Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 218/2023

ZO ('Ilmentatur')

Vs

Bank of Valletta p.l.c.

Reg. Nru. C 2833

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

Seduta tas-6 ta' Ġunju 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 l-mezż ta komunikażzjoni 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-*website* uffiċjali u dan permezz tal-kredenzjali li l-bank ikun taha 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'xi pajjiż Baltiku jew l-Irlanda minn fejn huwa kważi impossibbli li jsir *recall* effettiv tal-flus ġaladarba il-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 li kanal ta' komunikażżjoni 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-13 t'Ottubru 2023, l-Ilmentatur irċieva l-messaġġ frowdolenti fuq il-*mobile* permezz ta' SMS fejn is-soltu jirċievi notifiki mill-BOV.

- Billi l-Ilmentatur ħaseb li dan kien messaġġ ġenwin mill-BOV, għafas il-*link* u dahal 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'€4,321.

- Dan sar f'kont tal-bank tal-frodist fl-Irlanda u l-frodist kien poġġa struzzjonijiet biex il-pagament isir '*same day*'.[1]

[1] Pagna (p.) 12

- B'mod qarrieqi il-pagament kien jindika li l-benefiċarju kien jisimha Chloe Connolly[2] u bħala dettalji tal-pagament indika *"for my son, please spend wise"*

- Il-BOV bagħat SMS ftit wara[3] li sar il-pagament biex jinforma 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*.[4]

- Sar *recall* mill-BOV[5] iżda dan ma ġiex aċċettat mill-Bank tal-Irlanda.

- Il-każ ġie rrapportat lill-pulizija għal aktar investigazzjoni tal-frodi.[6]

L-Ilment

L-Ilmentatur saħaq li jara tliet raġunijiet għalfejn il-BOV kien negliġenti u kkawżalu dan it-telf:

1. "*This event happened on Friday afternoon and was reported immediatey from my end, however, the bank did not stop the payment which usually takes 3 – 4 days to arrive, and their excuse was that during the weekend they do not work.*

2. *During the instructions from the fraudulent website, there was a request for a signature 2 from the BOV app. On this screen, there is no warning whatsoever that by inputting a code in this section you are approving a payment request.*

3. *The number where this scammer was sending from was showing exactly the same as the BOV number and was even on the same*

[2] P. 12 Is-sistema SEPA timxi strettament skont l-*IBAN number* u s'issa ma tagħmilx konnessjoni mal-isem u l-indirizz tal-benefiċjarju kif dikjarat fit-trasferiment. Għalhekk, għall-frodist faċli jagħti isem u indirizz fittizju biex jevita xi mblokk mill-*monitoring systems* tal-Bank. Huwa ntiż li meta tidħol il-PSD 3 jew PSR 1, dan il-*linkage* bejn l-IBAN u l-identità tal-benefiċjarju tkun tassattiva.
[3] P. 20
[4] P. 18
[5] P. 84, 87, 88, 90, 93 - 95
[6] P. 14 - 16

conversation on my phone so there is no way that I can tell if the bank was sending the messages or someone else."[7]

Bħala rimedju, l-Ilmentatur talab li l-Bank jirrifondi l-pagament li huwa ma awtoriżżax għal €4,321 u spejjeż iddebitati lilu ta' €30.

Risposta tal-Provditur tas-Servizz

Fir-risposta tagħhom, il-BOV qalu:

1. *"Whereas ZO (''the complainant'') states that he had ''received a message from the original BOV number'' which informed him that his Visa Debit Card and mobile signatures are on hold and asked him to visit ''bov-ebanking.com'' or visit his branch.*[8] *He then proceeded with following the instructions provided in the link and ''after submitting this info it requested a signature 2 from the app and was stating what numbers to input on the app.''*[9]

2. *Whereas the complainant attached the details of the transaction in question, bearing reference number 2328603050332000. According to the Bank's records, this transaction was duly authorised on the 13th of October 2023 at 13:58. 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.*

[7] P. 3
[8] *Ibid.*
[9] *Ibid.*

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;*[10]

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.''

[10] Article 4(30) of PSD2.

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 possession of strong customer authentication). Besides this, he also inputted the last 5 digits of the IBAN number of the recipient, and this satisfies the element outlined in article 5(c) abovementioned.*

   Upon entering these details, a code would have been generated which needs to be used to approve the transaction. The customer accesses this section from the section entitled 'Transaction Signing', 'Signature 2' and then sees a section entitled 'Amount' and another entitled 'Payee Code'. This can be seen from the document attached as 'DOC.B' which is easily accessible on the Bank's website). These phrases all clearly indicate that one is approving a transaction.

   Therefore, it is completely unfounded for the complainant to say that 'on this screen, there was no warning whatsoever that by inputting a code in this section you are approving a payment request.'[11]

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*

[11] *Ibid*.

sent using your Security Number/s or BOV Mobile PIN or biometric data.'[12]

'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.'*[13]

8. *Whereas in fact, every token used to generate codes in order to approve a payment has a certificate associated with it. In fact, the certificate number associated with the token with which the payment in question was approved is the same one associated with the token of ZO 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.[14]

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

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

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.

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 recipients' IBAN. This fact should have raised suspicion within the complainant since if he had no intention of approving a payment,*

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

The complainant should also have exercised caution since as he said himself 'I was not sure of this message'[16] when he received it. Therefore, he could have confirmed this doubt 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.'[17]*

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 Banks' 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 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'[18] which amongst other provide the following:*

---

[16] *P. 3 of the complaint.*
[17] *DOC.C: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 7.*
[18] *DOC.F 'BOV Mobile Banking – Tips for Safer Mobile Banking'.*

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

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.'*[19] *It also explains what personal details such scam may ask for which indicates that the communication is not genuine.*

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*

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

Bank on social media in the 6 months preceding the incident of ZO. 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'[20] which provides the following:*

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

21. *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.*

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

22. *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.*

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

Timeline of Events

24. *Whereas the payment was approved on the 13th of October at 13:58. 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'.*

25. *Therefore, when the complainant called the Bank on the 13th of October 2023 at 14:01, the Bank blocked the cards and internet banking of the complainant. The Bank also made a recall request to the correspondent and beneficiary banks, which request is made through a digital, internal system between Banks. This request was made at 14:45 on the 13th of October to the correspondent bank and at 15:04 to the beneficiary bank. Multiple reminders were also sent by BOV as can be seen from 'DOC.I'.*

26. *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.*

27. *Therefore, the Bank respectfully submits that it did its' utmost to recover the funds and give them to the complainant. However, this was not*

successful and the Bank informed the complainant of this as seen from the email attached by ZO with his complaint.[21]

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 his actions which show gross negligence.*

Conclusion

29. *For the reasons articulated above, the Bank respectfully submits that the Complainant's 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 complaint's claims.*

[21] P. 9 of the complaint.

33. With expenses".[22]

Seduti

Saru żewġ seduti nhar it-02 t'April 2024[23] u t-23 t'April 2024.[24]

Il-partijiet waqt ix-xhieda u s-sottomissjonijet 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.

Qal ukoll:

> ***"Ngħid li ftit qabel ma rċevejt il-messaġġ, kont ipprovajt nagħmel payment through l-app tal-BOV u ma kienx ħallieni. Kien tella' xi error, xi ħaġa – ma niftakarx x'kien hemm miktub eżatt – imma ma kienx ħallieni nagħmlu dan il-payment.***
>
> ***Allura dan il-messaġġ aktar deher ġenwin li hemm xi ħaġa ħażina fl-app."***

Min-naħa l-oħra, l-BOV isostni li huwa kien għal kollox konformi mal-liġi kif tipprovdi l-PSD 2[25] u l-*Banking Directive 1*[26] 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 negiliġenza grossolana min-naħa tiegħu li tagħmlu għal kollox responsabbli biex iġorr il-konsegwenzi tal-frodi li ġarrab.

[22] P. 27 - 33
[23] P. 97- 99
[24] P. 100 - 103
[25] *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.*
[26] *Directive 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which is modelled on the requisites of Directive (EU) 2015/2366.*

Fil-fatt, fil-kontroeżami, l-Ilmentatur ammetta li kien huwa li daħħal il-*codes* li tah il-frodist (li huwa kien ħaseb li kien il-BOV), inkluż l-ammont u l-aħħar ħames ċifri tal-kont tal-frodist biex seta' jsir il-pagament speċifiku, għalkemm qal li ma kienx jaf li b'hekk kien qed jawtoriżża pagament.

Sottomissjonijiet finali

Fis-sottomissjonijiet, il-partijiet sostnew il-pożizzjoni li kienu ħadu fl-Ilment, fir-Risposta u waqt is-seduti.

L-Ilmentatur isostni li:

"Il-Bank għandu l-obbligu li jissalvagwardja lill-klijenti tiegħu u mhux jippretendi li l-klijenti huma kollha bankiera u esperti fil-frodi".[27]

Sostna wkoll li qatt ma kien għamel pagament simili u pagament li kien għamel lill-terzi xi sentejn qabel ma kienx għamlu permezz tal-*Internet banking.*

Il-BOV għamel sottomissjonijiet finali[28] li, però, ma qalu xejn ġdid ħlief li anke l-*Malta Communications Authority* (ara s-sezzjoni li jmiss) kienu ikkonfermaw li l-BOV ma kellux mezzi kif jista' jwaqqaf lil xi frodist milli jippersonifika ruħu qisu l-Bank u juża l-SMS li normalment juża l-Bank biex jingħataw notifiki lill-klijenti tiegħu.

Rigward jekk l-Ilmentatur kienx għamel pagament simili jew le, il BOV qal:

> "*Illi ZO jispjega ukoll li 'tranżazzjoni ta' din in-natura qatt ma għamilt. It-tranżazzjoni li qed isemmi l-bank kienet sentejn qabel u kienet differenti.' Il-Bank jirreferi għal tranżazzjoni li għamel ZO fl-10 ta' Mejju 2022. Din it-tranżazzjoni kienet tat-tip 'third party payment', kif kienet ukoll it-tranżazzjoni in kwistjoni f'dawn il-proċeduri. Sabiex għamel din it-tranżazzjoni, ZO kellu jdaħħal id-dettalji tal-benefiċjarju u d-dettalji tal-pagament, inkluż l-ammont u l-IBAN. Sabiex saret din it-tranżazzjoni, ZO ma kellux għalfejn juża s-Signature 2 għaliex il-proċess ta' dan il-pagament sar kompletament minn fuq il-mobile app, filwaqt li l-pagament in kwistjoni ġie inizzjat minn fuq l-Internet Banking ta' ZO u uża wkoll il-*

[27] P. 105
[28] P. 108 - 114

mobile biex japprova pagament permezz tas-Signature 2. Madankollu, fiż-żewġ pagamenti huwa kellu jdaħħal id-dettalji neċessarji biex japprova l-pagament, partikolarment l-ammont u l-IBAN jew parti minnu."[29]

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.

Iżda l-Arbitru jħoss il-bżonn jemfasiżża bil-qawwa li filwaqt li huwa minnu li l-banek ma għandhomx mezż kif jipprojbixxu li jsir *spoofing/smishing* fil-mezżi ta' komunikażzjoni li jużaw mal-klijenti, m'humiex jagħmlu biżżejjed biex iwissu b'mod effettiv lill-klijenti biex joqgħodu attenti; biex ma jagħfsux *links* li jkunu

[29] P. 112

f'dawn il-messaġġi avolja jkun jidher li ġejjin mill-bank konċernat fuq il-mezż 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-gurnali/TV jew fuq il-paġna tal-*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*[30] 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[31] 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 awtoriżżat 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 awtoriżżazzjoni 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. Ċirkonstanzi 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

[30] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[31] *Article 64 of PSD 2*

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.[32] [33]

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:

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatur**
Ilmentatur li jkun wera traskuraġni grossolona	0%	100%
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	50%	(50%)
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ	(30%)	30%

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

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatur**
biex sar il-pagament ilmentat		
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	0%	0%
Sub-total	20%	80%
Tnaqqis għal ċirkostanzi speċjali	0%	0%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar[34]	20%	(20%)
TOTAL FINALI	40%	60%

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 60% tal-piż u l-40% 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 ħames ċifri fis-*Signatures* tal-*App* iżid id-doża ta' negliġenza tal-Ilmentatur.

Il-mudell jiskużah biss għax ma kienx irċieva twissija diretta mill-BOV dwar dawn l-iskemi frawdolenti fix-xhur ta' qabel dan il-każ u, għalhekk, joffrilu kumpens ta' 20%. Jiskużah ukoll għax ma kienx għamel pagamenti *online* simili bħal dawn fl-aħħar 12-il xahar u, allura, ma kienx midħla ta' kif isiru dawn il-pagamenti mill-*mobile app* tal-BOV. Għalkemm kien għamel pagament f'Mejju 2022, jiġifieri

[34] P. 112 il-pagament imsemmi kien sar aktar minn 12-il xahar qabel il-każ tal-pagament frawdolenti.

aktar minn 12-il xahar qabel u, għalhekk, l-ammont ta' dan il-każ ma kienx wieħed li kellu jqajjem suspetti lill-BOV, xorta jiskużah b'miżura ta' 20% oħra.

B'kollox għalhekk qed jiġi intitolat għal kumpens ta' 40% tal-pagament frawdolenti li ġie debitat lill-kont tiegħu.

L-Arbitru ma jsibx lill-BOV naqas b'xi mod u ppreġudika l-pożizzjoni tal-Ilmentatur għax ir-*recall* tal-pagament konċernat ma tatx rizultat.

L-ewwelnett, la l-pagament jiġi approvat fuq bażi *same day* dan jitlaq mill-ewwel u l-ebda *recall* ma twaqqfu. Kif ukoll il-Bank ressaq provi li immedjatament wara li l-klijent ċempel fil-ħin ta' 14.01 biex jirrapporta l-frodi, il-Bank bagħat *recall* fil-ħin ta' 14:45 lill-bank intermedjarju (UNCRITIMM)[35]u fil-ħin ta' 15:04 lill-bank benefiċjarju (REVOIE23XXX),[36] u mhux tard kif sostna l-Ilmentatur għax ***"their excuse was that during the weekend they do not work."***[37]

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' elf u seba' mija u tmienja w għoxrin ewro u erbgħin ċenteżmu. (€1,728.40).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti l-imgħax bir-rata ta' 4.50% fis-sena[38] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[39]

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

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[35] P. 84
[36] P. 93
[37] P. 3
[38] Ekwivalenti għall-*'Main Refinancing Operations (MRO) interest rate'* kurrenti stabbilit mill-Bank Ċentrali Ewropew.
[39] [39] 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.

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