Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 050/2024

BU

('l-Ilmentatriċi')

vs

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

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

Seduta tat-22 ta' Novembru 2024

L-Arbitru,

Wara li ra l-Ilment li fis-sustanza tiegħu jittratta r-rifjut tal-Provditur tas-Servizz li jirrimborża lill-Ilmentatriċi l-ammont ta' €12,345 rappreżentanti flus li ngibdu mill-kont tagħha mal-BOV mingħajr awtorizzazzjoni.

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 id-*'daily limit'* ta' pagamenti li jkun maqbul bejn il-Bank u klijent tat-tip *'retail'.*
- Il-frodist jirnexxilu jippenetra b'mod frawdolenti l-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *email.*
- Il-frodist jagħti *link* fil-messaġġ tiegħu u jistieden lill-klijent biex jagħfas fuq il-*link* biex jagħmel '*validation'* jew *'re-authentication'* tal-kont tiegħu.
- Minkejja diversi twissijiet maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-Bank ma jibagħatx *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 jirnexxilu jippenetra l-kont tal-klijent u jagħmel trasferiment ta' flus ġeneralment fuq bażi *'same day'* li jmorru fil-kont tal-frodist, ġeneralment f'kont bankarju f'pajjiż barrani minn fejn huwa kważi impossibbli li jsir *recall* effettiv tal-flus ġaladarba l-klijent jirrapporta lill-bank tiegħu li ġie ffrodat. Ħafna drabi l-frodist ikun pront jiġbed jew jittrasferrixxi 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' komunikazzjoni normalment użat bejn il-bank u l-klijent jiġi ppenetrat mill-frodist u li l-bank messu nduna li kien pagament frawdolenti għax ġeneralment il-klijent ma jkollux storja ta' pagamenti bħal dawn.

  Il-Bank isostni li l-ħtija hija kollha tal-klijent għaliex permezz ta' traskuraġni grossolana (*gross negligence)* ikun ta aċċess tal-kredenzjali sigrieti tal-kont tiegħu lill-frodist u b'hekk iffaċilita l-frodi.

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

- Fil-jum tal-Ħadd, nhar il-5 ta' Novembru 2023, l-Ilmentatriċi indunat li jumejn qabel kien sar pagament ta' €12,345, li ma kienx awtorizzat minnha, permezz tal-*internet banking* minn kont tagħha mal-Bank.

- L-Ilmentatriċi ssostni li kienet irċeviet xi *emails* mill-BOV biex tidħol tiċċertifika l-firma billi tagħfas *link* li kienet inkluża fl-*email* konċernata. Hija għafset il-*link* meta irċeviet l-*email* għat-tieni darba.[1] [2]

- Kif għafset il-*link* daħlet fil-*website* li kienet tidher tal-BOV. Dakinhar kienet imħabbta ħafna għax hi għandha negozju li torganizza tiġijiet u kellha tieġ Indjan li kien fit-tieni ġurnata tiegħu.

[1] Paġna (P.) 3
[2] P. 98

- Jidher li min hemm sar il-pagament ilmentat li kien favur HARSHDEEP SINGH u kien jindika li kien self biex isir ħlas ta' karozza lussuża. Il-pagament sar f'kont miżmum mal-*Banco Comercial Portugues* (BCOMPTPLXXX) fuq bażi *'same day'*[3] [4]u li ma kienet irċeviet l-ebda notifika mill-Bank dwar dan il-pagament kif normalment kienet tirċievi permezz ta' SMS.[5]

- Dan sar f'kont tal-bank ikkontrollat mill-frodist fil-Portugal. Il-Bank jgħid li l-Ilmentatriċi rrapportat il-każ il-Hadd, 5 ta' Novembru 2023, iżda dak il-ħin seta' jibblokka biss il-*cards* u l-*internet banking* tal-Ilmentatriċi. L-għada, t-Tnejn, 6 ta' Novembru 2023, saret talba ta' *recall* biex jitreġġa' lura l-pagament, iżda dan ma tax riżultat pożittiv.[6]

- B'mod qarrieqi l-benefiċjarju tal-pagament kien indika l-indirizz tal-benefiċjarju bħala San Ġiljan, Malta, biex inaqqas xi suspett mis-sistema tal-BOV li tagħmel *monitoring* tal-pagamenti.[7]

- Il-pagament sar f'affari ta' ftit minuti fejn l-ewwel *login* sar fil-ħin ta' 13:02, ġie vverifikat fil-ħin ta' 13:05, u l-*logout* sar fil-ħin ta' 13:06.[8]

- Peress li l-BOV ma bagħatx SMS wara li sar il-pagament biex jinforma b'dan lill-Ilmentatriċi, din indunat biss b'dan jumejn wara li kien sar il-pagament. Kif indunat bil-pagament mhux awtorizzat, ċemplet lill-BOV biex tirrapporta l-frodi iżda l-pagament diġà kien ġie proċessat jumejn qabel.

- Il-każ ġie rrapportat lill-pulizija nhar is-6 ta' Novembru 2023 għal aktar investigazzjoni tal-frodi.[9]

[3] P. 16 – pagament *same day* isir immedjament kif jiġi awtentikat mill-Bank.
[4] P. 20
[5] P. 25 - 26
[6] P. 8, 37
[7] P. 20
[8] P. 40 - 41
[9] P. 13 -14

Ikkunsidra l-Ilment[10]

L-Ilmentatriċi ssottomettiet li hi m'awtorizzat ebda tranżazzjoni u li l-Bank huwa responsabbli għax ħalla lil

> ***"Scammers to send people a link which takes it to the bank's internet banking site."***[11]

Ilmentat li l-Bank seta' ppreġudika il-pozizzjoni tagħha għax m'għamilx talba immedjatment kif irrapportat il-każ biex il-flus jitreġġgħu lura u ppretendiet li l-Bank għandu joffri dan is-servizz anke fil-jum tal-Ħadd.

Ilmentat ukoll għax il-Bank ma nformahiex mill-ewwel li kien sar dan il-pagament frawdolenti:

> ***"The bank normally informs me via text of any payments that go out of my accounts. This time they sent me a text informing me of two payments I had made from my current account***[12]***... however the eur 12345 from an account that I hardly use to make payments was not reported to me. If they had I would have been in time to stop the transaction."***[13]

Għalhekk talbet lil BOV jagħmel tajjeb għat-telf li ġarrbet u jirrifondilha s-somma ta' €12,345.

Ikkunsidra wkoll, fl-intier tagħha, ir-risposta tal-Provditur tas-Servizz,[14]

Fejn il-Provditur tas-Servizz spjega u ssottometta li kien konformi mar-regolamenti bankarji tal-pagamenti[15] [16] u li s-sistema tagħhom toffri *'two factor authentication'* skont dawn ir-regolamenti biex jiġi protett il-klijent li hu biss jista' jawtorizza pagamenti *online*.

---

[10] Formola tal-Ilment minn Paġna (P.) 1 - 7 b'dokumentazzjoni addizzjonali minn P. 8 - 26.
[11] P. 4
[12] P. 25
[13] P. 4
[14] P. 32 -38 b'dokumenti annessi minn P. 39 - 92.
[15] PSD2 DIRETTIVA (UE) 2015/2366 tal-Parlament Ewropew u tal-Kunsill tal-25 ta' Novembru 2015 dwar is-servizzi ta' pagament fis-suq intern, li temenda d-Direttivi 2002/65/KE, 2009/110/KE u 2013/36/UE u r-Regolament (UE) Nru 1093/2010, u li tħassar id-Direttiva 2007/64/KE.[15] Din id-Direttiva hija komunement imsejħa 'PSD2' għaliex issegwi direttiva oħra maħruġa mill-UE fuq l-istess suġġett.

[16] Directive-1.pdf (centralbankmalta.org) li tagħti effett lill-PSD2,

U li biex il-frodist ġibed il-flus mill-kont tal-Ilmentatriċi bifors li din kienet negliġenti b'mod grossolan u, għalhekk, skont dawn ir-regolamenti kellha ġġorr hi t-telf li ġarrbet minħabba li kixfet il-kredenzjali tal-kont tagħha u b'hekk iffaċilitat is-serq li sar mill-frodist.

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 kn**owledge (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;*

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 input 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, she also inputted the last 5 digits of the IBAN number of the recipient, and this satisfies the element outlined in article 5(c) above mentioned. Upon entering these details, a code would have been generated which needs to be used to approve the transaction. The customer accesses this section from the section entitled 'Transaction Signing 'Signature 2' and then sees a section entitled 'Amount' and another entitled 'Payee Code'. This can be seen from the document attached as 'DOC.B' (which is easily accessible on the Bank's website). These phrases all clearly indicate that one is approving a transaction.*

7. *Whereas this payment was approved by the confidential details of the complainant with the use of her 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."

"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 ("Boy Mobile PIN"), or input your biometric data, are deemed as binding on you!"

8. *Whereas in fact, every token used to generate codes to approve a payment has a certificate associated with it. In fact, the certificate number associated with the token with which the payment in question was approved is the same one associated with the token of the complainant which she has previously used to make other payments which she is not contesting the legitimacy of. This can be seen from the document attached and marked as 'DOC.D'.*

9. *Whereas besides the fact that the payment was duly authorised, there is also the fact that the transaction amount was within the limit imposed for these kinds of transactions. With respect to the transaction in question in this arbitration, which is a 'third-party transaction', the normal 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). However, the complainant had requested the Bank to increase this limit to €25,000. Therefore, a transaction of €12,345 was well within this limit. Therefore, there were no suspicious signs for the Bank with respect to this transaction.*

   …..

12. *Whereas article 50(1) of the Directive provides:*

    The payer shall bear all of the lasses 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 her, this means that she either left her token in the hands of third parties or generated the necessary codes for the payment to be approved and passed them on to a third party. In order to generate such*

a code, she had to insert the amount of the transaction and the last 5 digits of the recipients' IBAN. This fact should have raised suspicion within the complainant since if she 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'.

14. *The fact that he provided all the details and followed all the necessary steps which enabled the approval of the transaction (even if he had no intention of doing it), 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 BQV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party."

.....

<u>Conclusion</u>

30. *For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and law because as explained above, the transaction was approved through the credentials of the complainant and through her token.*

31. *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.

32. *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.*

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

34. *With expenses.*

Seduti

Fl-ewwel seduta li nżammet fit-3 ta' Settembru 2024, l-Ilmentatriċi sostniet dak li kienet diġà rrapportat fl-ilment u żiedet:

"***Regarding the link that I received, I say that I had never seen any notice or alert from the bank that one could receive these type of fraudulent email or SMSes.***

I say that Bank of Valletta was the first bank, so I would say that I have been their client for thirty years. I would say that I never had any problems with them.

I say that when I followed the instructions to verify my signature, there was not an amount written that I could see. When I pressed the link, it was to verify my signature. I say that at no point in time during this process of verifying my signature did I receive a code on my mobile to affect the transaction or second approval or anything from my App, nothing at all. There was no second verification. I came to know about

this from my savings account and not from the current account which I usually use.

I say that when I called the 24/7 contact number of BOV's Customer Care on that Sunday, they told me that they could not help me. They told me that this number was for card fraud.

I say that this is a savings account where I deposit money and I rarely withdraw money from it. I believe that in 2020, there was a transaction of about €6,000, then there were two transactions of I think €10,000 and €9,000 which were withdrawn by the bank with my consent for investments. The Wealth Management branch withdrew these amounts of about €10,000 and €9,000. These were the only amounts which were over €5,000.

I say that since having this account, I have never withdrawn large sums of money from this account.

I confirm that I have never made a transfer to the amount of €12,345 in my whole life."[17]

Fil-kontroeżami hija xehdet:

"Asked whether I remember the sender's email address when I received the email allegedly coming from BOV, I say, no. I saw that it was from BOV.

Asked whether I have ever received before this incident an email from BOV with a link requesting me to verify my signature, I say, no, I don't believe so.

Being asked to describe the steps I have taken to verify my signature, I say that I went it, there was Verify your Signature, and I did a couple of steps. I do not know exactly, exactly but there was in writing, 'Verify your Signature', do this and do this. That's all it was, it was something very simple.

[17] P. 94 - 95

I say, no, I did not use my Mobile App for this process. I did it as usual on my PC. I went into the BOV's website and when I went to internet banking, it told me to verify my signature and I followed the steps to verify my signature.

Asked whether I used the physical key or the Mobile App during the process to generate the codes, I say that I generated a code to go into the internet banking. Asked from where I generated the code, I said the code was in my head and I had the other one in order to go in to verify my signature which I generated from my mobile. I only used the Mobile App to enter; I did not use it again.

I say, yes, I am aware that normally €5,000 is the limit of transactions on internet banking. I say that I have requested the bank to extend the limit on my current account. I cannot remember what I asked for, but my limit is €15,000. I do not remember when I asked for this limit to be extended.

Asked whether I am familiar with BOV's Terms and Conditions, I say not particularly.

Asked whether I made any follow ups with the police regarding my police report, I say, yes, numerous times. I have emails that I have sent to the police where they told me to wait, that they will come back to me. I phoned them, and all this. First, they told me to go to Cyber Crime; then it was online fraud, this sort of thing but they never came back to me. I have emails from the police saying that this takes a long time."[18]

L-Arbitru talab lill-Ilmentatriċi tissottometti kopja tal-*email* frawdolenti li kienet irċeviet[19] u lill-Bank biex jissottometti kopji tal-*bank statements* kollha tal-Ilmentatriċi (kurrenti u *savings*) għal sena qabel l-inċident ta' Novembru 2023.[20]

Talab ukoll lill-Bank biex jibgħat evidenza tat-talba tal-Ilmentatriċi biex tgħolli d-*daily limit* minn €5,000 (limitu normali għal klijenti tip *retail*) għal €25,000 (jew kif qalet l-Ilmentatriċi għal €15,000).[21]

[18] P. 95
[19] P. 98
[20] P. 100; 106 - 339
[21] P. 100; p. 340

It-tieni seduta nżammet fit-8 t'Ottubru 2024 fejn tela' jixhed Michael Gatt, uffiċjal eżekuttiv, fl-*Electronic Payments Section* tal-BOV li qal:

> ***"Mitlub nispjega kif ġiet awtorizzata t-tranżazzjoni mertu ta' dan l-arbitraġġ, ngħid li bħal kull tranżazzjoni li ssir bħal f'dan il-każ, (li f'dan il-każ saret bil-mobile), l-ewwel nett irid li jkollok il-mobile f'idejk. Once li għandek il-mobile, tidhol fl-app tal-BOV u biex taċċessa l-app trid il-PIN. Mela għandek il-PIN tal-mobile u għandek il-PIN tal-app. Li dan il-PIN ikun jafu biss il-klijent.***
>
> ***Minn hemm tipproċedi għal Transaction Sign In, tagħfas fuq Signature 2 f'dan il-każ, iddaħħal l-ammont, imbagħad iddaħħal il-Payee Code. Il-Payee Code ikun ibbażat fuq l-aħħar ħames digits tal-IBAN li tkun daħħalt. Terġa' tagħti l-PIN, u once li daħħal il-PIN fuq l-Internet Banking, it-tranżazzjoni titlaq.***
>
> ***Mingħajr dawn l-isteps, it-tranżazzjoni ma tista' ssir bl-ebda mod.***
>
> ***Ngħid li l-PIN mhuwiex il-Login ID; il-Login ID hu xi ħaġa oħra. Hu s-six digit number li jkun jafu l-kllijent biss u bil-Login ID biss ma jiġri xejn. Jekk nagħtik il-Login ID u saħansitra nagħtik il-One-Time Password, kulma ser jiġri hu li int ser tara biss il-kontijiet tiegħek. At any moment ma tista' tagħmel l-ebda tranżazzjoni b'dik l-informazzjoni biss.***
>
> ***Biex inti tagħmel tranżazzjoni, għandek il-mobile, tmur fuq l-app u ddaħħal il-PIN; mill-PIN tmur fuq Transaction Sign In, minn Transaction Sign In iddaħħal l-ammont li trid tutilizza, iddaħħal il-Payee Code li huwa bbażat fuq l-aħħar ħames digits tal-IBAN. Terġa' tagħti l-PIN u t-tranżazzjoni ssir. Mingħajr dawn l-isteps kollha t-tranżazzjoni ma ssirx.***
>
> ***Meta ngħid terġa' ddaħħal il-PIN inkun qed nirreferi mhux għall-PIN oriġinali imma għal dak il-PIN li jiġi iġġenerat speċifikament għal dik it-tranżazzjoni, iċ-Challenge jew l-Authorisation Code.***
>
> ***Qed niġi referut għal Dok. E anness mar-risposta tal-BOV dwar il-limits tat-tranżazzjonijiet li wieħed jista' jagħmel permezz tal-Internet Banking.***

Ngħid li by default upon application, il-limit tal-personal ikun €5,000. Ma jfissirx li dak ma jistax jinbidel, però, jinbidel biss jekk ikollna request mingħand il-customer. Once li jkollna request mingħand il-customer, u l-customer jiġi verified, dak il-limit jogħla skont il-bżonnijiet tal-customer – f'dan il-każ kien €25,000 – u jogħla across all accounts – not one account - li huma attached ma' dak il-kuntratt."[22]

Waqt il-kontroeżami qamu dawn il-konfronti:

ILMENTATRIĊI	PROVDITUR TAS-SERVIZZ
Id-*daily limit* kien €15,000	Id-*daily limit* kien €25,000[23] [24]
Ma niftakarx li daħħalt l-informazzjoni biex jiġi awtorizzat il-pagament. Kont qed nobdi biss struzzjonijiet to *'verify your signature'.*	Il-*logs* tal-Bank li ġew ippreżentati[25] juru li l-Ilmentatriċi awtorizzat il-pagament hi mill-*internet banking* tagħha bl-istess *token* li normalment tuża biex tawtorizza pagamenti normali tagħha.
Il-fatt li l-pagament kien għal ċifra 12345 u ħafna ilmenti oħra li ġa ġew deċiżi mill-Arbitru juru wkoll tendenza għal ammonti f'numri konsekuttivi, messu skatta sinjal lill Bank biex iwaqqaf dan il-pagament għax kien jidher frawdolenti	Il-Bank ma jwaqqafx pagamenti għax l-ammont ikun f'numri konsekuttivi jekk il-pagamenti jkunu awtorizzati kif suppost.
It-*transaction limit* ma kienx intiż li japplika fuq is-*savings account* minn fejn sar il-pagament. Il-Bank ma	Iż-żieda fil-*limit* hija marbuta mal-*Login ID* tal-klijent u tapplika fuq il-kontijiet kollha tal-klijent li jkunu koperti bil-*Login ID* u mhux *limit* differenti għal kull kont. L-Ilmentatriċi kienet taf li anke l-*limit* tal-

[22] P. 341 - 342
[23] P. 100 - 101.
[24] P. 189 anke fis-27-08-2022 saru pagament li jaqbżu l-€15,000
[25] P. 40 – 41; 55

jmessux applika l-*limit* għoli fuq il-kontijiet kollha.	kontijiet *savings* ma kienx €5,000 għax ġieli għamlet pagamenti għal ammonti akbar anke mis-*Savings*.[26]
Il-Bank naqas meta ma bagħatx SMS rigward dan il-pagament frawdolenti.	Il-Bank mhux obbligat li jibgħat *SMS notifications*, wisq anqas li jibgħat notifika għal kull tranżazzjoni.

Sottomissjonijet finali

Fis-sottomissjoniet finali tagħhom, il-partijiet irrepetew dak li kien diġà ntqal fl-Ilment, fir-Risposta u fis-seduti. Kif inhija l-prassi, argumenti ġodda li ma kinux tqajjmu qabel ma ġewx ikkunsidrati.

Analiżi u konsiderazzjoni

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

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

[26] P. 101

Mhux biżżejjed li jagħmlu avvizi 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*[27] 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 cara[28] 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.

Il-mudell jagħti wkoll konsiderazzjoni għal xi ċirkostanzi partikolari tal-każ. Jista' jkun hemm ċirkostanzi partikolari fejn il-messaġġ tal-frodist ikun anqas suspettuż.

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

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.[29] [30]

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 u jaġġustah għaċ-ċirkostanzi partikolari ta' dan il-każ, jasal għal din id-deċiżjoni:

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	Perċentwal ta' ħtija tal-Ilmentatriċi
Ilmentatriċi li tkun uriet traskuraġni grossolana	0%	100%

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

Tnaqqis għax irċeviet il-messaġġ fuq *channel* normalment użat mill-Bank	25%	(25%)
Żieda għax l-Ilmentatriċi ikkoperat b'mod sħiħ biex sar il-pagament ilmentat	(15%)	15%
Żieda għax tkun irċeviet twissija diretta mill-Bank fl-aħħar 3/6 xhur	(0%)	0%
Sub-total	10%	90%
Tnaqqis għal ċirkostanzi speċjali	20%	(20%)
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	0%	0%
TOTAL FINALI	30%	70%

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 70% tal-piż u l-30% l-oħra jġorrhom il-BOV.

Il-mudell normalment inaqqas il-ħtija tal-klijent b'50% għax ikun irċieva messaġġ jew komunikazzjoni fuq il-kanal li normalment jirċievi notifiki mill-Bank. Dan japplika l-aktar għal każi ta' *smishing* fejn l-ilmentatur ikun irċieva SMS fuq il-kanal normali tal-Bank.

Iżda, f'dan il-każ, l-Ilmentatriċi irċeviet *email* li kienet pjuttost ċara li kienet frawdolenti peress li kienet ġejja minn:

BOV Group <inoue@net-service24.co.jp>

Għalhekk, flok b'50%, qed inaqqas il-ħtija tal-Ilmentatriċi b'25% għaliex kien aktar faċli li l-Ilmentatriċi tinduna li l-*email* li rċeviet kienet qarrieqa milli jkun il-każ meta l-messaġġ jasal fuq il-kanal ta' SMS li l-Bank juża għan-notifiki tiegħu lill-klijent.

Ma nġabet ebda evidenza li l-Bank qatt kien bagħat xi komunikazzjoni lill-Ilmentatriċi permezz ta' *email* u dan, għalhekk, kellu jqajjem aktar suspett min-naħa tal-Ilmentatriċi dwar l-awtentiċità tal-*email*.

Il-mudell isib il-fatt li l-Ilmentatriċi bilfors baqgħet tikkopera mal-frodist billi fis-*Signatures* tal-App setgħet tara l-ammont u l-aħħar ħames numri tal-IBAN, u saħansitra anke daħħlet is-*6-digit code* li tagħti l-aħħar awtorizzazzjoni biex isir il-pagament. Dan iżid id-doża ta' negliġenza tal-Ilmentatriċi għax hi kienet midħla ta' dawn il-pagamenti u setgħet tinduna li kienet qed tawtorizza pagament u mhux qed tawtentika xi firem diġitali.

Iż-żieda skont il-mudell oriġinali hija 60% tat-tnaqqis li jkun sar qabel, jiġifieri 15% (marbuta ma' tnaqqis ta' 25%) flok 30% (b'rabta ma' tnaqqis normali ta' 50%).

Il-mudell ma jżidx ir-responsabbiltà tal-Ilmentatriċi għax tkun irċeviet xi twissija mill-bank biex ma tagħfasx *links* bħal dawn fl-aħħar tliet/sitt xhur qabel il-każ.

Lanqas jista' l-Arbitru jiskuża lill-Ilmentatriċi għax ma għamlitx pagamenti *online* simili għax hi stess ammettiet li kienet midħla ta' kif isiru dawn il-pagamenti *online* bl-*internet*.

L-Arbitru wiżen jekk kienx hemm xi ċirkostanzi speċjali li jiskużaw lill-Ilmentatriċi f'dan il-każ. L-Ilmentatriċi tlum lill-Bank li ma bagħatilhiex notifika dwar dan il-pagament kif għamel fil-każ ta' pagamenti oħra li saru fl-istess jum.

Filwaqt li l-Arbitru jifhem li l-Bank ma għandux obbligu regolatorju biex jibgħat dawn in-notifiki, huwa stramb kif f'każ ta' pagament pjuttost kbir ma ntbagħtet l-ebda notifika bħalma saru notifiki għal pagamenti ferm iżgħar li saru fl-istess jum mill-kont kurrenti.

La l-Bank isostni li *daily limit* japplika għall-kontijiet kollha u mhux biss għall-kont kurrenti, kien ikun aktar floku li toħroġ notifika fuq pagament pjuttost kbir minn

kont li mhux soltu jsiru pagamenti minnu milli notifika dwar pagamenti iżgħar minn kont li minnu jsiru pagamenti regolari u ta' sustanza.

Huwa minnu li anke kieku ntbagħtet notifika hemm probabilità li l-pagament la kien kategorizzat *same day*, xorta ma kienx ikun jista' jitwaqqaf.

Iżda, l-Arbitru jrid jagħti xi benefiċċju tad-dubju lill-Ilmentatriċi anke għax hemm element, għalkemm pjuttost marġinali, li l-fatt li l-pagament kien qed isir fuq bażi *same day* minn kont li mhux soltu kien jintuża għal pagamenti bħal dawn, seta' nqabad mis-sistemi ta' moniteraġġ ta' pagamenti tal-Bank. Għalhekk, l-Arbitru qed iqis li hemm element ta' ċirkostanzi speċjali ta' 20%.

l-Arbitru tixtieq jittratta d-difiża tal-Ilmentatriċi li l-Bank kellu ħtija għaliex:

1. **Il-fatt li l-ammont kien għal ammont ta' ċifri konsekuttivi messu wassal biex il-Bank jinduna li dan kien pagament frawdolenti u messu waqqfu.**

   L-Arbitru ma jarax relevanza f'dan l-argument għax anke kieku l-Bank kellu sistema ta' moniteraġġ sensittiva għal dan, il-frodist kien sempliċiment ivarja l-ammont. Is-sistema ta' moniteraġġ ta' pagamenti trid tkun sensittiva għall-fatt jekk il-pagament kienx stramb biżżejjed paragunat mal-pagamenti li normalment isiru mill-klijent biex iqajjem suspett ta' frodi.

   F'dan il-każ, l-Arbitru jqis li l-pagament ma kienx stramb biżżejjed biex iqajjem suspett raġonevoli għax l-Ilmentatriċi ma kinetx estranea għal pagamenti ta' dan l-ammont, kif jixhdu l-i*statements* tal-kontijiet ippreżentati.[31]

2. **Li l-limitu ogħla li kien japplika għall-Ilmentatriċi (jekk hux €15,000 kif sostniet l-Ilmentatriċi jew €25,000 kif sostna l-Bank ma hux relevanti għall-pagament ta' €12,345) ma kellux japplika għall-kont *savings* minn fejn ħareġ il-pagament.**

   Fid-difiża tiegħu dwar dan, il-BOV qal li *limit* ogħla ta' €25,000 kien japplika għall-kontijiet kollha li kienu aċċessibbli *online* għall-klijenta bil-USER ID tagħha u li hi kienet ilha taf b'dan għax kienet hi stess li applikat

[31] P. 127; 128; 129;132;189;198; 199; 204;205;216;256;273;277;305;317;325;331;335; (fost oħrajn)

għal limitu ogħla mill-5 ta' Ġunju 2018[32] u spiss kient tagħmel pagamenti *online* ta' aktar minn €5,000.

Speċifikament, il-Bank għamel referenza għall-pagamenti ta' €10,000, €15,000, €8,000, u €8,000 li ħarġu minn *savings account* (għalkemm mhux l-istess wieħed li minnu sar il-pagament kontestat) bejn 14.10.2023 u 23.08.2024,[33] u pagament ta' €7,000 fi 03.05.2022 minn kont ieħor *savings*.[34] Il-Bank sostna li dan jipprova li l-Ilmentatriċi kienet taf li l-limitu ogħla kien japplika fuq il-kontijiet kollha.

L-Arbitru jsib dan l-argumenti konvinċenti biex jipprova li l-Ilmentatriċi kienet taf li l-limitu ogħla kien japplika wkoll għas-*savings account* inkluż dak li minnu sar il-pagament frawdolenti.

Il-fatt li minn dan il-kont partikolari ma kien qatt sar pagament kbir, li iżda kienu saru minn kontijiet oħra tagħha kemm *savings* kif ukoll kurrenti, ma jservix ta' prova kontra l-BOV li messu waqqaf dan il-pagament. Il-klijent għandu dritt joħroġ pagament minn fejn jidhirlu li huwa l-aħjar għalih, u la l-ammont tal-pagament ma kienx stramb paragunat ma' pagamenti li saru minn kontijiet *savings* oħra, l-Arbitru ma jsostnix l-argument tal-Ilmentatriċi.

Iżda, għal quddiem, l-Arbitru qed jagħmel rakkomandazzjoni li għandha tiġi kkunsidrata sewwa mill-banek u mir-regolaturi biex dejjem jitnaqqas ir-riskju ta' frodi.

B'kollox, għalhekk, l-Arbitru qed jordna kumpens ta' 30% tal-pagament frawdolenti li ġie debitat lill-kont tagħha.

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 s-somma ta' tlett elef, seba' mija u tlett ewro punt ħamsa żero (€3,703.50).

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

[32] P. 340
[33] P. 127 – 129
[34] P. 132

Rakkomandazzjoni

Biex jitnaqqas ir-riskju ta' frodi, l-Arbitru jirrakkomanda li l-banek idaħħlu sistemi, li diġà jeżistu f'istituzzjonijiet internazzjonali, fejn il-klijent ikollu facilità li kontijiet ta' tifdil fejn normalment jinżammu ammonti kbar ma jkollhomx faċilità li minnhom isiru pagamenti *online* ħlief trasferimenti għall-kont kurrenti tal-klijent. B'hekk, il-klijenti jkunu aktar protetti rigward somom ta' tifdil.

Għal dan il-għan, kopja ta' din id-deċiżjoni u r-rakkomandazzjoni qed tintbagħat lill-Bank Ċentrali ta' Malta u lil *Malta Financial Service Authority* (MFSA) bħala regolaturi tal-pagamenti u tal-banek rispettivament.

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-data tan-notifika ta' dik l-interpretazzjoni jew il-kjarifika jew il-korrezzjoni hekk kif provdut taħt l-artikolu 27(3) tal-Att.

Kull talba għal kjarifika tal-kumpens jew talba għall-korrezzjoni ta' xi żbalji fil-komputazzjoni jew klerikali jew żbalji tipografiċi jew żbalji simili mitluba skont l-

artikolu 26(4) tal-Att, għandhom isiru lill-Arbitru, b'notifika lill-parti l-oħra, fi żmien ħmistax (15)-il ġurnata min-notifika tad-Deċiżjoni skont l-artikolu msemmi.

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