Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 033/2024

VD

('Ilmentatur')

Vs

Bank of Valletta p.l.c.

Reg. Nru. C 2833

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

Seduta tas-26 ta' Lulju 2024

Dan huwa ilment li jirrigwardja pagament frawdolenti li sar għan-nom tal-Ilmentatur lil terzi mill-kont li għandu mal-Provditur 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 il-mezzi ta' komunikazzjoni normalment użati bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *e-mail.*
- 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-*website* 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, il-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-piż tal-pagament frawdolenti. Il-klijent isostni li l-Bank ma pproteġihx meta ħalla kanal ta' komunikazzjoni li 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:

- Fid-19 ta' Jannar 2024, għall-ħabta ta' 09:05, l-Ilmentatur irċieva l-messaġġ frawdolenti fuq il-*mobile* permezz ta' SMS fejn is-soltu jirċievi notifiki mill-BOV.[1]

- Billi l-Ilmentatur ħaseb li dan kien messaġġ ġenwin mill-BOV, għafas il-*link* u daħal f'*website* li huwa ħaseb li kienet tal-BOV għax dehret identika.

- Mexa pass pass mal-istruzzjonijiet kollha li tah il-frodist u, permezz t'hekk daħħal id-dettalji biex isir pagament ta' GBP1,990 ekwivalenti għal €2.382.66.[2]

[1] Paġna (p.) 89
[2] P. 12

- Dan sar f'kont tal-bank tal-frodist fil-Gran Brittanja (GB) u l-frodist kien poġġa struzzjonijiet biex il-pagament isir '*same day priority payment*'.[3]

- B'mod qarrieqi, l-pagament kien jindika li l-benefiċjarju kien jisimha Denicka Cooper u bħala dettalji tal-pagament indika *"Please make sure help goes towards mother".* Indika l-indirizz tal-benefiċjarju bħala XXXXXXX, biex inaqqas xi suspett mis-sistema tal-BOV li tagħmel *monitoring* tal-pagamenti.[4]

- Il-BOV bagħat SMS[5] wara li sar il-pagament biex jinforma b'dan lill-Ilmentatur.

- L-Ilmentatur kien pront ċempel lill-BOV fuq in-numru indikat biex jirrapporta l-frodi iżda l-pagament diġà kien ġie pproċessat peress li kien fuq bażi *same day*.

- Sar *recall* mill-BOV iżda dan ma ġiex aċċettat mill-Bank benefiċjarju.[6]

- Il-każ ġie rrapportat lill-pulizija għal aktar investigazzjoni tal-frodi.[7]

L-Ilment[8]

L-Ilmentatur saħaq li l-SMS frawdolenti kien irċevih fuq l-istess numru li s-soltu jirċievi messaġġi mill-BOV. Qal li l-Bank qatt ma kien infurmah biex joqgħod attent minn messaġġi bħal dawn, u kien biss wara, fil-5 ta' Frar 2024 li rċieva twissija bħal din fuq l-istess SMS.

Sostna li huwa ma kienx awtorizza l-pagament konċernat u meta ċempel lill-Bank ftit wara li rċieva notifika li kien sar il-pagament (fil-ħin ta' 16:44 fil ġurnata tal-Ġimgħa), ġie nfurmat li *recall* seta' jsir biss it-Tnejn filgħodu. Sostna li kieku l-Bank għamel ir-*recall* mal-ewwel kif huwa rrapporta, kieku kien ikun hemm ċans li l-pagament jinżamm.

[3] *Ibid*.
[4] *Ibid*.
[5] P. 90
[6] P. 84
[7] P. 16 - 17
[8] P. 1 – 6 u dokumenti annessi p. 7 - 17

Bħala rimedju huwa talab lill-Provditur tas-Servizz jirrifondilu l-pagament ta' €2.382.66 u l-ispejjeż relatati ta' €32.

Risposta tal-Provditur tas-Servizz

Fir-risposta tagħhom, il-BOV qalu:

1. *"Whereas Mr. VD (''the complainant'') states that "I was scammed through the messaging system used by the bank to send me official sms.''*[9] *Mr. VD did not attach a copy of this SMS, however, from the information provided it seems that he received this SMS on the 19th of January 2024 and it informed him to 'access a link to verify my signatures.'*[10]

2. *Whereas the complainant attached the details of the transaction in question, bearing transaction ID number 137623510.*[11] *According to the Bank's records, this transaction was duly authorised on the 19th of January 2024 at 09:25.*[12] *As part of the Bank's security system which is in line with the Payment Services Directive 2 (PSD 2), there are various levels of authentication to ensure that the transaction was carried out by the complainant, from credentials and systems registered in his name. In fact, this transaction had no indication that it was fraudulent.*

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

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

[9] Fol. 002 of the complaint
[10] Fol. 007 of the complaint
[11] Fol. 012 of the complaint
[12] DOC.A: Log of transaction

> *'**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:*

> *'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 himself in his token which is either the BOV app or the physical internet banking key (this is the element of*

[13] Article 4(30) of PSD2.

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) 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 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 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*

[14] DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' P. 5

*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 Mr. VD which he has previously used to make other payments which he 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.)*

   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 above-mentioned Commission Regulation provides that the Bank can decide to not apply strong customer authentication for transactions which are considered to have a low level of risk.*[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 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).

[15] *Ibid*., P. 4
[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.

11. *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.***

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 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 recipient's 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'. He could have confirmed this SMS with the Bank who would have immediately informed him that the SMS was not genuine.*

14. *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 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 BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party.'*[18]

15. *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 Bank's website or from the BOV Mobile App. Whereas the Bank never before requested the complainant (or any other customer) to access their internet Banking from a link in a SMS, because it has the adequate systems for this service to be accessed.*

    In fact, the Bank warns customers to be careful what information they disclose, particularly on links. In fact, in May 2014, the published 'Tips for Safer Mobile Banking'[19] *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.*

[18] DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' P. 7
[19] DOC.F: '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.'*

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 above-mentioned document and others similar to it are easily accessible from the Bank's 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.*

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.'*[20]

    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 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*

[20] DOC.G: 'Spot the Scam: Bank impersonation Scams'

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 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, on the 11th of November 2023 at approximately 13:02, the Bank sent an SMS to Mr. VD with the following text:*

    '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.'

21. *Therefore, it is unfounded for Mr. VD to say that 'the bank never informed me personally by sending me an sms or email about this type of scam.'*[21] *He states that 'the bank sent me an sms to warn me about the scam on the 5th of February 2 weeks after I fell victim.'*[22] *As explained, the Bank had sent Mr. VD an SMS in November and the SMS he is referring to, which was sent in February, was part of the second set of SMS sent by the Bank to warn its customers. These SMS's are being sent every 3 months.*

22. *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'*[23] *which provides the following:*

    - *Use the genuine internet website of the bank. Never access the bank's website through links contained in emails or SMS, unless you are sure of the identity of the sender. It is always best to access the bank's website by* ***typing in the web address, as provided by the bank, directly in the browser.***

[21] P. 3 of the complaint
[22] *Ibid*.
[23] 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.*

23. *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.*

24. *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.*

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

<u>Timeline of Events</u>

26. *Whereas the payment was approved on the 19th of January 2024 at 09:25. 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'.

27. *Therefore, when the complainant called the Bank on the 19th of January 2024 at 17:07, the representative blocked the cards and internet banking of the complainant. The following working day, Bank also made a recall request to the beneficiary banks, which request is made through a digital, internal system between Banks.*

28. *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. Therefore, the suggestion of the complainant that BOV 'could have alerted the foreign bank to keep this money'[24] is not possible to implement since BOV cannot dictate to other Banks what procedure to follow.*

29. *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. VD accordingly (**'DOC.I'**). The complainant states that this negative reply was 'due to the delay of 3 days to start this procedure.'[25]*

    As explained, Mr. VD called the Bank on Friday after business hours and as per procedure, the recall was initiated the next working day which was Monday.

30. *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.

[24] P.3 of the complaint
[25] *Ibid*.

Conclusion

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

32. *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.

33. *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.*

34. *The Bank reserves all rights/actions pertaining to it at law, and respectfully requests the Arbiter to reject and dismiss the complaint's claims."*[26]

Seduti

Saru żewġ seduti nhar it-3 ta' Ġunju 2024[27] u s-17 ta' Ġunju 2024.[28]

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

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

[26] P. 23 – 29 u dokumenti annessi p. 30 - 84
[27] P. 85 - 87
[28] P. 93 - 96

Qal ukoll:

"***Dak il-ħin jien ma ndunajtx li kienet scam u ħsibt li jekk m'inix ser nagħmilha, ma nkunx nista' nuża l-Internet Banking biex nixtri online jew xi ħaġa hekk.***

Dħalt fiha, tidħol f'website bil-logo tal-BOV. Jgħidlek biex iddaħħal il-User ID, li ddaħħal is-soltu, imbagħad, jagħtik step-by-step xi trid tagħmel fuq l-app tal-Mobile Banking (għax jien l-app użajt mhux l-Internet Banking). Imbagħad, tidħol f'Signatures u jagħtik xi numri li trid iddaħħalhom u trid iddaħħal xi numri fil-website. Imbagħad, jgħidlek, 'You can use your Signatures', xi ħaġa hekk. Ma niftakarx eżatt għax għadda ħafna żmien.

Ngħid li, mbagħad, fl-għaxija nirċievi SMS nerġa' mill-BOV, f'16:44, qisu xi seba' sigħat wara, li ħareġ payment mill-kont li għandi u jekk il-payment ma kienx awtorizzat, biex inċempel immedjatament.

Ngħid li hekk għamilt, ċempilt immedjatament imma milli jidher kien għadda ħafna ħin u l-flus kienu laħqu telqu minn Malta. L-ewwelnett, dakinhar ma kinux qabduhom għax kienu għalqu l-uffiċċju tat-transactions. Imbagħad, it-Tnejn kienu qaluli li l-flus kienu diġà telqu.

Ngħid li rajt żewġ affarijiet li ma sarux sew.

1. ***Jien ma kontx naf din tas-Signatures x'inhi; li mis-Signatures qed tagħti l-flus, u qatt ma jgħidlek li hemm transaction għaddejja. Meta tajt il-flus kien dejjem lil third party u trid iddaħħal ħafna dettalji: dettalji tal-klijent li ser tibgħatlu l-flus; il-currency; l-ammont; l-IBAN number sħiħ.***

   Ngħid li dawn qatt ma għamilthom meta dħalt f'din l-iscam. Fl-aħħar, xorta, meta tawtorizza jagħtik summary sħiħa ta' x'awtorizzazzjoni tkun ser tagħmel, jiġifieri din qatt ma rajtha fl-app jiena.

2. ***It-timing tal-message – kieku l-message intbagħat mill-ewwel, kif jintbagħtuli messages meta nkun għamilt online shopping, (meta nawtorizza x-shopping jibgħatli message li jien għamilt ix-shopping), kieku kien ikolli ċans inċempel biex inwaqqaf din it-transaction."***[29]

Waqt il-kontroeżami, l-Ilmentatur ikkonferma li kontra dak li kien iddikjara fl-Ilment, fil-11 ta' Novembru 2023 kien irċieva twissija fuq l-istess SMS mill-BOV

[29] P. 85 - 86

biex joqgħod attent u ma jagħfasx fuq *links* għax il-Bank ma jibgħatx *links* fuq SMS.[30]

Sostna wkoll:

"Jien ma mortx Pay third party. Ma qallix biex immur Pay third party u ndaħħal il-beneficiary name; jgħidlek Select Relation, Select Reason, tagħmel Continue u, mbagħad, tagħmel il-currency, Euro. Ngħid li dawn l-affarijiet qatt ma għamilthom jien. Ngħid li jien qatt ma mort Signatures biex nagħmel Pay third party.

Ngħid li meta nkun irrid nagħmel pagament normali, nidħol Home tal-BOV Mobile, hemm My Financials, hemm Mobile Payment, Mobile Top Up u BOV Signatures. BOV Signatures qatt ma mort jien meta nagħmel Pay Third Party.

Ngħid li l-ewwel darba li dħalt fiha din; qatt ma kont dħalt fiha.

Ngħid li ma kontx naf li qed nagħmel xi transactions.

Ngħid li meta nkun irrid nagħmel pagament, indaħħal id-dettalji kollha. Ngħid li jiena mhux bl-Activation Code nagħmilha imma bil-Biometric."[31]

Min-naħa l-oħra, l-BOV isostni li huwa kien għal kollox konformi mal-liġi kif tipprovdi l-PSD 2[32] u l-*Banking Directive* 1[33] 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-Ilmentatur bilfors kien hemm negliġenza grossolana min-naħa tiegħu li tagħmlu għal kollox responsabbli biex iġorr il-konsegwenzi tal-frodi li ġarrab.

Xehed Michael Gatt, *Senior Manager* fil-*Payments Section* tal-Bank li qal:

"*Bħal kwalunkwe tranżazzjoni li tiġi awtorizzata mill-Internet Banking tista' ssir jew bil-Physical Key jew mill-Mobile App. Fil-każ tal-Mobile App tmur fuq il-mobile tiegħek. Il-mobile tiegħek ikollu PIN jew biometrics. Tiftħu, tagħżel l-App, tagħżel Signature 1 jew Signature 2, f'dan il-każ, Signature 2. Kif inti tmur*

[30] P. 91
[31] P. 87
[32] *Directive (EU) 2015/2366 commonly referred to as PSD 2meant to safeguard the consumer (PSU) from having responsibility for payments which are not properly authorised.*
[33] *Directive 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which is modelled on the requisites of Directive (EU) 2015/2366.*

fuq Signature 2, ser iddaħħal l-amount. Għandek ukoll il-Payee Code. Kif inti tagħtih biex ikompli, ser jitolbok il-PIN, u mbagħad tiġi ġġenerata l-One-Time Password.

Imbagħad titlaq it-tranżazzjoni. Mingħajr dawn l-isteps kollha li semmejt, it-tranżazzjoni ma tistax titlaq.

Ngħid li l-One-Time Password, flimkien mal-Login ID u s-six-digit number li jkun jaf biss il-User, tintuża biex inti tilloggja fl-Internet Banking biex tara l-account tiegħek u l-bilanċi. Bis-Signature 1 biss ma jiġri xejn. U hemm ukoll is-Signature 2. Sabiex it-tranżazzjoni tiġi ffirmata, għandek dawk l-isteps kollha u t-tranżazzjoni titlaq.

Once li t-tranżazzjoni tiġi awtorizzata – f'dan il-każ kienet instant payment – din it-tranżazzjoni tintbagħat min-naħa tal-bank."[34]

Peress li l-Ilmentatur kien qed isostni li meta għamel pagamenti normali qatt ma kien daħal fis-sezzjoni ta' *Signatures* u jiġġenera s-6-*digit code* biex jawtorizza l-pagament, Michael Gatt intalab jispjega jekk l-Ilmentatur kienx żbaljat u qal:

"***Le, għax l-awtorizzazzjoni ssir jew bil-PIN jew bil-biometrics. Infatti, għalhekk il-limits fuq il-mobile banking huma baxxi aktar milli huma fuq l-Internet Banking. L-ilmentatur jawtorizza bil-biometrics meta jidħol Payment to Third Party jagħmel, per eżempju, tranżazzjoni ta' €100, juża l-fingerprint u titlaq. F'dan il-każ, il-frodista talbu biex jgħaddi għas-Signature 2 u skont il-logs, għamel dak kollu fis-Signature 2.***

Il-code tal-aħħar biex tiġi approvata t-tranżazzjoni bilfors irid jiġi ġġenerat mis-Signature 2 jew inkella bil-Physical Key li f'dan il-każ m'għandux."[35]

Sar ukoll kontroeżami dwar il-fatt li l-SMS li kkonferma li sar il-pagament intbagħat lill-Ilmentatur diversi sigħat wara li huwa allegatament kien awtorizza l-pagament u, għalhekk, seta' ppreġudika l-possibilità li l-pagament jiġi mwaqqaf.

Michael Gatt qal:

"***Mistoqsi jekk tranżazzjoni titlaqx mill-ewwel mill-bank, jekk il-flus jitilqux mill-ewwel jew jekk hemmx xi ċans li wieħed jista' jwaqqafhom peress li meta***

[34] P. 93 - 94
[35] P. 94

l-ilmentatur ċempel lill-Customer Care, qalulu ser jiċċekkjaw laħqux telqu l-flus għax kieku jwaqqfuhom.

Ngħid li fil-każ tal-ilmentatur, il-frodista daħal BIC Code ħażin. Meta jiġri hekk, jew ikun hemm xi żball li l-bank jista' jirranġa l-pagament, ma jibqax fil-kju normali imma jmur fil-kju li jgħidulu 'Repair'. Hemmhekk issirlu manual intervention u l-pagament jitlaq. Meta jitlaq il-pagament, inti tirċievi l-SMS.

Qed jingħad li l-ilmentatur irċieva l-SMS seba' sigħat wara. Ngħid għax il-frodista daħħal BIC Code (Bank Identifier Code) ħażin.

L-Arbitru jintervjeni u jgħid li mhux qed isegwi għax it-Transaction Log kollha turi 'Success', waħda wara l-oħra u jistaqsi jekk minn din it-Transaction Log jirriżultax li ddaħħal code ħażin.

Ngħid li dik it-tip ta' tranżazzjoni kellha l-BIC Code ħażin. Meta jiġri hekk – il-frodista ddeċieda li jdaħħal il-BIC Code hu – il-bank ma jibqax Straight to Processing, tiġi Non-STP. Il-bank għandu dipartiment li jirranġa dawn it-tip ta' tranżazzjonijiet, biex it-tranżazzjoni tkun tista' titlaq. Ma jkun hemm xejn suspettuż għax once li t-tranżazzjoni awtorizzajtha inti, awtorizzajtha inti.

F'dan il-każ, il-code li daħħal il-frodista kien BARCGB2XXX u dak mhuwiex tajjeb.

L-Arbitru jistaqsi lix-xhud minn fejn joħroġ dan kollu mid-dokumenti li ġew ippreżentati mill-bank.

Ngħid li meta aħna rajna l-logs hawnhekk għandek, 'Your instructions have been received and have been reviewed. Please do not resubmit this payment,' jiġifieri minn hemm ġie triggered li t-tranżazzjoni ser tiġi reviewed, u għidna ħa naraw għalfejn it-tranżazzjoni ser tiġi reviewed. U r-raġuni għalfejn ġiet reviewed hija għaliex kien hemm a wrong BIC. Ovvjament, il-klijent ma jkunx jaf.

Mistoqsi mill-Arbitru jekk din tkunx ta' trigger biex nikkuntattjaw lill-klijent, ngħid li le, hija proċedura normalissima li jkun hemm ħafna għal raġunijiet differenti li pagament issirlu manual intervention.

Ngħid li kien hemm delay u aħna ċċekkjajna u spjegajna lis-Sur VD għalfejn kien hemm din id-delay.

L-ilmentatur jgħid li fuq l-SMS hemm miktub li jekk it-tranżazzjoni mhix awtorizzata biex iċċempel, ngħid li kif nista' nispjega, l-bank mhux obbligat li

jibgħat SMS u l-SMS mhuwiex a security measure. L-SMS qiegħed hemm biex jekk it-tranżazzjoni ma' tkunx konformi mal-affarijiet tiegħek, inwaqqfu kollox u ma jerġgħux isirulek tranżazzjonijiet oħra.

L-ilmentatur jistaqsi r-raġuni 'Please make sure that help goes towards mother,' kellux iqanqal imqar suspett żgħir, u jekk tali raġuni kinitx raġuni li wieħed jagħti lill-bank, ngħid li dak huwa free text u jkun hemm ħafna raġunijiet li jagħmlu sens biss għall-klijent li jkun qed jagħmel il-pagament. Ngħid li once li inti ffirmajt, bħal meta tiffirma ċekk, l-obbligu tagħna hu li nipproċessaw il-pagament.

Ngħid li fil-pagamenti kollha li kien hemm, kien hemm il-BIC Code ħażin u għalhekk kien hemm żball li ried jiġi indirizzat. Il-pagamenti meta saru, saru Same Day, dakinhar li s-Sur VD rċieva l-SMS li semma l-aħħar darba. By the time li s-Sur VD rċieva l-SMS, xorta mar on a Same Day basis u dan ifisser li ma tkunx tista' twaqqfu. Jekk ma jkunx Same Day u klijent iċempel mill-ewwel ikun hemm ċans li jitwaqqaf imma peress li sar Same Day ma tkunx tista' twaqqfu.

L-ilmentatur jgħid li, allura, jekk f'dawk is-seba' sigħat induna bil-pagament xorta ma setax iwaqqafhom il-flus.

Il-pagament ma sarx immedjatament kif il-frodist għamel it-tranżazzjoni, ma sarx fid-09:26. Il-pagament sar diversi sigħat wara u l-ilmentatur ma setax jinduna li sar pagament jekk il-pagament kien għadu ma sarx."[36]

Sottomissjonijet finali

Fis-sottomissjonijiet finali tiegħu, l-Ilmentatur saħaq:

"*Wara li smajt il-verżjoni tal-ħaddiema tal-BOV jien xorta nibqa' nsostni li l-bank naqas milli jipproteġini mill-frodi diversi drabi. Meta ssir tranżazzjoni minn fuq il-mobile u tasal fl-aħħar step biex tawtorizzaha l-app tal-bank itellalek summary ta' xi tkun qiegħed tawtorizza biex jekk ma taqbilx ma' xi ħaġa twaqqaf kollox. Imma f'dan il-każ qabel ma għamilt l-awtorizzazzjoni, l-app m'urietni xejn x'kont qed nawtorizza allura jien ma stajtx ninduna li kont qed nagħmel tranżazzjoni ta' flus meta jien kont mingħalija qiegħed niżblokka s-signatures kif qalli fil-messaġġ li rċevejt fuq in-numru tal-bank.*

[36] P. 95 - 96

It-tieni punt fejn naħseb li l-bank naqas lejja hu meta s-sistema tal-bank waqqfet it-tranżazzjoni biex isir intervent manwali. Jien nifhimha li la kien hemm xi ħaġa ħażina fit-tranżazzjoni, f'dan il-każ il-BIC code ħażin, tal-inqas il-persuna li tkun qed tiċċekkja l-affarijiet tikkuntattja l-klijent biex tgħidlu. U b'hekk il-klijent jista' jikkonferma jew le jekk għandhiex titkompla t-tranżazzjoni. L-obbligu tal-bank mhux biss li jsir il-pagament imma wkoll li jkun hemm kollox sew aktar u aktar meta jidħlu pagamenti li ħa jmorru barra l-pajjiż. F'dan il-każ, il-bank iddeċieda waħdu li jibdel il-BIC code hu u lili ma nfurmani b'xejn meta dawn kellhom ħin biżżejjed għax il-pagament dam 7 sigħat biex ħareġ wara li saret it-tranżazzjoni u b'hekk kont inkun nista' nikkonferma li l-pagament m'awtorizzajtux jien u l-flus ma kienu joħorġu qatt mill-kont."[37]

Min-naħa l-oħra, il-BOV apparti li reġa' saħaq dak li kien diġà qal rigward li l-pagament sar wara li l-Ilmentatur kien awtorizzah b'negliġenza grossolana, u li l-Bank kien konformi mar-regolamenti meta mexxa bil-pagament, żied ukoll:

"*Illi s-Sur VD jgħid li "meta ssir tranżazzjoni minn fuq il-mobile u tasal fl-aħħar step biex tawtorizzaha l-app tal-bank itellalek summary ta' xi tkun qiegħed tawtorizza biex jekk ma taqbilx ma' xi ħaġa twaqqaf kollox." Bir-rispett il-Bank jissottometti li jeżistu diversi tipi ta' pagamenti li wieħed jista' jagħmel permezz tas-sistemi tal-Bank. F'dan il-każ, il-pagament in kwistjoni huwa third-party payment magħmul permezz tal-internet baning u approvat permezz tal-BOV Mobile app. Il-proċedura li għandha tiġi segwita sabiex jiġi approvat dan it-tip ta' pagament hija dik spjegata f'DOC.B anness mar-risposta tal-Bank. F'dawn it-tip ta' pagamenti l-Bank ma jtellalekx 'summary' fuq l-app għaliex il-klijent ikollu biżżejjed indikazzjonijiet sabiex jinduna li qiegħed jagħmel pagament. Għaldaqstant, ma kien hemm l-ebda nuqqas min-naħa tal-Bank u s-sistemi tiegħu huma konformi mal-livell ta' sigurtà imposta fuq il-Bank mill-PSD2.*

Is-Sur VD jgħid li jħoss li l-Bank naqsu wkoll 'meta s-sistema tal-bank waqqfet it-tranżazzjoni biex isir intervent manwali'. Huwa jgħid li 'jien nifhimha li la hemm xi ħaġa ħażina fit-tranżazzjoni ... tal-inqas il-persuna li tkun qed tiċċekkja l-affarijiet tikkuntattja l-klijent biex tgħidlu.' Kif spjega x-xhud Michael Gatt, f'dan il-każ ġara li kien hemm il-BIC Code ħażin. Huwa spjega li:

[37] P. 98

*'meta jiġri hekk, **jew ikun hemm xi żball li l-bank jista' jirranġa**, l-pagament ma jibqax fil-kju normali imma jmur fil-kju li jgħidulu 'Repair'. Hemmhekk issirlu manual intervention u l-pagament jitlaq.'*[38]

F'dan il-każ hemm bżonn issir distinzjoni bejn żball li jista' jiġi rranġat mill-Bank f'pagament u żball li jaffettwa l-integrità tal-pagament, li Bank ma jkunx jista' jirranġa. Dan tal-aħħar huwa xi żball fl-awtorizzazzjoni tal-pagament, li ovvjament il-Bank ma jistax imiss għaliex inkella ma jkunx hemm il-kunsens tal-klijent għall-approvazzjoni tal-pagament ai termini tal-PSD2. F'dan il-każ kien hemm l-awtorizzazzjoni korretta tal-pagament, għaldaqstant il-Bank kien obbligat li jipproċessah. In fatti, kif spjega s-Sur Gatt, il-Bank għandu dipartiment li jirranġa dawk l-iżbalji minimi tal-pagamenti li jmorru fir-'repair' kju,[39] *sabiex il-Bank ikun jista' jaqdi l-obbligu tiegħu u jipproċessa l-pagamenti. Kif spjega s-Sur Gatt, meta pagament imur f'dan il-kju, 'ma jkun hemm xejn suspettuz' u 'hija proċedura normalissima li jkun hemm ħafna għal raġunijiet differenti li pagament isirlu manual intervention.'*[40]

In fatti, skont ir-records tal-Bank jirriżulta li l-pagament effettivament telaq mill-Bank fil-16:55:01 nhar id-19 ta' Jannar 2024 u ġie approvat fid-09:25:31. Għaldaqstant, fil-frattemp il-pagament kien fil-kju kif spjega s-Sur Gatt sabiex issir il-manual intervention u meta din saret, il-pagament telaq."[41]

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

[38] Seduta ta' nhar is-17 ta' Ġunju 2024, paġna 95 tal-proċess
[39] *Ibid*.
[40] P. 95
[41] P. 103 -104

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.

Iżda l-Arbitru jħoss il-bżonn jemfasiżża 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-*website* 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-*website*, 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*[42] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha

[42] Deċiżjoni 13 ta' Settembru 2018 C-54/17

anke konsumatur medju li jkun raġonevolament infurmat u attent. L-Arbitru jara ilmenti minn ilmentaturi li faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[43] 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, jagħmel awtorizzazzjoni speċifika tal-pagament a favur tal-frodist. Dan il-fatt huwa wkoll inkluż fil-mudell.

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.[44] [45]

Deċiżjoni

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:

[43] *Article 64 of PSD 2*
[44] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[45] PSD 2 Eu 2015/2366 Artiklu 68(2).

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	Perċentwal ta' ħtija tal-Ilmentatur
Ilmentatur li jkun wera traskuraġni grossolana	0%	100%
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	50%	(50%)
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ biex sar il-pagament ilmentat	(30%)	30%
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	(20%)	20%
Sub-total	0%	100%
Tnaqqis għal ċirkostanzi speċjali	20%	(20%)
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	0%	0%
TOTAL FINALI	20%	80%

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 80% tal-piż u l-20% l-oħra iġorrhom il-BOV.

Il-mudell isib li l-fatt li l-Ilmentatur baqa' jikkopera mal-frodist billi mela l-ammont u l-aħħar 5 ċifri fis-*Signatures* tal-App u anke daħħal is-6-*digit code* li tagħti l-aħħar awtorizzazzjoni biex isir il-pagament, iżid id-doża ta' negliġenza tal-Ilmentatur.

Il-mudell isib ukoll lill-Ilmentatur negliġenti li għamel dak li l-Bank kien espressament, permezz ta' SMS anqas minn 3 xhur qabel, qallu biex joqgħod attent u ma jagħfasx fuq *links* inklużi f'xi SMS li tista' tidher li tkun ġejja mill-Bank għax dan ikun *scam* peress li l-Bank qatt ma jibgħat *links* permezz ta' SMS.

Għalhekk, l-Arbitru ma jagħtix skuża ta' 20%, kif għamel f'diversi każi ma' dawk li ma jkunux irċevew twissija diretta permezz ta' SMS mill-Bank.

Lanqas jista' l-Arbitru jiskużah għax ma għamilx pagamenti *online* simili għax għalkemm qal li dawn kien jagħmilhom *online* u kien jimla d-dettalji huwa u ma kienx jidħol fis-*Signatures* għax kien japprova bil-*biometrics*, dan ma jibdilx is-sustanza li f'dan il-każ approva pagament hu stess u mela informazzjoni fis-*Signatures* li kienet ċara li kien qed isir pagament. Biex sar il-pagament, l-Ilmentatur daħħal l-ammount, daħħal l-aħħar ħames ċifri tan-numru tal-kont u daħħal is-6-*digit code* u dawn huma indizzji ċari li kien qed jagħmel pagament.

Iżda l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jiġi parzjalment skużat sa 20%.

Kif intqal waqt is-seduti, il-pagament ma telaqx mal-ewwel kif l-Ilmentatur allegatament awtorizzah, minkejja li kien fuq bażi '*same day priority payment*'. Dan għall-fatt li kien hemm żball bil-BIC (*Bank Identifier Code*) u b'hekk inħolqot ħtieġa li kellu jiġi approvat b'intervent manwali.

L-Arbitru jħoss li ġaladarba l-proċess ta' pagament kellu jiġi investigat b'mod speċifiku b'intervent manwali, kien hemm ċerti indizzji li setgħu iqajmu suspett li dan il-pagament ma kienx regolari. Dawn l-indizzji jinkludu li pagament kien qed isir *same day priority* lil persuna li kellha indirizz hawn Malta iżda f'kont ma' bank barrani, u r-raġuni tal-pagament kienet *'please make sure help goes towards mother'*.

Dawn mhux indizzji konklussivi iżda indizzji li l-Bank kien ra bħalhom f'pagamenti frawdolenti oħra u li setgħu xegħlu bozza biex il-pagament jiġi referut mill-ġdid mal-Ilmentatur.

B'kollox, għalhekk, qed jiġi intitolat għal kumpens ta' 20% tal-pagament frawdolenti li ġie debitat lill-kont tiegħu.

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

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-Ilmentatur is-somma ta' erba' mija u tlieta w sebgħin ewro punt erbgħa sebgħa. (€473.47)

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 4.25% fis-sena[46] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[47]

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

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

<u>Nota ta' Informazzjoni relatata mad-Deċiżjoni tal-Arbitru</u>

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-

[46] Ekwivalenti għall-*'Main Refinancing Operations (MRO) interest rate'* kurrenti stabbilita mill-Bank Ċentrali Ewropew.
[47] [47] 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.

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 anonimiżżati skont l-artikolu 11(1)(f) tal-Att.