Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 077/2025

DE

('l-Ilmentatriċi')

vs

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

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

Seduta ta' 23 ta' Marzu 2026

L-Arbitru,

Ra l-Ilment[1] datat 23 t'April 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €9,134 rigward żewġ pagamenti onlajn li saru nhar is-7 ta' Novembru 2023 mill-kont li l-Ilmentatriċi għandha mal-BOV, favur terzi mingħajr l-awtorizzazzjoni tagħha, liema pagamenti wara rriżulta li kienu frawdolenti.

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-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *e-mail.*

[1] Formola tal-Ilment minn Paġna (P.) 1 - 7 b'dokumentazzjoni addizzjonali minn P. 8 - 43.

- 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' komunikazzjonili 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 id-dettalji relevanti:

- Nhar is-7 ta' Novembru 2023, fil-ħin ta' 12:31, irċeviet email li kienet tidher li ġejja mil-Bank li kellha titlu '*Action Needed: Mobile Signature Usage Temporarily Limited.*'[2]

- Billi l-Ilmentatriċi tagħmel użu frekwenti mill-faċilità ta' onlajn payments u billi ma ntebħitx li din l-email kienet frawdolenti, kif setgħet tinduna

[2] P. 25 - 26

kieku ħarset lejn il-URL tal-email li ma kienx normali tal-BOV,[3] għafset il-link.[4]

- L-Ilmentatriċi ammettiet li qatt qabel ma kienet irċeviet xi email ġenwina mill-BOV fejn tiġi mitluba tagħfas xi link, għalkemm qalet li rċeviet diversi emails mill-BOV jistiednuha żżur il-Bank jew il-website biex tagħmel aġġornament ta' dokumenti KYC u notifiki simili.[5]

- Kif għafset il-link daħlet f'site li kienet tidher identika għal dik normali tal-Bank u ma kien hemm xejn li seta' jindika li kienet frawdolenti. Hemm użat it-token biex iddaħħal il-*username* u l- *password*. Mistoqsija jekk tatx id-dettalji normali li kienu jintalbu meta jsir pagament onlajn, hija qalet li ma tiftakarx.[6]

- L-għada meta kienet qed teżamina t-tranżazzjonijiet indunat li kienu saru żewġ pagamenti ta' €6,789 u €2,345, it-tnejn favur xi ħadd Soukaina Liouballa b'referenza ta '*Loan repayment*'. Il-benefiċjarju kien deskritt bħala '*family/friend*' b'indirizz f'Malta.[7]

- Għamlet kuntatt mal-BOV biex tirrapporta l-frodi u għamlet rapport dwar il-frodi fl-Għassa tal-Pulizija tal-Mosta fejn kien hemm vittmi oħra ta' frodi li kienu qed jagħmlu l-istess tip ta' rapport.

- Tat kopja tar-rapport lil BOV biex ikun jista' jagħmel *recall* urġenti iżda hi ssostni li l-Bank dam ma għamel ir-recall tant li reġa' talabha kopja tar-rapport li kienet diġà tat. Issostni li d-dewmien biex isir ir-*recall* ippreġudika l-prospett li *recall* jirnexxi.

- Il-pagamenti li kellhom kumulu ta' aktar mil-limitu normali ta' €5,000 setgħu isiru bla xkiel għax l-Ilmentatriċi kienet tuża l-kont tagħha għan-negozju bħala intermedjarja ta' assikurazzjoni u għalhekk kienet talbet limitu ogħla ta' €25,000.[8]

[3] L-email kellha bħala sors 'sigantures@bov.com.mailer-diel.de'
[4] P. 96
[5] Ibid.
[6] P. 97 - 98
[7] P. 3
[8] P. 52

- Ma jidhirx li saru notifiki tal-pagamenti permezz ta' SMS mill-Bank u dan jista' jispjega għalfejn l-Ilmentratici indunat biss bil-frodi l-għada ta' meta kienu effettivament saru l-pagamenti fuq bażi urġenti '*same day*'.

- Il-Bank isostni li ma kien hemm ebda dewmien biex isir *recall* ġaladarba l-Ilmentatriċi nnotifikat lil BOV bil-frodi iżda billi l-pagamenti kienu diġà telqu għax kienu fuq bażi *same d*ay, ir-*recalls* ma rnexxewx u l-Ilmentatriċi ġiet infurmata b'dan[9].

L-Ilment

L-Ilmentatriċi saħqet li hija ma approvatx il-pagamenti u ma tafx min hu il-benefiċjarju tal-pagamenti. Sostniet li l-Bank naqasha għax kellu l-obbligu li jżomm u jreġġa' lura pagamenti li ma kinux awtorizzati u li s-sistemi tal-Bank ma kinux joffru protezzjoni lill-konsumatur kif mitlub mir-regolamenti bankarji.

Kieku kellu sistemi tajbin inkluż dawk ta' moniteraġġ tal-pagamenti, il-Bank kien jinduna li mill-kont tan-negozju tagħha ma kinetx tagħmel pagamenti personali favur benefiċjarji barranin li għandhom indirizz f'Malta. Kif ukoll li hi mhix it-tip ta' bniedma li tagħti jew tħallas lura xi self fuq bażi personali.

Għalhekk titlob lil BOV jirrifondilha s-somma ta' €9,134, il-valur tal-pagamenti u €61 spejjeż konnessi.

Risposta tal-Fornitur tas-Servizz

Fir-risposta[10] tagħhom, il-BOV qalu:

1. '*Whereas Ms. … (''the complainant'') states that on the 7th of November 2023 she received an email purportedly from BOV asking her to take action since her mobile signatures were going to be blocked. She does not explain what actions she performed upon receipt of this email. Subsequently, on the 8th of November, she noticed 2 transactions and states that she "never authorised these transactions."*[11]

[9] P. 56 - 57; 89 - 90
[10] P. 50 - 57 u dokumenti annessi p. 58 - 90
[11] P. 3

2. *Whereas the complainant attached the details of the transactions in question, bearing transaction ID 134400923 and 134401038 respectively.*[12] *According to the Bank's records, these transactions were duly authorized on the 7th of November 2023 at 13:20 and 13:23 respectively.*[13] *According to the Bank's systems these transactions were 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 transactions were duly authorised. In fact, these transactions had no indication that they were fraudulent.*

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

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

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

5. *Whereas apart from strong customer authentication, the Bank implements also a system of 'dynamic linking' as outlined in the Commission Delegated* Regulation (EU) 2018/389, which supplements the PSD 2. Article 5 provides the following:

[12] P. 23 - 24
[13] DOC. A – Transaction logs of the complainant.
[14] 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 each 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).*

7. *Whereas these payments were approved by the confidential details of [the complainant] with the use of her token. The Bank had no control over these transfers because they were 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.''[15]

*"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.''*[16]

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 payments in question were 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 payments were 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.) *Moreover, [the complainant] had requested the Bank to implement a higher daily limit for transactions which can be done via internet banking. In fact, her limit is €25,000. Therefore, there were no suspicious signs for the Bank with respect to this transaction. One should also note that the PSD2 does not*

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

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.[17]

10. *Moreover, the above-mentioned Commission Regulation provides that the Bank can decide not to apply strong customer authentication for transactions which are considered to have a low level of risk.*[18] *Therefore, one can conclude that when a transaction is considered to be of a higher risk, the Bank should implement the use of strong customer authentication. In fact, the Bank applies strong customer authentication in every transaction in order to ensure 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 complainant is alleging that these transactions were not authorised and has evidence of this, then the Bank is still not obliged to refund her since, even if [the complainant] did not have the intention to approve the payments, she still followed the necessary steps to approve them. 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.***

Whereas article 50(1) of the Directive provides:

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

*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**.*

12. *Whereas if the complainant is alleging that the transactions were not authorised by her, this means that she generated the necessary codes for the payments to be approved and passed them on to a third party. In order to generate such codes, 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'. Therefore, these transactions were not approved because "exercise the necessary security measures to prevent unauthorised access to the complainant's account"[19], but because [the complainant] gave full access of her account to the fraudster and even approved the payments herself.*

13. *The fact that she provided all these details and followed all the necessary steps **twice**, 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

[19] P. 4

applicable, from falling into the hands, or coming to the knowledge, of any third party.''[20]

14. *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 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'*[21] *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."*

15. *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.*

16. *Whereas the Bank also publishes various campaigns to raise awareness within its' customers about possible scams which may be circulating. In fact, in May 2021 the Bank published a page entitled 'Warning: Scam Alerts' attached and marked as* ***'DOC.G'*** *where the Bank explained that SMS fraud occurs when a fraudster sends a message impersonating itself as the Bank or another well-known entity. The Bank warns its' customers to never access links which do not contain the Bank's official URL which is 'www.bov.com'.*

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

17. *Whereas this impersonation of the Bank's communication channels constitutes spoofing and smishing which, as will be explained throughout the proceedings, cannot be controlled by the Bank and is in the control of the telecommunications provider. Moreover, the Bank does not send confidential information in its' usual SMSs, nor does it ask customers to provide information through an SMS or email.*

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

19. *Whereas 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.***

    - *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****.*

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

- *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.*

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

21. *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.*

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

Timeline of Events

23. *Whereas the payments were approved on the 7th of November 2023 at 13:20 and 13:23. These kind of payments are 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'.*

24. *Therefore, when the complainant called the Bank on the 8th of November 2023, the representative blocked the internet banking of [the complainant]. The Bank also made a recall request on the same day at 11:57 and 13:04 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 reply in respect to one of the payments that an indemnity was required. However, the charge to cover the indemnity was not commensurate to the amount lost, therefore BOV closed the claim. With respect to the other payment, no reply was received and the Bank thus also closed this claim. An extract of this communication is attached as ***'DOC.H'****. The Bank informed [the complainant] accordingly and suggested that she follows up the matter with the police.*[23]

25. *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.*

With expenses."

Seduti

Saru tliet seduti fl-10 ta' Settembru 2025, fid-19 ta' Novembru 2025, u fil-21 ta' Jannar 2026.

L-Ilmentatriċi bażikament irrepetiet dak li kienet diġà qalet fl-Ilment u li huwa deskritt hawn fuq.

Il-Bank sostna li l-Ilmentatriċi kienet traskurata b'mod grossolan (gross negligence) meta għafset il-link u kompliet tikkopera mal-frodisti billi ddaħħal informazzjoni sigrieta li setgħet hi biss iġġib mill-mobile jew it-token tagħha u b'hekk awtorizzat il-pagamenti ilmentati li f'għajnejn il-Bank deheru normali u regolari.

Il-Bank sostna li għandu sistemi kemm ta' *'pre' u 'post' 'transaction monitoring'* u l-pagamenti għaddew mill-'*pre test*' għax deheru awtorizzati iżda kienu ġew

[23] DOC. I – Emails from Customer Resolutions Unit.

indikati suspettużi fil-*'post test'*. Iżda sadantittant kien daħal l-ilment u bdew ir-*recalls*.[24]

Sottomissjonijet finali

Fis-sottomissjoniojiet finali, il-partijiet sostnew dak li kien diġà ħareġ mill-Ilment, mir-risposta u mhix xhieda waqt is-seduti**.**

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, ippubblika 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 kull ma 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

[24] P. 105

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 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*[25] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha 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[26] 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.

[25] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[26] *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.[27] [28]

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:

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

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatriċi**
Ilmentatriċi li tkun uriet traskuraġni grossolana	0%	(100%)
Tnaqqis għax irċeviet il-messaġġ fuq *channel* normalment użat mill-Bank	0%	(0%)
Żieda għax l-Ilmentatriċi ikkoperat b'mod sħiħ biex sar il-pagament ilmentat	(0%)	0%
Żieda għax tkun irċeviet twissija diretta mill-Bank fl-aħħar 3 xhur	(20%)	20%
Sub-total	(20%)	(80%)
Tnaqqis għal ċirkostanzi speċjali	(20%)	20%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	0%	0%
TOTAL FINALI	**(40%)**	**(60%)**

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 60% tal-piż u l-40% l-oħra iġorrhom il-BOV.

Il-mudell isib li mill-messaġġ frawdolenti li wasal fuq email, l-IImentatriċi setgħet faċilment tinduna li kienet 'scam'.[29] Ma kienx fuq *channel* li qatt uża qabel il-BOV.

Ġaladarba ma ngħatatx il-kumpens li s-soltu jingħata lil min ikun għafas link fuq xi *channel* li normalment juża l-Bank, allura m'hemmx każ li jitnaqqas dan il-kumpens għax l-Ilmentatriċi baqghet tagħti informazzjoni sigrieta biex effettivament jigu awtorizzati l-pagamenti ilmentati.

Lanqas jista' l-Arbitru jiskużaha għax ma kinetx midħla ta' kif isiru pagamenti onlajn bit-token għax hi stess stqarret li kienet tagħmel dawn it-tip ta' pagamenti sikwit u allura setgħet intebħet li meta qed iddaħħal informazzjoni fil-website kienet effettivament qed tawtorizza pagmenti.

Iżda peress li ma nġabet l-ebda evidenza li l-BOV kien bagħat xi twissijiet diretti lill-Ilmentatriċi biex toqgħod attenta li ma tagħfasx 'links' inklużi f'xi messaġġi li jistgħu jidhru li jkunu ġejjin mill-BOV għalhekk jiskuża lill-Ilmentatriċi għal 20% tat-telf.

L-Arbitru qed jalloka rifużjoni ta' 20% għal ċirkostanzi speċjali, peress li l-Ilmentatriċi fil-ġranet preċiż qabel l-inċident kienet qed tiġi mitluba biex tibdel il-*password* tal-Mobile App. (*characters* ikun twal)[30]. Dan seta' ħoloq sitwazzjoni f'moħħ l-Ilmentatriċi li l-messaġġ frawdolenti kien relatat mat-talbiet ġenwini biex taġġorna l-*password*.

B'kollox, għalhekk, qed tiġi intitolata għal kumpens ta' 40% tal-pagamenti frawdolenti li ġew iddebitati lill-kont tagħha.

L-Arbitru ma jsibx li l-Bank naqas b'xi mod li pagamenti ma ġewx imwaqqfa mill-*payment monitoring systems* li jopera. Meta pagamenti jsiru fi żmien ftit minuti diffiċli li l-*monitoring systems* tiskatta biex jitwaqqfu l-pagamenti għax meta ġara dan il-każ ma kienx hemmx aspettattiva li dawn il-mekkaniżmi jaħdmu '*in real time'* b'mod istantanju.[31]

[29] P. 25
[30] P. 91
[31] Minn Ottubru 2025, daħlu regolamenti li jirrekjedu konferma tal-benefiċjarju tal-IBAN indikat fit-trasferiment onlajn.

Mill-kont tagħha kienu jgħaddu pagamenti anke ferm akbar mill-ammont ta' dan l-ilment. Huwa ovvju li *pre-transaction monitoring* ikollu parametri anqas ristretti mill-*post transaction monitoring* għax jekk le, jinżammu pagamenti li jiġġammjaw is-sistema ta' pagamenti li hija essenzjali għal operat ġenerali tal-ekonomija.

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-Ilmentatriċi is-somma ta' tlett elef, sitt mija u tlieta u ħamsin ewro punt sitta żero (€3,653.60).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.15% fis-sena[32] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv. [33]

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-

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

[33] [33] 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. Dettalji personali tal-Ilmentatriċi/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.