Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 099/2026

ZO

('l-Ilmentatur')

vs

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

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

Seduta tal-25 t'Awwissu 2026

L-Arbitru,

Ra l-Ilment[1] datat l-1 t'April 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi tal-anqas 90% tat-telf li sofra meta saru żewġ pagamenti frawdolenti mill-kont tiegħu[2] mal-BOV li b'kollox jammontaw għal €12,550.

Dawn il-pagamenti saru nhar il-21 ta' Lulju 2025, kif spjegat fit-tabella:

Ħin	Ammont €	Referenza
10:20:49	3,000	p. 62; 149
10:26:55	9,550	p. 62; 149
10:30:59	2,000	p. 62
Payment blocked	(2,000)	
TOTAL	**12,550**	

[1]Paġni (P.) 1 - 8 b'dokumentazzjoni addizzjonali minn p. 9 - 42.
[2] P. 140 Il-kont fil-fatt qiegħed f'isem l-Ilmentatur bħala Trustee ta' THE GARLAND TRUST.

Il-pagamenti kollha saru favur ċertu Dionis Saite.

Quddiem l-Arbitru ġew 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 jirnexxielu jippenetra b'mod frawdolenti il-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *e-mail.*

- Il-frodist jagħti *link* fil-messaġġ tiegħu u jistieden lill-klijent biex jagħfas fuq il-*link* biex jagħmel *'validation'* jew 're-*authentication'* tal-kont tiegħu.

- Minkejja diversi twissijiet[3] 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-klijent, il-klijent b'nuqqas ta' attenzjoni jagħfas il-*link*.

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

- B'riżultat, jinħoloq nuqqas ta' ftehim bejn il-bank u l-klijent dwar min hu responsabbli jġorr il-piż tal-pagament frawdolenti. Il-klijent isostni li l-bank ma pproteġihx meta ħalla kanal ta' komunikazzjoni li normalment użat bejn il-bank u l-klijent jiġi ppenetrat mill-frodist, u li l-bank messu nduna li kien pagament frawdolenti għax, ġeneralment, il-klijent ma jkollux storja ta' pagamenti bħal dawn. Il-bank isostni li l-ħtija hija kollha

[3] L-Uffiċċju tal-Arbitru ukoll ħareġ twissijiet – ara: https://www.youtube.com/watch?v=3podDv2R_Jc&t=3s

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:

- Peress li l-BOV xamm xi ħaġa mhix f'lokha meta kienu diġà għaddew l-ewwel żewġ pagamenti, inżamm it-tielet pagament u sar kuntatt b'inizjattiva tal-Bank mal-Ilmentatur biex jinfurmawh bil-pagamenti u jaraw jekk kienx hu li awtorizzahom. Din kienet telefonata li saret fil-ħin ta' 10:36 minn rappreżentanta 'Brooke' li kellha diskursata ta' nofs siegħa mal-Ilmentatur.

- Waqt din id-diskursata, l-Ilmentatur stqarr li kien irċieva fil-ħin ta' 09:42 SMS fuq *BOV Mobile* biex jagħfas *link* għax il-Bank ried li jwaqqaf pagament li kien jidher dubjuż.[4]

- Fil-ħin ta' 09:52 irċieva SMS fuq l-istess BOV *Mobile chat* biex jgħidlu li ser iċemplulu mill-BOV fuq numru 99118001, u wara ftit ċemplitlu ċerta Stephanie li qalet li kienet rappreżentanta ta' BOV biex tgħinu jwaqqaf il-pagamenti.

- Peress li Stephanie kienet konvinċenti u awtentika, l-Ilmentatur xejn ma basar li din kienet frodista u baqa' jikkopera magħha billi taha l-informazzjoni li talbitu inkluż l-*Activation Code*[5] li bih il-frodista setgħet tagħmel pagamenti frawdolenti li f'għajnejn il-BOV dehru li kienu awtorizzati normalment mill-Ilmentatur.

- Wara li saru dawn il-pagamenti, irċieva wkoll SMS ieħor biex taparsi jinfurmawh li l-pagamenti suspettużi ġew miżmuma meta fil-fatt kienu qed isiru.[6]

- 'Brooke' mal-ewwel infurmatu li Stephanie kienet frodista għax il-Bank ma jċemplix fuq in-numru indikat u qatt ma jibgħat SMS b'*links* fihom. 'Brooke' għamlet rapport li permezz tiegħu it-tielet pagament ta' €2,000

[4] P. 128
[5] P. 129
[6] *Ibid.*

laħaq ġie miżmum. Ġew iffriżati kemm l-*internet banking* kif ukoll il-*cards* kollha li kellu.

- Sar rapport lill-pulizija[7] dakinhar stess għall-ħabta ta' 13:20 u kopja tar-rapport ingħatat lill-Bank biex isir il-proċess ta' *recalls* f'attentat biex jiġu mblokkati l-fondi qabel ma jinġibdu mill-frodisti.
- Matul il-proċess, il-Bank offra rifużjoni ta' 30% (€3,765) ibbażata fuq il-mudell li kien ippubblika l-Arbitru iżda din l-offerta ma ġietx aċċettata u ppretenda li jiġi rimborżat għal 90%.

L-Ilment

L-argument prinċipali tal-Ilmentatur huwa:

> *"I feel that the Bank was uncooperative in its efforts to stop the transfers out neither in Malta nor at destination.*
>
> *I did not give any account number or password online or over the phone. The first girl "Stephanie" quoted to me some of my account numbers and their balances! She was perfectly credible and no one apart from the Bank should have access to my accounts. She certainly did not ask for any password.*
>
> *When my account was reactivated, on the transactions list of account ending 52582, I found that the two fraudulent transfers out were indicated - I suppose ordered- " PAYMENT ORDER OUTWARDS SAME DAY". I had certainly never used nor seen wording like this before: certainly this should have triggered immediate action from the Bank. A copy of the Transactions sheet is attached for reference.*
>
> *I chased the Bank for a refund to close the issue for many months.*
>
> *Finally, and only on the 22nd December 2025, after 5 months not 35 working days, BOV made me an offer of €3765 in full and final compensation. I objected to their offer and asked for at least 90%. They refused. I told them that I shall complain to you. The Arbitor for Financial Services.*

[7] P. 26

I believe that as I did not give any confidential information about my accounts with BoV to any outside party, the fault lies purely with the Bank's security and they should compensate me to the full or at least to 90% of the total stolen."[8]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[9] tagħhom datata 22 t'April 2026, il-BOV qalu:

II. The Bank's point of view

"4. Whereas according to the Bank's records[10] *the two transactions effected on the 21st July 2025, in the amounts of €9,550 and €3,000, were duly authorised through the Complainant's banking channels following successful authentication. As part of the Bank's security framework, which is fully aligned with the requirements of the Payment Services Directive 2 (PSD2), multiple layers of authentication were applied to ensure that the transaction originated from credentials and systems in the Complainant's name. In fact, the transaction had no indication that it was fraudulent at the time of processing;*

5. 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:

> *'40. (1) A payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction'*

6. Whereas the Bank implemented the necessary measures to ensure that its systems are secure and in line with the PSD2 which provides the following on Strong Customer Authentication (SCA):

> *''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*

[8] P. 4
[9] P. 48 - 59 u dokumenti annessi p. 60 - 119
[10] Doc. A

> *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'.*[11]

7. Whereas apart from SCA, the Bank also implements a system of dynamic linking as outlined in Commission Delegated Regulation (EU) 2018/389, which supplements PSD2.

8. Whereas these payments were approved using the confidential details of the Complainant. The Bank had no control over the transfers because they were initiated without the Bank's intervention. Once the Bank receives legitimate instructions for a third-party payment through its secure and authenticated channels, the Bank is obliged to implement them, as it is reasonably expected that the only person with access to such confidential details and systems is the account holder. In this case, the transactions were duly authorised following successful validation of the Complainant's credentials, and there was no indication of fraud at the time of processing. In fact, this is outlined in the Bank's terms and conditions 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.'*[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]

[11] Article 4(30) of PSD2
[12] Doc. B, page 5
[13] Emphasis added

9. Whereas moreover the abovementioned Commission Regulation provides that the Bank can decide not to apply SCA for transactions which are considered to have a low level of risk. Therefore, one can conclude that when a transaction is considered to be of a higher risk, the Bank should implement the use of SCA. In fact, the Bank always implements the use of SCA to ensure that it implements the highest level of security possible (even if a transaction is considered to be low risk). In fact, in this case, both transactions were approved through SCA;

10. Whereas without prejudice to the above, if the Complainant is alleging that these transactions were not authorised by him, 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 performed the necessary actions which enabled its approval. 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:*
>
> *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.'*

11. Whereas article 50(1) of the Directive provides that:

> *'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 the fact that the Complainant provided the necessary details which enabled the approval of the payment, goes against the Bank's terms and conditions which provide 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.'*[14]

13. 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/mobile banking from a link in a SMS, because it has the adequate systems for this service to be accessed. In fact, the Bank warns customers to be careful what information they disclose, particularly on links;

14. Whereas it is significant to state that prior to the incident, the Complainant's registered number received eight anti-fraud SMS warnings from the Bank between November 2023 and July 2025 consistently instructing him not to click links and not to disclose passwords, PINs, verification codes or online-banking credentials via SMS/email/phone:

[14] Doc. B, page 7

(i) 10th November 2023 – SPOT THE SCAM. Please be vigilant. BOV never sends links by SMS. DO NOT click on any links and do not provide personal information, passwords or card details.

(ii) 5th February 2024 – SPOT THE SCAM. BOV will NEVER send you an sms/email with weblinks that ask you to provide card details, PIN, verification codes or online banking passwords.

(iii) 25th April 2024 – SPOT THE SCAM. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests.

(iv) 22nd July 2024 – SPOT THE SCAM. BOV will NEVER ask you to unblock accounts, ask for Card Details, PIN, Verification codes or Passwords via telephone or sms/email with links.

(v) 22nd October 2024 – SPOT THE SCAM. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests.

(vi) 21st January 2025 – SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links.

(vii) 16th April 2025 – SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links.

(viii) 16th July 2025 – SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links.

15. Whereas the content of the abovementioned SMS warnings was clear, repeated and unambiguous, and was specifically designed to prevent customers from falling victim to spoofing and smishing fraud, whereby fraudsters impersonate banks through SMS messages containing links and urgent instructions as well as through telephone calls;

16. Whereas the Bank further reinforced these warnings through campaigns carried out across newspapers, television, radio and social media, aimed at educating customers on how to identify spoofed communications and avoid disclosing personalised security credentials. These initiatives included television and radio appearances by Bank representatives explaining the nature of such fraud and how it may be detected, as well as multiple informational posts and articles disseminated throughout 2025, as evidenced by the documentation produced;[15]

17. 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 (MFSA) 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'[16] *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.'*

18. Whereas despite all these warnings, the Complainant still carried out all the necessary actions which enabled the payments to be approved and

[15] Doc. C

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

therefore, he breached the terms and conditions and this against the above-mentioned article 45(1) of the Directive.

19. Whereas besides this, he also acted against article 45(2) of the Directive because he did not take all the reasonable steps to keep his bank transfer number 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 them;

20. Whereas therefore, any alleged fraud occurred due to the participation of the Complainant who provided confidential information to a fraudster and followed the instructions given to him. All this contributed to his gross negligence;

III. Timeline of Events

21. Whereas upon being notified by the Complainant of a suspected scam on the 21st July 2025, the Bank's Customer Service Centre ("CSC")[17] *immediately authenticated the Complainant and blocked his internet banking access to prevent further unauthorised transactions. The Bank also stopped all credit and debit cards linked to the Complainant's profiles. The matter was escalated internally to the relevant units. On the same day, the Bank successfully blocked a €2,000 transaction before completion, demonstrating that protective controls were promptly activated. The Complainant was advised to urgently file a police report to support any recall requests. On the 28th August, the Complainant contacted CSC requesting the Beneficiary IBANs of the fraudulent payments, stating these had been requested by Police. These were duly provided to the Complainant;*[18]

22. Whereas the Bank immediately initiated recall requests for the two payments of €9,550[19] *and €3,000*[20] *that had already been executed. Camt056 fraud recall messages were sent via RTGS, and SWIFT MT992 notifications were transmitted to the beneficiary bank. Direct emails were*

[17] CSC - Recording 1
[18] CSC - Recording 2
[19] Doc. D
[20] Doc. E

also sent to the beneficiary bank, clearly marked as "FRAUDULENT – TOP URGENT," requesting urgent action to block and return the funds. It is important to note that the outcome of the recall process depends entirely on the receiving bank's internal procedures and availability of funds. The Bank has no control over other banks and therefore cannot dictate the timeframe for their response or guarantee the success of the recall;

23. Whereas the Bank respectfully submits that it acted promptly and diligently to recover the funds. Once the Bank received a reply from the beneficiary bank, it informed the Complainant accordingly. On the 19th September 2025, the Bank was notified that only a minimal amount of funds remained available for return. The Bank then informed the Complainant of the outcome and explained the next available steps[21]*. This demonstrates that the Bank exhausted all possible recovery channels within its control;*

24. Whereas the Bank continued to pursue the recall and kept the Complainant informed of all developments. The Complainant was advised that the success of the recall process depended on the cooperation of the foreign bank, which was outside the Bank's control.[22] *The Bank provided transaction documentation and updates upon request and offered the Complainant the option to apply the Office of the Arbiter's compensation model once the recall process was exhausted;*

25. Whereas after a thorough internal review and approval process, the Bank made a without prejudice offer of €3,765 (30%) in full and final settlement to the Complainant on the 22nd December 2025,[23] *in line with the Arbiter's established model for similar cases. The Complainant rejected this offer and demanded reimbursement of at least 90%;*

26. Whereas Customer Resolutions issued reminders requesting confirmation of the Complainant's position between January and March 2026. Upon continued rejection of the offer, the matter was reviewed

---

[21] Doc. F
[22] Doc. G
[23] Page 029 of the Complaint

again internally, and the Bank confirmed that its position remained unchanged. The Complainant was informed accordingly;

IV. Rebuttal of the Complainant's specific allegations

27. Whereas the Complainant alleges that the scammer appeared to possess knowledge of his account details and balances, the Bank respectfully submits that this assertion is speculative and unsupported by any evidence. The Bank's systems are fully compliant with PSD2 and employ robust security measures including multi-factor authentication, secure device registration, and ongoing transaction monitoring. The Complainant's claim that the scammer had "perfectly credible" information is based solely on his own perception and cannot be substantiated. There is no evidence before the Arbiter that any Bank employee was involved or that any internal breach occurred. The Bank relies strictly on the facts as presented and documented; any suggestion of "insider involvement" or systemic failure is unproven and must be dismissed as conjecture. The Bank's position is further reinforced by the absence of any adverse findings in transaction monitoring, beneficiary screening, or device authentication logs. Accordingly, the Bank submits that its security framework operated as required by law and regulation, and that liability cannot be imputed to the Bank on the basis of unsubstantiated speculation;

28. Whereas the Complainant claims that the Bank was uncooperative, the Bank's timeline of events demonstrates prompt and diligent action at every stage: immediate blocking of banking access and cards, successful cancellation of a €2,000 payment, same-day initiation of recall procedures for the disputed payments, persistent follow-up with the beneficiary bank, and regular communication with the Complainant regarding the status of recalls and compensation. The Bank exhausted all possible recovery channels within its control and kept the Complainant informed throughout;

29. Whereas the Complainant expects full reimbursement or at least 90% and does not appear to accept any responsibility for the outcome, the Bank respectfully submits that liability for unauthorised transactions is

> *governed by PSD2, Article 45 and Article 50 of Directive 1 of the Central Bank of Malta, as well as the Bank's terms and conditions. Customers are required to safeguard their credentials and follow all security guidance. Despite repeated warnings, the Complainant carried out actions which enabled the payments to be approved, including providing confidential information to a fraudster and following instructions received via a suspicious link. These actions constitute gross negligence and breach of contractual obligations. The Bank's offer of compensation was made strictly in line with the Arbiter's established model and as a gesture of goodwill, not as an admission of liability."*

BOV ipprovdew ukoll reġistrazzjoni ta' telefonata bejn l-Ilmentatur u l-Bank fil-ġurnata li saru l-pagamenti ilmentati li għaliha saret referenza hawn fuq. Kien hemm telefonata oħra li saret wara fejn l-Ilmentatur talab in-numri IBAN tal-kont fejn marru l-flus biex jgħaddihom lill-pulizija. Dawn ingħataw verbalment waqt it-telefonata.

Seduti

Fl-ewwel seduta tal-15 ta' Mejju 2026, l-Ilmentatur spjega l-każ kif diġà riprodott hawn fuq. Ammetta li sar jaf bil-frodi wara li ċemplitlu 'Brooke' mill-BOV biex tinfurmah bil-pagamenti li saru u ż-żamma tat-tielet pagament.

Ammetta wkoll li l-pagamenti li saru kienu taħt il-limitu tal-pagamenti tal-kont li wara ġie stabbilit li kien jammonta għal €25,000.[24]

Waqt kontroeżami qal:

> ***"Naqbel li fil-21 ta' Lulju 2025 irċevejt SMS li kien jidher li ġej mill-bank.***
>
> ***Mistoqsi naqbilx li f'dan l-SMS (paġna 40 tal-proċess) kien hemm miktub li ġew applikati xi limits, u sabiex ikolli aċċess kelli nagħmel Sign In, ngħid, iva u tawni numru li stajt nagħmel click in jew inkella nċempel fuq in-numru eżatt tal-Customer Care għax iċċekkjajtu. Kien tajjeb, preċiż in-numru tal-bank.***

[24] P. 150

Nikkonferma li fuq l-SMS frawdolenti kien hemm in-numru ġenwin tal-bank.

Mistoqsi ċempiltx dan in-numru, ngħid li le.

Mistoqsi naqbilx li dan l-SMS ma kienx jirrikjedi emerġenza immedjata fejn flusi kienu qed jittiedu mingħajr il-permes tiegħi, ngħid iva, jekk qed tpoġġiha hekk, imma jiena inkwetajt għax qal li imblokkjawli l-account.

Mistoqsi għafastx il-link, ngħid li jien ma niftakarx. Imma naħseb li għafast il-link la jien ma ċempiltx.

Qed jingħad li fil-Police Report hemm li jien għafast il-link. Ngħid li mela definitely li għafast il-link għax aktar stajt niftakar preċiż meta mort nagħmel ir-rapport milli issa.

Qed jingħad li l-link kien daqsxen stamb u kellu Ref 12922.

Mistoqsi jekk ġinix f'moħħi li din ma kinitx link uffiċjali tal-bank minħabba din il-forma, u li ma kellux bov.com fuq wara tal-link, ngħid li mhux qiegħed quddiemi imma ma niftakarx eżatt.

Qed jingħad li ma kien hemm xejn relatat mal-BOV f'dan il-link u mistoqsi indunajtx kienx hemm xi ħaġa stramba, ngħid li le, lanqas għaddieli mit-toqba ta' moħħi għax jiena l-Customer Care number għaraftu u, allura, assumejt li kien mill-Customer Care. I had never come across it la qabel u lanqas minn dak iż-żmien 'l hawn.

Ngħid li għafast il-link u qaltli li mblokkawli xi transfers li kienu qegħdin isiru.

Mistoqsi niftakarx fejn ħaditni din il-link, ngħid li assolutament ma niftakarx.

Mistoqsi ħadtx xi screenshot ta' din il-website li dħalt fiha meta għafast il-link, ngħid irrid niċċekkja.

Ngħid li pjuttost milli ġara xi ħaġa, ċemplitli din il-mara u li ma bgħatt lil ħadd għax kieku kien hemm follow-up kont nagħmel xi ħaġa. U jien ma għamilt xejn assolutament. I do not recall getting into a website. I would *have noticed if I were in a website. I definitely did not give any or put on the line any number which would have been confidential.*

Dak li jien żgur li dakinhar la semmejt u lanqas ktibt xi numru kunfidenzjali. L-uniku numru li ssemma' kien in-numru ta' 903871, l-Activation Code biex nidħol fuq il-website tal-kont tiegħi.

Qed jingħad li jien kont semmejt li daħħalt xi numru. Ngħid, assolutament li le, dak kien l-uniku numru li semmejt, konvintissimu minn dan.

Qed niġi mistoqsi mill-Arbitru fehemx tajjeb li jien qed nicħad li bil-link jew verbalment bit-telefon tajtha xi numri, l-kredenzjali tiegħi li s-soltu npoġġi biex nidħol fil-kont tiegħi il-bank.

Jien ngħid bl-eċċezzjoni tan-numru 903871. It is not a secret code. Dan in-numru hu l-User ID. Dan niftakar li ssemma' jew semmejtulha jew għamiltu. The User ID came up in conversation.

Qed jingħad li biex nidħol fil-kont tiegħi irrid kemm il-User ID u kemm il-One-Time Password.

I definitely did not do that.

Ngħid li din minkejja li ma tajthiex il-One-Time Password, kienet qisha daħlet fil-kont u bdiet tgħidli x'għandi u x'ma għandix.

Nikkonferma li hekk qed ngħid.

Jien għamiltha ċara mill-bidu. Għidtilhom bilfors li kien hemm xi ħadd minn ġewwa bl-informazzjoni li kellha mingħajr ma tajtha link jiena.

Mistoqsi jekk inix qed ngħid li meta għafast il-link ma dħaltx ġo website, ngħid li l-unika reaction li ċemplitli.

Qed jingħad li jien għidt li daħħalt il-User ID x'imkien.

Ngħid li le, forsi fid-diskors magħha. Naf li ssemma'. Hemmhekk żgur ma daħħaltux għax jekk għafast il-link, ma kellix bżonn indaħħal in-numru.

Qed jingħad li skont jiena irċevejt telefonata u din it-telefonata damet nofs siegħa.

Ngħid li it took a long time, xi twenty minutes, thirty jew thirty-five minutes għax ma niftakarx sew.

Mistoqsi waqt dawk it-tletin minuti jew sakemm qrajt il-messaġġ u ċemplitli din il-persuna ġinix f'moħħi li nċempel il-bank fuq in-numru uffiċjali, ngħid li assolutament ma daħalli l-ebda suspett.

Ngħid li ma ċempiltx il-bank fuq in-numru uffiċjali għax hi kienet vera polite, vera nice. Qaltli li jkun hemm ħafna minn dawn l-affarijiet. Qaltli li they often come across them. Imma li għandi nserraħ moħħi għax huma jieħdu ħsieb. Kienet qed tinstema' li tieħu ħsieb l-interessi tal-bank. Ma kien hemm xejn li qajjimli suspett.

L-Arbitru jagħmel referenza għall-Police Report fejn hemm miktub:

'Afterwards he received a message:

'Here is your activation code. Please use it within one hour to activate your BOV Mobile App.'

U jagħtik code.

Mistoqsi x'ħin irċevejt dan il-messaġġ, ngħid xi 9:32. Naħseb li l-ewwel irċevejt dan, għafast il-link u ċemplitli hi fil-pront wara.

Qed jingħad li jien qed nitkellem fuq l-ewwel messaġġ li kien fih il-link. Dan il-messaġġ ma kienx fih link.

Mistoqsi dan it-tieni messaġġ meta rċevejtu, ngħid li ma nafx ngħid offhand.

L-Arbitru jispjega li dan il-messaġġ ikun mibgħut miċ-channel tal-BOV (Channel BOV Mobile) għax ikun messaġġ ġenwin mill-bank, jiġifieri xi ħadd (il-frodist) ikun talab lill-bank għall-activation code u l-bank bagħat dan l-activation code fuq il-mobile tiegħi.

Mistoqsi x'għamilt b'dan il-code, ngħid li ma niftakarx.

L-Arbitru jagħmel referenza għal SMS ieħor li hu msemmi fil-Police Report li jgħid:

'BOV Alert. The following transfer has been successfully blocked by our Fraudulent Department.'

L-Arbitru qed jagħtini permess biex jekk insib l-SMS bl-activation code, nibgħatu lill-Arbitru u li, fejn għandi ngħidlu fi x'ħin irċevejtu u jekk niftakarx jekk il-code kontx ikkomunikajtulha verbalment jew jekk kontx poġġejt fuq xi website.

Rigward in-numru 903871 ngħid li dan ma daħħaltu mkien imma ssemma'.

Qed jingħad li mar-risposta tal-bank ġiet annessa lista ta' SMSes (paġna 53) li l-bank bagħat lil kull klijent fejn bdew mill-10 ta' Novembru 2023 u kull tliet xhur kien jibgħat SMS biex ifakkar dan il-messaġġ. U l-aħħar messaġġ li rċevejt qabel ma saret din il-frodi, kien biss ħamest ijiem qabel, fis-16 ta' Lulju, fejn jgħidlek:

'Spot the Scam. BOV will never ask you to transfer money or provide your card account details, PIN codes or passwords via phone, SMS, emails or links.'

Ngħid li iva irċevejt ħafna minnhom matul is-snin, però, qatt ma kelli każ li xi ħadd iċempilli u jgħidli l-account numbers tiegħi."[25]

Wara s-seduta, l-Ilmentatur bagħat kopja tal-SMSs li kien irċieva, fosthom, dak li kien ġenwin mill-BOV bl-*activation code xm44tGu3*[26] kif kien diġà rrapporta fir-rapport tal-pulizija

Saret seduta oħra fit-2 ta' Lulju 2026[27] għall-provi ta' BOV.

Xehed Michael Gatt li huwa inkarigat mill-*electronic payments.* Spjega li mingħajr ma

1. l-klijent ikun żvela l-kodiċi sigrieti inkluż il-*One Time Password* (OTP) biex jidħol fl-*internet banking*

[25] P. 121 - 124
[26] P. 128 - 129
[27] P. 132 - 138

2. jiżvela wkoll l-*Activation Code* li bagħat il-bank permezz ta' SMS, li permezz tiegħu setgħu jiġu awtorizzati pagamenti mill-frodist daqslikieku kien awtorizzahom il-klijent,

il-pagamenti ilmentati ma setgħux isiru. Ikkonferma li l-pagamenti saru wara li, permezz tal-*activation code* li b'xi mod ġie kkomunikat mill-Ilmentatur lill-frodist, il-frodist seta' jirreġistra l-BOV *Mobile Application* fuq *device* tiegħu u, fil-fatt, il-pagamenti ilmentati saru permezz ta' *token* ġdid li kien għadu kif ġie rreġistrat permezz tal-*activation code*.

Xehed ukoll Ryan Caruana bħala *Group Chief Anti-Financial Crime Officer* (u MLRO) ta' BOV. Huwa spjega s-sistema ta' moniteraġġ ta' pagamenti tal-Bank li hija *risk-based approach* skont ir-regolamenti. Qal li ma kien hemm xejn fin-natura tal-pagamenti li jindika li l-Bank naqas b'xi mod billi s-sistema ma waqqfithomx.

> ***"Ngħid li l-klijent, fl-aħħar xhur, fl-aħħar snin, imma dawn it-tranżazzjonijiet huma fuq l-aħħar tnax-il xahar, għamel tranżazzjonijiet ferm akbar minn dawn it-tranżazzjonijiet li sfortunatament ġie ffrodat bihom.***
>
> ***Ngħid li fl-aħħar ġimgħat, kien hemm pagament ta' €20,000 illi mar cross-border, ġo l-Italja li hu pajjiż simili ħafna tal-Lussemburgu meta wieħed jara r-risk rating ta' dak il-pajjiż kif ukoll tranżazzjonijiet oħrajn li marru wkoll lejn pajjiżi simili b'ammonti akbar minn dak li l-klijent ġie ffrodat bihom.***
>
> ***Ngħid li jekk wieħed irid jibqa' mal-obbligu tal-bank li juża r-risk-based approach, m'hemm xejn ħażin li din it-tranżazzjoni minn account li huwa użat regolari, minn account li telqu tranżazzjonijiet cross border għal pajjiżi barra minn Malta, lejn low-risk countries li huma akbar minn dik it-tranżazzjoni li ġie ffrodat biha, ma kien hemm l-ebda obbligu – anzi kont immur kontra l-obbligu ta' point B ta' page 18 tal-Guidance Document tal-FIAU – kieku kelli nwaqqaf dik it-tranżazzjoni illi kienet tkun allura mingħajr bażi għalfejn kelli nwaqqafha."***[28]

---

[28] P. 135

…

"Ngħid li nirreferi għall-pagamenti li saru f'Ġunju u Lulju fis-sena li għaddiet.

Ngħid ukoll li kien hemm tranżazzjonijiet lejn l-Ingilterra ta' €170,000, tranżazzjonijiet lejn l-Italja ta' €123,000.

Ngħid li kien hemm ukoll pagament ta' €2,000 li kien imwaqqaf mill-bank għax il-monitoring system ħadmet u ħadmet tajjeb.

Waħda mill-frodi li rajna fil-passat, kien hemm counterparty li kien hemm isem komuni li l-bank innota illi kien hemm dawn it-tip ta' red flags li l-pagament kien sejjer lejn bank ieħor ġol-Lussemburgu wkoll u li hemmhekk il-pagament waqaf u allura żammejna tranżazzjoni frawdolenti oħra milli ssir."[29]

Waqt kontroeżami kompla jixhed:

"Qed jingħad li għalkemm jien għidt li kienu saru ħafna transactions ta' somom akbar, kien hemm somma waħda li kienet akbar għax it-transfers l-oħra l-kbar kienu bejn accounts tal-klijent biex jiffinanzja dan il-kont, li ħareġ il-flus biex issellef l-account u ħadhom lura aktar tard.

Qed jingħad ukoll li kien hemm pagament wieħed biss u jgħid ċar li kien 'For Consultancy Fees with regard to Sicily. Legal fees Sicily on behalf of Lucia Mizzi.' L-oħrajn huma continuation għall-istess nies u li mhux vera li kien hemm ħafna pagamenti kbar.

Ngħid li kien hemm tranżazzjoni lejn l-Ingilterra ta' €170,000; kien hemm tnax-il tranżazzjoni illi marru lejn l-Italja.

Qed jingħad li l-pagament ta' 170,000 kien To repay loan lill-Barclays Bank u din ma kinitx xi anonymous addressee. It went to Rathbone Investment Management to repay a loan with Barclays Bank p.l.c.

Ngħid li f'dawn l-aħħar tnax-il xahar, lejn l-Italja, kien hemm tnax-il tranżazzjoni differenti li jammontaw għal €123,943, kif ukoll żewġ tranżazzjonijiet oħra illi kienu t-tranżazzjonijiet frawdolenti illi kienu

[29] *Ibid*.

sejrin lejn il-Lussemburgu, kienu l-inqas fl-ammont illi tranżazzjonijiet oħra li marru f'ġurisdizzjonijiet oħra kienu ħafna akbar fl-ammont.

Qed jingħad li jien qed niġbor l-ammonti kollha tat-tranżazzjonijiet l-oħra minflok ma nieħu l-każi individwalment. Qed jingħad li l-Ilmentatur qatt ma ħallas lejn il-Lussemburgu. Lejn Sqallija għax kien hemm proġett.

Mistoqsi kif ħadd ma nnota li l-Ilmentatur l-ewwel darba fl-istatements kollha li kellu mal-BOV li kienu ilhom ħafna żmien, li ħarġu żewġ orders fl-istess ġurnata lil dan l-indirizz Luxembourg, l-istess bniedem wieħed ta' €9,550 u l-ieħorta' €3,000 u l-uniċi tnejn li qatt kellu, PAYMENT ORDER OUTWARDS SAME DAY.

Ngħid li biex inwieġeb għal din id-d-domanda nirreferi għal tranżazzjoni li għamel l-Ilmentatur lejn l-Ingilterra fejn kienet l-ewwel tranżazzjoni lejn l-Ingilterra u li ma kinitx frawdolenti.

Qed jingħad li l-Ilmentatur mar il-branch personalment biex seta' jagħmel din it-tranżazzjoni lejn l-Ingilterra għax ma jistax jagħmel transfer ta' 170,000 online arbitrarily."[30]

Fl-aħħar xehed Luke Cutajar li kien l-uffiċjal inkarigat mir-*recalls* biex isir attentat biex il-flus jiġu rkuprati qabel ma jinġibdu mill-frodist.

Ikkonferma li r-*recalls* saru fil-ħin tal-11.00 a.m., kwarta wara li ġew informati bil-frodi, u li dawn ma tawx eżitu pożittiv għax kulma kien fadal fil-kont kien biss ammont ta' €22, li biex jiġu żbankati ntalbet *indemnity* li tinvolvi spejjeż akbar.

Sottomissjonijiet finali

Fis-sottomissjonijiet finali, il-partijiet bażikament sostnew il-pożizzjoni tagħhom kif esibita fl-ilment, fir-risposta u fix-xhieda waqt is-seduti**.**

[30] P. 136 - 137

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 jippersonifika l-Bank u jiffroda lill-klijenti.

Analiżi u konsiderazzjoni

L-Arbitru, 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 użat 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 jenfasizza 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, iridu jagħmlu iżjed biex iwissu b'mod effettiv lill-klijenti biex joqgħodu attenti; biex ma jagħfsux *links* li jkunu f'dawn il-messaġġi avolja jkunu jidhhru li ġejjin mill-bank konċernat fuq il-mezz li normalment juża l-bank biex jibgħat messaġġi lill-klijenti.

Mhux biżżejjed li jagħmlu avviżi kontinwi fuq il-*website* tagħhom. Mhux biżżejjed li joħorġu twissijiet fuq il-*mass media* jew *social media.* Il-konsumatur huwa impenjat bil-problemi tal-ħajja ta' kuljum u ma għandux jiġi pretiż li billi jsir avviż fuq il-*website*, fil-ġurnali/TV jew fuq il-paġna ta' *Facebook* tal-bank, b'daqshekk il-konsumatur jinsab infurmat.

F'każijiet serji ta' frodi bħal dawn jeħtieġ li l-banek jużaw komunikazzjoni diretta mal-klijent permezz ta' SMS jew *email*. Dan l-aspett huwa wieħed mill-fatturi inklużi fil-mudell.

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

Il-Qorti Ewropea tal-Ġustizzja (CJEU) fil-każ ta' *Wind Tre and Vodafone Italia*[31] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara każi fejn l-Ilmentaturi faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[32] 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.

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.[33] [34]

[31] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[32] Article 64 of PSD 2
[33] (EU) 2018/389 tas-27 ta' Novembru 2017 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[34] PSD 2 EU 2015/2366 Artiklu 68(2).

Deċiżjoni

L-Arbitru jiddeċiedi skont kif ipprovdut 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.

Qabel ma japplika l-mudell għaċ-ċirkostanzi partikolari ta' dan il-każ, l-Arbitru jrid jasal għal ġudizzju dwar il-bilanċ tal-probabbiltà tal-argumenti opposti tal-partijiet dwar kif l-*Activation Code*, li mingħajru l-i*scammer* ma setax jawtorizza pagamenti, ġie a konoxxenza tal-frodist.

Irid jiġġudika jekk kienx mgħoddi mill-Ilmentatur billi daħħal l-informazzjoni fil-*website* frawdolenti jew ikkomunikah verbalment, jew jekk, kif isostni l-Ilmentatur, dan l-*Activation Code* għalkemm kien fil-fatt irċevieh, ma kien bl-ebda mod għaddih lill-frodista.[35]

Fl-assenza ta' spjega aktar kredibbli, l-Arbitru jara probabbiltà li kien l-Ilmentatur li b'xi mod ikkomunika l-*Activation Code* lill-i*scammer*. Sal-mument li ċemplitlu 'Brooke', l-Ilmentatur kien għadu jemmen li Stephanie, il-frodista, kienet fil-fatt rappreżentanta vera ta' BOV li kienet qed tgħinu jwaqqaf pagamenti frawdolenti. Veru każ tal-midinba tippoża ta' qaddisa.

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

[35] P. 145

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

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

Meta ppubblika l-mudell, l-Arbitru spjega li dan japplika b'mod ġenerali imma l-Arbitru jibqa' ħieles li ma jimxix miegħu f'każijiet speċifiċi li jirrikjedu apprezzament partikolari. Però, l-Arbitru jiġġustifika, bi spjegazzjonijiet adegwati fid-deċiżjonijiet tiegħu, meta ma jimxix ma' dan il-mudell, fejn applikabbli.

F'dan il-każ partikolari, il-mudell isib li l-Ilmentatur ikkopera mal-frodist billi għaddielu kull informazzjoni li kienet meħtieġa biex jiġu approvati l-pagamenti, inkluż b'mod partikolari l-*activation code* biex jinbidel id-*device* li fuqu hemm l-APP li tapprova pagamenti.

L-Arbitru jifhem li waqt it-telefonata konvinċenti mas-suppost rappreżentanta tal-Bank, l-Ilmentatur warrab is-salvagwardji soliti għax mill-informazzjoni li bdiet tagħtih dehret telefonata ġenwina.

Għalhekk, l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jitnaqqaslu l-piż ta' negliġenza grossolana b'doża ta' 40%, jiġifieri 20% aktar mill-20% normalment spjegat fil-mudell.

Dan huwa każ fejn il-frodist mhux biss bagħat SMS qarrieq iżda sostna l-kredibbilità tal-SMS permezz ta' telefonata konvinċenti minn persuna titkellem bil-Malti li tat informazzjoni li l-Bank biss seta' jkollu.

L-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat minn persuna li tippersonifika b'mod espert lill-Bank permezz ta' telefonata '*live*', allura, l-SMS bil-*link* frawdolenti tidher anqas suspettuża, minkejja t-twissijiet li l-Bank kien ħareġ.

F'dan l-aġġustament, minħabba ċirkostanzi speċjali, l-Arbitru qed jieħu wkoll kunsiderazzjoni ta' dawn il-fatturi:

A. opinjoni li diġà esprima f'deċiżjoni ta' każ ASF 116/2023 li meta jiġi rreġistrat *device* ġdid, irid isir proċess sħiħ ta' rikonferma mill-Bank li dan sar fuq talba ġenwina tal-klijent.

   F'dan il-każ, iżda, l-Arbitru jinnota li filwaqt li ma kienx hemm bidla tal-*mobile device* u l-istess numru baqa' rreġistrat mal-Bank,fil-proċess kien hemm bidla fis-*software token* li jawtorizza l-pagamenti.

   L-Arbitru jirrakkomanda li meta jkun hemm reġistrazzjoni ta' *software token* fuq *device* ġdid (li jkun jinvolvi wkoll *unenrolment* minn fuq id-*device* ta' qabel għax il-*mobile app* tista' tkun irreġistrata fuq *device* wieħed biss) għandu wkoll ikun hemm eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

L-argument li l-pagamenti setgħu jsiru biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi u għalhekk hemm bżonn ta' konsiderazzjoni profonda biex filwaqt li jinżammu pagamenti b'xamma ta' frodi, ma nsirux restrittivi b'mod li jiġu mblokkati pagamenti ġenwini li ovvjament huma f'maġġoranza kbira.

Hemm eżempji ta' istituzzjonijiet finanzjarji u banek li għandhom sistemi ta' pagamenti b'teknoloġija avvanzata, fejn f'każ serju ta' dubju jintbagħat SMS fuq il-*mobile* irreġistrat, jinforma li qed jintalab li jsir pagament u l-klijent jingħata kodiċi li jdaħħal fis-sistema biex jikkonferma l-pagament. Dan isaħħaħ is-sigurtà u jevita dewmien biex isir kuntatt permezz tat-telefon mal-klijent.[36]

B. L-argument li l-Bank huwa b'xi mod responsabbli għat-telf imġarrab, għax kellu obbligu li s-sistema ta' moniteraġġ ta' pagamenti tkun sensittiva biżżejjed biex twaqqaf il-pagamenti ilmentati, huwa miċħud.

BOV waqqfu t-tielet pagament u pagamenti oħra li setgħu saru fil-limitu ta' €25,000 għal pagamenti fil-ġurnata. Dan huwa sinjal ċar ta' sistema li ħadmet b'mod effikaċi. Ġie stabbilit mit-telefonata rreġistrata ta' 'Brooke' li l-Ilmentatur ma kienx irrealizza li ġie ffrodat, u 'Brooke' kellha tkun persważiva biex l-Ilmentatur jifhem li 'Stephanie' kienet frodista.

F'Ġunju 2025, l-Ilmentatur mill-istess kont kien għamel erba' trasferimenti esterni ta' €5,000-ilwieħed, pagament estern ta' €20,000, u pagament ieħor estern ta' €2,484, kollha deskritti bħala *Professional Service/Consultancy Fees*.

[36] Dan it-tip ta' sistema diġà qed jopera permezz ta' *3D Secure* f'każ ta' pagamenti bil-*card* lill-*merchants* għal xiri *online*.

Iż-żewġ pagamenti ilmentati saru xahar wara u wkoll ġew spjegati bħala *Professional Service.*

Għal din ir-raġuni, iż-żieda għal ċirkostanzi speċjali hija ta' 20% u mhux ta' 30%, bħal fil-każ ASF 033/2026, fejn l-Arbitru sab nuqqas fis-sistema ta' moniteraġġ ta' pagamenti, speċjalment wara l-introduzzjoni ta' *Instant Payments* f'Ottubru 2025.

Il-mudell jiġi għalhekk emendat kif ġej:

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatur**
Ilmentatur li jkun wera traskuraġni grossolana	0%	(100%)
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	(50%)	50%
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	20%	(20%)
Sub-total	0%	(100%)
Tnaqqis għal ċirkostanzi speċjali	(40%)	40%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(40%)**	**(60%)**

B'kollox, għalhekk, l-Ilmentatur jiġi intitolat għal kumpens ta' 40% tat-telf li sofra minn pagamenti frawdolenti li ġew iddebitati fil-kont tiegħu mal-Bank.[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' ħamest elef u għoxrin ewro (€5,020).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% 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.

Fl-aħħarnett, l-Arbitru jirreferi għal rapporti mhux konfermati li l-pulizija irnexxielhom jimblokkaw xi fondi misruqa mill-frodisti u, għalhekk, eventwalment jista' jkun hemm xi rkupru minn dan is-sors.

Jekk jirriżulta rkupru bħal dan, biex ma jkunx hemm possibilità ta' arrikkament inġustifikat, l-Arbitru jordna li l-flus ta' xi rkupru jiġu allokati bl-istess mod kif ġie allokat it-telf f'din id-deċiżjoni, jiġifieri 40% għall-BOV u 60% għall-Ilmentatur.

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[37] 40% ta' €12,550

[38] Ekwivalenti għall-*'Main Refinancing Operations (MRO) interest rate'* kurrenti stabbilita 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.

<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. Dettalji personali tal-Ilmentatur/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.