xejn; ġieli xtrajna u ħallasna normali.

Ngħid li kien hemm miktub li jekk inti ma tagħmilx din il-biċċa xogħol se jwaqqfulek il-bank signature. U konna ppanikjati, bejn li qed ngħixu bil-flus li kellna mġemmgħin, u bejn li qed nirċievu dawn l-emails u telefonati, għax darba minnhom kienet ċemplitli waħda mill-bank fejn qaltli, 'Importanti li tagħmluhom dawn l-updates tad-details tagħkom,' fejn kont għidtilha li aħna konna l-Ingilterra u malli ninżlu Malta mmorru dritt il-bank. Imma ma nafx jiena!'[28]

Waqt il-kontroeżami stqarret:

'***Ngħid li jiena għalhekk ġejt misguided għax kollox kien l-istess kif nagħmel is-soltu – li jitla' n-numru u int tikteb dak, li inti tkun moħħok mistrieħ li tgħid mela allura la jien irċevejt in-numru tal-One-Time Password hemmhekk, mela l-affarijiet qegħdin kif ikunu s-soltu. Jien għalhekk ġejt qisni ttraduta għax bdejt nagħmel l-affarijiet kif nagħmel is-soltu.***

Mistoqsija minn fejn ġibt l-informazzjoni li daħħalt fuq il-website li għidt li kienet eżatt bħal tal-BOV - dawn in-numri tat-2-Factor Authentication, ngħid li jkun hemm miktub l-instructions fiha.

[28] P. 170

Mistoqsija minn fejn iġġenerajtha, ngħid li jiena ma ġġenerajt xejn. Ngħid li bdew jitilgħu skont il-page li kont fuqha.

Ngħid li kien hemm miktub li jien irrid indaħħal il-code 4321 u jiena ktibtu u, mbagħad, kien hemm miktub 'Thank U Said' u jien għidt, '4321, Thank U Said?!' Ngħid li dawn kienu kollha miktubin u ngħid li jien żgur li ma ktibt xejn.

Mistoqsija fejn ktibt il-code 4321, ngħid li kien hemm erba' kaxxi ħdejn xulxin u trid tiktibhom int. Ngħid li jien ktibt il-4321, però, ma kienx hemm 'amount' jew flus. Għalija kien il-Pass Code li hu qed jitlobni biex nikteb biex terġa' tiġi din il-mobile signature (jew x'inhi) li huma qalu li kienet restricted. Ngħid li ma kienx hemm il-Euro sign, British Sterling, jew xi ħaġa hekk. Ngħid li ma kienx hemm xi amount li trid tħallas tant għax kieku ma kontx inkompli. Ngħidu li lilna ma talbuniex xi password jew PIN Number, xejn minn dan.

Mistoqsija kinux fuq il-Mobile App jew fuq il-website, ngħid li qisha nfetħet il-Mobile App imma ma ħriġtx minn dik il-link u ftaħt il-Mobile App għax kienu l-istess ħaġa – il-kuluri, l-layout, kollox – għalhekk aħna ġejna misguided.'[29]

Waqt it-tieni seduta, xehed Michael Gatt, għall-BOV li spjega li l-pagament ilmentat kien awtorizzat mill-Ilmentaturi bit-*2 factor authentication* u li, allura, bilfors li l-Ilmentaturi baqgħu jikkoperaw mal-frodist sal-punt li awtorizzaw il-pagament permezz ta' kodiċi b'6 numri mis-*Signature 2* tal-BOV APP.

Fil-kontroeżami, ġie mistoqsi jekk il-BOV messux induna li dan kien pagament stramb peress li kien qed isir minn IP *address* barrani u li l-Ilmentaturi qatt ma kienu għamlu pagamenti *online* ta' dan it-tip.

L-Arbitru spjega li dawn il-kunsiderazzjonijiet ser jiffurmaw parti mill-ġudizzju tiegħu f'dan il-każ.

Il-partijiet waqt ix-xhieda u s-sottomissjonijiet finali[30] żammew il-pożizzjoni kif spjegata fl-Ilment u fir-Risposta tal-BOV.

L-Ilmentatur iwaħħal fil-BOV talli ħalla lill-frodist jippenetra l-kanal ta' komunikazzjoni li normalment juża l-Bank biex jikkomunika miegħu u talli ma ndunax li l-pagament kien frodi.

[29] P. 171 - 172
[30] Sottomissjonijiet finali tal-BOV saru bil-miktub p. 182 - 187

Min-naħa l-oħra, l-BOV isostni li huwa kien għal kollox konformi mal-liġi kif tipprovdi l-PSD 2[31] u l-*Banking Directive* 1[32] maħruġa mill-Bank Ċentrali ta' Malta.

Il-BOV saħaq li huwa kellu sistema robusta u għal kollox konformi mat-*two factor authentication provisions* tal-PSD 2 u, allura, la l-pagament kien awtentikat b'mod sħiħ mill-Ilmentaturi bilfors kien hemm negliġenza grossolana min-naħa tagħhom li tagħmilhom għal kollox responsabbli għall-konsegwenzi tal-frodi li ġarrbu.

Konsultazzjoni mal-*Malta Communications Authority*

Biex l-Arbitru jifhem l-intriċċi teknoloġiċi dwar kif frodist jista' jippersonifika ruħu qisu l-bank biex jiffroda lill-klijenti, stieden għal konsultazzjoni lill-espert tas-*security* kemm tal-BOV kif ukoll tal-*Malta Communications Authority* (MCA).

Mill-konsultazzjoni joħroġ illi dan it-tip ta' frodi magħruf teknikament bħala *Spoofing* u *Smishing* jew kollettivament bħala *Social Engineering Scams,* ma jippermettix lill-bank li jieħu xi prekawzjoni (għajr ovvjament twissijiet effettivi biex il-klijenti joqgħodu attenti) biex il-frodist ma jkunx jista' juża dan il-kanal ta' komunikazzjoni biex jiffroda lill-klijenti.

Analiżi u konsiderazzjoni

L-Arbitru huwa tal-fehma li għall-fini ta' trasparenza u konsistenza, biex jasal għal deċiżjonijiet dwar ilmenti bħal dawn, ikun floku li jippubblika mudell dwar kif jaħseb għandha tinqasam ir-responsabbiltà tal-frodi bejn il-bank konċernat u l-klijent iffrodat u dan billi jieħu konsiderazzjoni ta' fatturi li jistgħu ikunu partikolari għal kull każ.

Għal dan il-għan, l-Arbitru qed jannetti ma' din id-deċiżjoni mudell li ppubblika u li ser jiġi wżat biex jasal għal deċiżjoni dwar kif ser isir '*apportionment'* tal-konsegwenzi tal-frodi. Il-mudell fih ukoll diversi rakkomandazzjonijiet biex il-banek ikomplu jsaħħu l-protezzjoni tal-konsumatur kontra frodisti li kulma jmur dejjem isiru aktar kapaċi u kreattivi.

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

Iżda l-Arbitru jħoss il-bżonn jemfasizza bil-qawwa li filwaqt li huwa minnu li l-banek ma għandhomx mezz kif jipprojbixxu li jsir *spoofing/smishing* fil-mezzi ta' komunikazzjoni li jużaw mal-klijenti, m'humiex jagħmlu biżżejjed biex iwissu b'mod effettiv lill-klijenti biex joqgħodu attenti; biex ma jagħfsux *links* li jkunu f'dawn il-messaġġi avolja jkun jidher li ġejjin mill-bank konċernat fuq il-mezz li normalment juża l-bank biex jibgħat messaġġi lill-klijenti.

Mhux biżżejjed li jagħmlu avviżi kontinwi fuq il-websajt tagħhom. Mhux biżżejjed li joħorġu twissijiet fuq il-*mass media* jew *social media*. Il-konsumatur huwa impenjat bil-problemi tal-ħajja ta' kuljum u ma għandux jiġi pretiż li billi jsir avviż fuq il-websajt, fil-ġurnali/TV, jew fuq il-paġna ta' *Facebook* tal-bank, b'daqshekk il-konsumatur jinsab infurmat. F'każijiet serji ta' frodi bħal dawn jeħtieġ li l-banek jużaw komunikazzjoni diretta mal-klijent permezz ta' SMS jew *email*. Dan l-aspett huwa wieħed mill-fatturi inklużi fil-mudell.

Min-naħa l-oħra, l-Arbitru jifhem li l-fatt li l-klijent jiżbalja billi jagħfas *link* li jkun ġie mwissi biex ma jagħfasx għax tista' tkun frawdolenti, b'daqshekk din ma tkunx awtomatikament taqa' fil-kategorija ta' negliġenza grossolana skont il-liġi.

Il-Qorti Ewropea tal-Ġustizzja (CJEU) fil-każ ta' *Wind Tre and Vodafone Italia*[33] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent.

L-Arbitru jara ilmenti minn ilmentaturi li faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[34] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

Għalhekk, il-banek jeħtieġ li jkollhom sistema ta' pagamenti robusta biżżejjed biex il-pagament ma jsirx jekk ma jkunx speċifikament awtorizzat mill-klijent/ilmentatur. Il-banek ma jistgħux ma jerfgħux responsabbilità jekk iħallu toqob fis-sistemi tagħhom li permezz tagħhom il-frodist ikun jista', bla ma jkun hemm aktar involviment tal-klijent/ilmentatur, jagħmlu awtorizzazzjoni speċifika tal-pagament a favur tal-frodist. Dan il-fatt huwa wkoll inkluż fil-mudell.

[33] Deċiżjoni 13 Settembru 2018 C-54/17
[34] *Article 64 of PSD 2*

Il-mudell jagħti wkoll konsiderazzjoni għal xi ċirkostanzi partikolari tal-każ. Jista' jkun hemm ċirkostanzi partikolari fejn il-messaġġ tal-frodist ikun anqas suspettuż. Ċirkostanzi fejn il-klijent ikun f'negozjati għal xi self mill-bank jew li l-klijent ikun imsiefer u jkun qed jagħmel tranżazzjonijiet li mhux soltu jagħmilhom, u b'hekk inaqqsu s-suspett tal-klijent li l-messaġġ li rċieva jista' jkun frawdolenti.

Il-mudell għandu wkoll għarfien dwar jekk l-Ilmentatur ikunx midħla tas-sistemi ta' pagamenti *online* mal Bank billi jkun għamel xi pagament simili (ġenwin) fit-12-il xahar ta' qabel. Dan jgħin ukoll biex tiġi ffurmata opinjoni jekk il-*monitoring* tal-pagamenti li l-Bank huwa doveruż jagħmel (kif spjegat fil-mudell) huwiex effettiv.[35] [36]

Applikazzjoni tal-mudell għal dan l-ilment

L-Arbitru jiddeċiedi skont kif provdut f'Artiklu 19(3)(b) b'referenza għal dak li, fil-fehma tiegħu, ikun ġust, ekwu u raġonevoli fiċ-ċirkostanzi u merti sostantivi tal-każ.

Meta l-Arbitru japplika l-mudell propost għal dan il-każ partikolari, jasal għal din id-deċiżjoni:

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentaturi**
Ilmentatur li jkun wera traskuraġni grossolona	0%	100%
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	50%	(50%)

[35] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS *supplement* ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[36] PSD 2 EU 2015/2366 Artiklu 68(2).

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentaturi**
Żieda għax l-Ilmentatur ikkopera b'mod sħih biex sar il-pagament ilmentat	(30%)	30%
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	(0%)	0%
Sub-total	20%	80%
Tnaqqis għal ċirkostanzi speċjali	30%	(30%)
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	20%	(20%)
TOTAL FINALI	**70%**	**30%**

Għalhekk, skont il-mudell, l-Ilmentaturi għandhom iġorru 30% tal-piż u s-70% l-oħra jġorrhom il-BOV.

Il-mudell isib li l-fatt li l-Ilmentaturi baqgħu jikkoperaw mal-frodist billi mlew l-ammont u l-aħħar 5 ċifri fis-*Signatures* tal-App, u anke daħħlu s-6-*digit code* li tagħti l-aħħar awtorizzazzjoni biex isir il-pagament, iżid id-doża ta' negliġenza tal-Ilmentaturi.

Il-mudell isib ukoll li m'hemmx lok għal żieda fir-responsabbilità tal-Ilmentaturi għax qatt ma kienu irċevew twissija diretta mill-BOV biex ma jagħfsux fuq *links* li jidhru f'*emails* jew SMS li jidhru ġejjin mill-Bank.

L-Arbitru jiskuża l-Ilmentaturi għax qatt ma kienu għamlu pagamenti onlajn simili u, allura, ma kinux midħla tal-pannelli ta' *Signature* 2 li tawtorizza pagament.

Iżda l-Arbitru jħoss li f'dan il-każ hemm ċirkostanzi ferm speċjali li jimmeritaw skuża b'doża ta' 30% u mhux biss ta' 20% indikati fil-mudell. Il-fatt li l-Ilmentaturi kienu ilhom xhur alloġġjati Londra għal kura ta' mard gravi, irrenda inevitabbli li jippanikjaw meta rċevew komunikazzjoni li kienu ser jitilfu l-aċċess għal flushom. Imsefrin kif kienu ma setgħux imorru personalment il-Bank u seta' kien diffiċli jikkomunikaw mal-Bank fil-ħin. Il-fatt li l-BOV kien qed isus fuqhom biex jaġġornaw il-profil tagħhom wassal biex l-*email* qarrieqa tnissel aktar ansjetà u żiedet il-konvinzjoni li kienet komunikazzjoni ġenwina tal-Bank.

Għalhekk, l-Arbitru qed iżid l-allokazzjoni normali ta' 20% għal 30% rigward ċirkostanzi speċjali peress li f'dan il-każ, maċ-ċirkostanza speċjali ta' safar, tiżdied it-tul u n-natura tas-safar.

B'kollox, għalhekk, l-Arbitru qed isib lill-Ilmentaturi intitolati għal kumpens ta' 70% tal-pagament frawdolenti li ġie debitat lill-kont tagħhom.

L-Arbitru ma jsibx lil BOV li naqas b'xi mod u ppreġudika l-pożizzjoni tal-Ilmentaturi għax ir-*recall* tal-pagament konċernat ma tatx riżultat. La l-pagament jiġi approvat fuq bażi *same day*, mhux probabbli li *recall* tista' twaqqfu.

Lanqas ma jista' jlum lil BOV li ma bagħatx SMS biex jinforma lill-Ilmentaturi dwar il-pagament għax sa issa ma hemmx regola li tobbliga lill-Bank jagħmel dan.

Anke kieku ntbagħat SMS fil-ħin, kien ikun diffiċli jitwaqqaf pagament li jkun ġie pproċessat fuq bażi *same day*.

Dwar jekk il-Bank kellux indizzji biżżejjed biex jinduna bil-frodi u jwaqqaf il-pagament, dan ma jirriżultax ġaladarba kien pagament uniku u li kien jidher awtentikat kif suppost. Ovvjament mhux possibbli li l-Bank jagħmel kuntatt ma' kull klijent li jagħmel xi pagament li ma jkunx tas-soltu għax m'hemmx obbligu ta' moniteraġġ ta' tranżazzjoni '*in real time*'. Jekk xejn, obbligu bħal dan jiskatta jekk ikun hemm serje sħiha ta' pagamenti mhux tas-soltu.

Għaldaqstant, *ai termini* tal-Artikolu 26(3)(c)(iv) tal-Kap. 555 tal-Liġijiet ta' Malta, l-Arbitru qed jordna lil *Bank of Valletta p.l.c.* iħallas lill-Ilmentaturi s-somma ta' tlett elef u erbgħa w għoxrin punt sebgħa żero ewro (€3,024.70).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti l-imgħax bir-rata ta' 2.90% fis-sena[37] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[38]

Peress li l-piż ġie allokat bejn il-partijiet, kull parti ġġorr l-ispejjeż tagħha.

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

Nota ta' Informazzjoni relatata mad-Deċiżjoni tal-Arbitru

Dritt ta' Appell

Id-Deċiżjoni tal-Arbitru legalment torbot lill-partijiet, salv id-dritt ta' appell regolat bl-artikolu 27 tal-Att dwar l-Arbitru għas-Servizzi Finanzjarji (Kap. 555) ('l-Att'), magħmul quddiem il-Qorti tal-Appell (Kompetenza Inferjuri) fi żmien għoxrin (20) ġurnata mid-data tan-notifika tad-Deċiżjoni jew, fil-każ li ssir talba għal kjarifika jew korrezzjoni tad-Deċiżjoni skont l-artikolu 26(4) tal-Att, mid-data tan-notifika ta' dik l-interpretazzjoni jew il-kjarifika jew il-korrezzjoni hekk kif provdut taħt l-artikolu 27(3) tal-Att.

Kull talba għal kjarifika tal-kumpens jew talba għall-korrezzjoni ta' xi żbalji fil-komputazzjoni jew klerikali jew żbalji tipografiċi jew żbalji simili mitluba skont l-artikolu 26(4) tal-Att, għandhom isiru lill-Arbitru, b'notifika lill-parti l-oħra, fi żmien ħmistax (15)-il ġurnata min-notifika tad-Deċiżjoni skont l-artikolu msemmi.

Skont il-prattika stabbilita, id-Deċiżjoni tal-Arbitru tkun tidher fis-sit elettroniku tal-Uffiċċju tal-Arbitru għas-Servizzi Finanzjarji wara li jiskadi l-perjodu tal-appell. Dettalji personali tal-ilmentatur/i jkunu anonimizzati skont l-artikolu 11(1)(f) tal-Att.

[37] Ekwivalenti ghall-*'Main Refinancing Operations (MRO) interest rate'* kurrenti stabbilita mill-Bank Ċentrali Ewropew.

[38] [38] Fil-każ li din id-deċiżjoni tiġi appellata, u tali deċiżjoni tkun ikkonfermata fl-appell, l-imgħax pagabbli jiġi kkalkolat mid-data tad-deċiżjoni tal-Arbitru.