Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 105/2026

OH

('l-Ilmentatriċi')

vs

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

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

Seduta tal-20 ta' Novembru 2026

L-Arbitru,

Ra l-Ilment[1] datat 07 t'April 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi aktar minn 20% tat-telf li sofriet meta sar pagament frawdolenti ta' €5,000 mill-kont tagħha mal-BOV.

Il-pagament sar fid-19 ta' Jannar 2026 fil-ħin ta' 10:39 favur Lee Garret Fennelly f'kont ma' ditta lokali liċenzjata (Moneybase).[2]

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'*.

[1]Paġni (P.) 1 - 12 b'dokumentazzjoni addizzjonali minn P. 13 - 42.

[2]P. 40; Fir-risposta tal-Bank jingħad li t-tranżazzjoni ġiet awtorizzata fil-ħin ta' 10:37:03 (P. 47). Il-log tal-*Internet Banking* juri żewġ awtorizzazzjonijiet ta' pagament, waħda fil-ħin ta' 10:37:03 u oħra fil-ħin ta' 10:39:33, filwaqt li l-messaġġ tal-pagament ilmentat inħoloq fil-ħin ta' 09:39:38 UTC, jiġifieri 10:39:38 ħin Malti (P. 57; 121).

- 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' fteħim bejn il-bank u l-klijent dwar min hu responsabbli jġorr il-piż tal-pagament frawdolenti. Il-klijent isostni li l-bank ma pproteġihx meta ħalla kanal ta' komunikazzjoni li normalment użat bejn il-bank u l-klijent jiġi ppenetrat mill-frodist, u li l-bank messu nduna li kien pagament frawdolenti għax, ġeneralment, il-klijent ma jkollux storja ta' pagamenti bħal dawn. Il-bank isostni li l-ħtija hija kollha tal-klijent għaliex permezz ta' traskuraġni grossolana (*gross negligence*), ikun ta aċċess tal-kredenzjali sigrieti tal-kont tiegħu lill-frodist u b'hekk iffaċilita l-frodi.

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

- Fid-19 ta' Jannar 2026, fil-ħin ta' 10:16, irċeviet messaġġ fuq it-*thread* 'BOV Mobile' li kien jgħid li n-numru +35679020447 kien ġie miżjud u li, jekk dan ma kienx awtorizzat, kellha tidħol fil-*link*

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

https://bovportals104.com/. Dan daħal fuq il-kanal ta' SMS fejn normalment tirċievi notifiki mill-Bank.[4]

– Billi emmnet li l-messaġġ kien ġenwin, għafset il-*link* u daħlet f'*website* li dehret identika għal dik tal-BOV, fejn daħħlet il-*User ID* u l-*One-Time Password*. Il-*website* infurmatha li kienet ser tirċievi telefonata mill-BOV minn wieħed minn żewġ numri.[5]

– Fil-ħin ta' 10:27 irċeviet telefonata min-numru +356991800001. Dan in-numru jixbah ħafna lin-numru 9918 0001 li minnu l-Ilmentatriċi kienet tirċievi SMS mill-Bank, iżda għandu 0 żejjed. Fl-ilment, l-Ilmentatriċi tgħid li t-telefonata waslet min-numru +356 9918 0001.[6]

– Il-frodista, mara li titkellem bil-Malti, qalet li kienet impjegata tal-BOV u li min-naħa tagħha kienet qed tidher tranżazzjoni ta' €5,000. Mingħajr ma l-Ilmentatriċi tatha dawn id-dettalji, il-frodista kkonfermatilha n-numru tal-kont u l-indirizz tad-dar tagħha.[7]

– Waqt it-telefonata, il-frodista talbitha tidħol fil-*BOV Mobile App* u ddaħħal fil-funzjoni tat-*Transaction Signing* iż-żewġ numri li kienu jidhru fuq l-iskrin. Qaltilha wkoll li t-tranżazzjoni kellha tgħaddi iżda li l-Bank kien ser idawwar il-flus lura. It-telefonata damet 15-il minuta u 39 sekonda.[8]

– Il-pagament ta' €5,000 sar bis-sistema ta' *Instant Payments*. Fil-ħin ta' 18:16 tal-istess jum, l-Ilmentatriċi rċeviet SMS mill-Bank li l-pagament kien ġie pproċessat.[9]

– Fl-20 ta' Jannar 2026 ippruvat iċċempel lura lin-numru li minnu rċeviet it-telefonata, iżda ma rnexxilhiex. Sussegwentement, meta reġgħet ippruvat tidħol fil-*link*, il-*browser* indikalha li l-*link* ma kinitx sigura.[10]

– Fil-21 ta' Jannar 2026 ċemplet lill-*fraud helpline* tal-BOV fejn ġie kkonfermat li kienet frodi. Il-Bank irċieva t-talba għar-*recall* fil-ħin ta'

[4] P. 3; 17
[5] P. 3; 125 - 126; 129
[6] P. 3;
[7] P. 3 - 4; 126
[8] P. 4; 19; 126 - 129
[9] P. 42;
[10] P. 4 - 5; 19; 127; 129

09:40 u fil-ħin ta' 09:44 bagħat *camt.056* lill-bank benefiċjarju. Fl-istess jum, l-Ilmentatriċi għamlet rapport lill-pulizija.[11]

- Fis-27 ta' Jannar 2026, irċeviet messaġġ frawdolenti ieħor fl-istess *thread*, din id-darba bil-*link* https://bovportal104.com/.[12]
- Fil-5 ta' Frar 2026, il-bank benefiċjarju informa lill-BOV li ma kienx fadal flus fil-kont tal-benefiċjarju u għalhekk ir-*recall* ingħalaq bla suċċess.[13]
- Fit-2 ta' Marzu 202,6 il-BOV offrielha, mingħajr preġudizzju, is-somma ta' €1,000, jiġifieri 20% tat-telf, wara li applika l-mudell tal-Arbitru. Fl-10 ta' Marzu 2026, l-Ilmentatriċi talbet rimborż ta' 75%, iżda fit-12 ta' Marzu 2026, il-Bank informaha li l-pożizzjoni tiegħu ma nbidlitx.[14]

L-Ilment

L-Ilmentatriċi qed titlob kumpens ta' mill-inqas 75% tat-telf ta' €5,000 għax skont hija:

> *"I respectfully submit that a settlement of 20% of the disputed amount is manifestly unfair given the circumstances of this case and the tactics used by the scammer to impersonate Bank of Valletta. In particular:*
>
> *1. The scammer exploited a continuous message thread previously used exclusively by BOV, making the fraudulent messages appear authentic and trustworthy.*
>
> *2. The messages and the telephone call utilised the same branding, language, and formatting consistent with official bank communications, which further increased their credibility.*
>
> *3. The scammer had ready access to my personal and banking information, including my account number and residential address, without any input from my side.*

[11] P. 36 - 37;
[12] P. 17
[13] P. 24; 122
[14] P. 21; 29; 33

4. The bank failed to prevent the unauthorised transaction, despite several warning signs:

- The transaction was outside my normal activity patterns. The account targeted is not linked to a card and is primarily used for transfers between my own accounts.

- In 2024 there were no external transactions, and in 2025 only three transactions were made to third parties.

- Despite being below the €5,000 threshold, this transaction should have triggered enhanced verification or intervention by the bank's fraud monitoring systems.

5. The bank has not implemented sufficient preventative safeguards, leaving long-standing customers vulnerable to sophisticated scams.

Furthermore, the bank's handling of this incident demonstrates a lack of consideration for loyal clients, who maintain other financial relationships with the bank, including shareholder and home loan accounts. It should also be noted that security breaches affecting BOV accounts are not rare, and I personally have been a victim of unauthorised withdrawals in the past. This history, coupled with the ongoing reports of similar scams from 2024 onwards, made me cautious and hesitant when interacting with the link, yet despite this, the fraudulent attempt was still able to target me in January 2026. The continued occurrence of such incidents over this period suggests a systemic failure in the bank's preventative measures and monitoring, leaving long-standing customers exposed to significant risk.

Given the above factors, I respectfully request that the Financial Arbiter reconsider the Bank's proposed settlement of 20%."[15]

Dwar ir-rimedju li qed titlob, l-Ilmentatriċi tgħid:

"I strongly believe that, in view of the circumstances outlined above, a compensation of at least 75% is warranted.

[15] P. 7

The fraudulent messages and call were highly convincing: the branding and language closely resembled official bank communications, and the initial link (bovportals) appeared legitimate, with no obvious signs of fraud, unlike the later suspicious link (bovportal104).

It is also relevant that the account targeted by the scam:

- *is not linked to a card;*
- *is mainly used for transfers between my own accounts;*
- *had only three external transactions in 2025 and none in 2024.*

Despite the sophisticated impersonation, the bank's systems failed to detect or prevent the unauthorised transaction, even though similar scams had reportedly been occurring. As stronger safeguards could have prevented this loss, I submit that a reimbursement of at least 75% represents a fair and reasonable allocation of responsibility between the bank and myself."[16]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[17] tagħhom datata 27 ta' April 2026, BOV qalu:

"4. Whereas according to the Bank's records[18] *the transaction effected on the 19th January 2026 in the amount of €5,000, was duly authorised at 10:37:03 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;*

[16] P. 8

[17] P. 46 - 56 u dokumenti annessi p. 57 - 124

[18] Doc. A

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 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*[19]*"*

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 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;*

9. *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*

[19] Article 4(30) of PSD2.

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 transaction was duly authorised following successful validation of the Complainant's credentials, and there was no indication of fraud at the time of processing;

10. *Whereas the Bank's terms and conditions state that:*

"All payments, Instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your security credentials [...] are deemed as binding on you. You authorise us to act on any Instruction that we receive through the Channels [...] You will be liable for any transactions that we carry out on your behalf.[20]*"*

"You will however be unlimitedly responsible for all transactions carried out via the Channels prior to notification to us [...] if you have: [...] not notified us immediately of having suspicions or noticing irregular or unauthorised transactions or on becoming aware that your BOV Channel Credentials have become compromised, lost or stolen; [...] acted in any other way with gross negligence or fraudulently."[21]

"[...] once the payment is authorised following the verification of payee check, the Bank does not bear liability if the payment is credited and sent to the wrong beneficiary."[22]

"We will not be responsible nor liable for losses or costs which you may suffer [...] if we fail to comply with any of our obligations due to [...] unforeseeable circumstances outside our reasonable control [...] or due to our obligations to comply with any applicable law or

[20]Doc. B, Page 24.
[21]Doc. B, Page 25.
[22]Doc. B, Page 18.

regulations [...] unless any such losses, costs, damages, actions or expenses arise due to the gross negligence of the Bank."[23]

11. *Whereas the Bank further submits that the disputed transaction fell within the daily and per-transaction limits*[24]*, wherein the maximum permitted for third party payments via personal internet banking is €5,000 per transaction and up to a maximum of €5,000 per day. The payment in question, being €5,000, was therefore within such parameters;*

12. *Whereas without prejudice to the above, if the Complainant is alleging that this transaction was not authorised by her, then the Bank is still not obliged to refund her, since even if she did not have the intention to approve a payment, she 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."

13. *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

[23]Doc. B, Pages 23 to 24.

[24]Doc. C (https://www.bov.com/bov-digital-banking-limits)

fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence"

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/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;*

15. *Whereas it is significant to state that prior to the incident, the Complainant's registered number received twelve anti-fraud SMS warnings from the Bank between November 2023 and January 2026 consistently instructing her not to click links and not to disclose passwords, PINs, verification codes or online-banking credentials via SMS/email/phone:*

    (i) *11th 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 on-line 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) *20th 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) *15th 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) *15th 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."*

(ix) *28th August 2025 – "BOV will never send you SMS messages asking you to press on links. Do not click on them as you risk being defrauded! In case of doubt call BOV on 21312020."*

(x) *4th September 2025 – "Il-Bank of Valletta qatt ma jibgħatlek SMS b'links biex tagħfas fuqhom. Tagħfashomx għax tista' tiġi misruq! Jekk tiġi f'dubju, ċempel lill-Bank fuq 21312020."*

(xi) *22nd October 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide any details via message links or inform you to click on any links via a mobile message."*

(xii) *21st January 2026*[25] *– "Spot the Scam: BOV never requests money or security details via phone or SMS. Stay safe - ignore suspicious calls or links and contact us directly."*

16. *Whereas the abovementioned warnings are part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. Besides these SMSs, the Bank also publishes information regarding scams to which customers may be vulnerable to. The Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams. In fact, in the past years, the Bank has published*

[25] Dan kien wara li ġara l-każ.

multiple newspaper articles and coordinated TV and radio appearances where Bank employees explain what spoofing is and how to identify it. A comprehensive list of the available resources till September 2025 is being attached as ***'Doc. D'****.*

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' 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 payment to be approved and therefore, she breached the terms and conditions and this against the above-mentioned article 45(1) of the Directive;*

19. *Whereas besides this, she also acted against article 45(2) of the Directive because she 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 her gross negligence;*

III. Timeline of Events

(i) ***19th January 2026*** *– the transaction in dispute of €5,000 was processed from the Complainant's account;*

(ii) ***21st January 2026*** *– the Complainant contacted the Bank*[26] *and spoke to a Bank representative, who immediately informed her that the SMS was a scam, blocked her card, and informed her that a recall would be initiated. The Bank's Customer Resolutions Unit sent an acknowledgement to the Complainant, confirming that the recall process had been initiated and requested supporting screenshots. As advised by the Bank's representative, a recall of funds was immediately initiated by the Bank's Payment Investigations Unit ("PIU")*[27] *of the €5,000 payment. A formal fraud recall request was sent through SEPA channels at 09:44:43, a SWIFT message and an email were sent to the beneficiary bank on the same day, alerting them to the fraudulent nature of the payments and requesting urgent cancellation and return of funds. The recall request reference the police report filed by the Complainant and included all transaction details;*

(iii) ***26th January, 29th January, and 2nd February 2026*** *– the Bank sent three further SWIFT reminders and two additional email reminders to the beneficiary bank, escalating the urgency and reiterating the request for the immediate return of funds*[28]*;*

[26] *"On 21 January 2026, I contacted the bank's fraud helpline [...]"* (Page 005 of the Complaint).
[27] Doc. E
[28] *Ibid.*

*(iv) **5th February 2026** – the beneficiary bank replied, confirming that no funds remained in the recipient's account, and therefore the recall could not be affected.* [29]*The Bank informed the customer of the outcome;*

21. Whereas in view of the above, the Bank submits that it acted without delay, initiating the recall process immediately, and followed up persistently with multiple reminders and escalations until the final response was received from the beneficiary bank;"[30]

Seduti

Fl-ewwel seduta tas-26 ta' Mejju 2026, l-Ilmentatriċi kkonfermat bil-ġurament il-kontenut tal-ilment u spjegat il-każ tagħha kif ġa riprodott hawn fuq.[31] Hija ammettiet li daħħlet il-*User ID* u l-*One-Time Password* fil-*website* frawdolenti u li, fuq struzzjonijiet tal-frodista, daħħlet il-kodiċi fil-funzjoni tat-*Transaction Signing*:

"Ngħid li meta dħalt fuq din il-website li kienet tidher li hi tal-BOV, dettalji fuq it-telefon ma tajtx. Jista' jkun li meta għafast il-link kien hemm qisu xi log in. Jista' jkun li daħħalt il-User ID fil-link, però, verbalment jien m'għidtux il-User ID.

Ngħid li at a certain point, daħħalt il-User ID u l-One-Time Password.

Qaltli li ser tibgħatli l-log in details u qaltli hi l-address tad-dar fejn ser tibgħatli l-log in il-ġdida, jiġifieri hi kellha din l-informazzjoni: kemm l-account number u kemm l-address tad-dar.

Ngħid li l-User ID u l-One-Time Password ma tajthomx lilha, kemm daħħalthom fil-link.

Ngħid li qaltli li xorta kelli nagħmel xi steps oħra biex inkomplu l-proċess. Qaltli li fuq l-iscreen kienu ser jidhru żewġ numri u rrid indaħħalhom meta nagħmel xi Signature. Jien għamilthom għax ħsibt li din persuna

[29]*Ibid.*
[30]P. 47 - 55
[31]P. 125

> ***mill-BOV u qaltli li l-flus ser jiġu reverted mill-BOV għax kienu ser jiġbduhom lura."***[32]

Mistoqsija mill-Arbitru jekk waqt il-frodi rċevietx SMS b'*activation code*, l-Ilmentatriċi qalet li le.[33] Dwar l-informazzjoni l-oħra li talbitha l-frodista, il-verbal jgħid:

> ***"Qed jingħad li apparti li daħħalt il-User ID u l-One-Time Password biex hi daħlet fil-kont tiegħi, waqt li kont magħha donnha talbitni xi informazzjoni oħra.***
>
> ***Ngħid, iva, kien hemm żewġ numri fuq l-iscreen, u qaltli biex nidħol bit-Transaction Signing mill-App, (u ddaħħal iż-żewġ codes. Naħseb Transaction 2 kienet. Ngħid li ma rċevejtx messaġġi."***[34]

Fil-kontroeżami qalet:

> ***"Qed niġi mistoqsija nikkonferma li fid-19 ta' Jannar 2026, jien irċevejt messaġġ li kien fih link u li jien għafast fuqu u dan kien jgħidli li ser iċempilli l-bank u daħħalt il-User ID u l-One-Time Password.***
>
> ***Ngħid li mhux il-messaġġ qalli li ser iċempel xi ħadd, imma l-website u naqbel li qalli biex indaħħal il-User ID u l-One-Time Password.***
>
> ***Mistoqsija jekk għidtx f'ħin minnhom li l-website kienet immarkata bħala unsafe, ngħid li iva. Saret l-iscam, ġie suspicious għax hi qaltli li ser iċċempilli u ma ċemplitlix, wara li kellha tiċċekkja l-accounts biex tara kienx hemm xi transactions oħrajn.***
>
> ***Mistoqsija din rajthiex qabel, ngħid li le. L-ewwel darba li ftaħt il-link BOVportal, il-link infetħet normali, bil-logo tal-BOV, kollox normali kien jidher. Kien after two days li ġiet immarkata unsafe mill-Google.***
>
> ***Mistoqsija meta rċevejt dan l-SMS u bdejt nitħadded ma' din il-persuna, ġinix xi suspett, ngħid li ma ġinix suspett għax 1) kienet persuna Maltija***

[32] P. 126 - 127
[33] P. 128
[34] *Ibid*.

qisni qed nitkellem ma' operator tal-BOV normali; u 2) identifikat ruħha bħala employee tal-BOV, u jiena ma ġewnix suspetti dak il-ħin.

Apparti minn hekk, jien kelli biża' li kif jien għandi n-number tiegħi tal-BOV Mobile u jien nista' ngħaddi t-transaction lil persuna oħra through BOV Mobile bħal kif jidhru fit-thread tal-BOV Mobile ...

Mistoqsija kemm damet bejn wieħed u ieħor din it-telefonata, ngħid li damet xi ħmistax-il minuta. Ngħid li suppost għaddejt il-call log.

Nikkonferma li talbitni biex nidħol fil-BOV Mobile App u nagħmel Signature 1 jew Signature 2.

Mistoqsija naqbilx li biex nagħmel pagament bl-Internet Banking hemm bżonn jittieħdu ċerti passi, u li hemm bżonn jingħataw kredenzjali personali tiegħi, ngħid li jien ma tantx nagħmel pagamenti bl-Internet Banking għax ħafna drabi nuża applications oħra mhux tal-BOV innifisha, jew ħafna drabi jkunu tal-BOV Mobile li jkunu ammonti ġeneralment żgħar li n-numri diġà saved u li għandhom l-application tal-BOV stess, Mobile-to-Mobile.

Mistoqsija nagħmilx pagamenti bl-Internet Banking lil xi ħadd ieħor li mhuwiex tal-Bank of Valletta, ngħid li ħafna drabi iktar ikunu Pay Third Parties. Ngħid li kienet proċedura differenti minn li kienet din tal-iscam.

Ngħid li ġeneralment mill-mobile nagħmilhom dawn mhux mill-website. Ġeneralment tidħol l-ewwel darba fl-app, jitolbok it-third party min hu, l-ammont kemm hu. Ngħid li bl-amment ma nafx eżatt għax kif għidt, ma tantx nużaha.

Ngħid li mhux l-istess bħal din it-tranżazzjoni.

Qed niġi referuta għar-risposta tal-bank fejn f'paġna 51 u 52 tal-proċess hemm lista ta' SMSes li l-bank kien bagħat lili fuq in-numru tiegħi fejn qed iwissini fuq dawn l-azzjonijiet li seħħew.

Mistoqsija irċevejtx dawn l-SMSes li jintbagħtu fuq in-numru 99180001, ngħid li irċevejt tal-21 ta' Jannar 2026, tat-22 t'Ottubru 2025.

> ***Qed jingħad li intbagħtu aktar SMSes perjodikament qabel dawn it-tnejn li semmejt u mistoqsija nikkonfemax li dawn irċevejthom, ngħid li nikkonferma; għallinqas t'Ottubru nista' nikkonferma.***
>
> ***Mistoqsija nafx bid-diversi kampanji li qed isiru fuq dawn it-tipi ta' scams, ngħid il-verità, bdejt ninnutahom ħafna aktar wara l-iscam. Saru jsiru anke fuq it-television."***[35]

L-Arbitru talab lill-Bank jippreżenta kopja tal-i*statement* tal-kont minn fejn sar il-pagament għat-tnax-il xahar ta' qabel il-frodi.[36] Il-Bank ippreżenta l-i*statement* immarkat bħala Doc. F.[37]

Fit-tieni seduta li nżammet fid-9 ta' Settembru 2026, Dr Theuma talbet li l-paġni 20 sa 22 u l-paġna 33 tal-ilment jiġu sfilzati mill-proċess peress li jinkludu korrispondenza mingħajr preġudizzju. L-Arbitru ma laqax din it-talba, iżda qal li peress li dawn il-paġni huma mingħajr preġudizzju, ma jikkommettux lill-Fornitur tas-Servizz.[38]

Il-Bank ressaq ix-xhieda ta' Michael Gatt, *Senior Manager* fid-Dipartiment tal-*Electronic Payments* tal-BOV, li kkonferma bil-ġurament l-*affidavit* tiegħu.[39] Fl-*affidavit* spjega li biex klijent jidħol fl-*Internet Banking* irid juża l-*User ID* flimkien ma' *One-Time Password*, u li biex isir pagament lil terzi persuni, il-pagament irid jgħaddi mill-proċess tat-*Transaction Signing* permezz ta' *Signature 2* fil-*BOV Mobile Application*. Spjega wkoll li kull *BOV Mobile Application* hija marbuta ma' *software token* b'*unique serial number* u li l-Bank qatt ma jitlob lill-klijenti tiegħu il-*Login ID*, il-*One-Time Password*, l-*Activation Code* jew kodiċijiet oħra ta' awtentikazzjoni permezz ta' SMS, *email* jew telefonata.[40]

Waqt is-seduta, ix-xhud qal:

> ***"Mistoqsi mill-Arbitru jekk, f'dan il-każ, il-pagamenti sarux wara li nbidel it-token, ngħid li t-token ma nbidilx f'dan il-każ. L-istess serial***

[35] P. 129 - 130
[36] P. 130
[37] P. 131 - 134
[38] P. 142
[39] *Ibid*.
[40] Affidavit ta' Michael Gatt, p. 135 - 136

number intuża on the 5th u jekk niftakar sew on the 19th. Jiġifieri, b'xi mod jew ieħor, xi ħadd ikkomunika ma' frodista l-OTP password.

Mistoqsi jekk kienx hemm xi activation code li permezz tiegħu nbidel it-token ngħid le. Ngħid li kien hemm proċess normali ta' signature signing.

Mistoqsi mill-Arbitru jekk hux qed ngħid li mill-mobile app tal-Bank, li jkun biss fuq il-mobile tal-klijent, ġie ġenerat il-kodiċi li awtorizza l-pagament u li hi, b'xi mod, ikkomunikat lill-frodista, ngħid eżatt.

Mistoqsi mill-Ilmentatriċi kif jista' jiġi kkomunikat lill-frodista, ngħid li fil-maġġor parti tal-każi li jiġri hu li, konxjament jew inkonxjament, inti tkun ikkomunikajt... Mhux ħa jgħidlek agħtini signature 2; jibda jgħidlek 'isma', idħol 'l hawn, idħol 'l hemm, idħol 'l hawn, idħol 'l hemm', jiġġenera dan in-numru u b'xi mod jiġi kkomunikat lilu. Jiġifieri probabbilment inkonxjament inti tkun għaddejt is-signature 2 number lill-frodista.

Dr Theuma tfakkar li, fis-seduta li għaddiet, l-Ilmentatriċi xehdet li tat il-user ID, il-one-time password, u mbagħad ukoll, waqt it-telefonata, wettqet hi stess il-proċess ta' transaction signing.

Mistoqsi minn Dr Theuma biex nispjega r-relevanza ta' dawn il-passi li ħadet l-Ilmentatriċi, ngħid illi biex tiġi ġġenerata transaction signing l-ewwel nett irid ikollok aċċess għall-mobile. Imbagħad, kif ikollok aċċess għall-mobile trid tkun taf il-log-in ID, imbagħad bil-mobile ħa tiġġenera transaction signing signature 1 biex tidħol fl-internet banking. At that stage, ma jiġri xejn għax inti just qed tara l-bilanċi. Tiġi ġġenerata transaction, u mbagħad trid terġa' tmur fit-transaction signing u tagħfas u tagħmel is-signature 2.

Hemmhekk, trid tentra numru li tagħtik is-sistema, jiġi ġġenerat l-OTP u jiġi ġġenerat code biex jiġi ffirmat it-tranżazzjoni.

Ngħid li ġeneralment il-Bank, meta jċempillek jitlob għall-aħħar tranżazzjoni li tkun għamilt, li jkollok aċċess għaliha biss.

Mistoqsi mill-Arbitru jekk hux qed ngħid li n-numru, il-kodiċi li minnu ġie awtorizzat il-pagament kien a conoscenza biss tal-Ilmentatriċi li kien fuq

il-mobile tagħha, u li ġaladarba dan ġie a conoscenza tal-iscammer, b'xi mod, l-Ilmentatriċi kkomunikatu lill-iscammer, ngħid iva, eżatt."[41]

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head Transaction Monitoring and Proactive Analysis* tal-BOV, li kkonferma bil-ġurament l-*affidavit* tiegħu.[42] Fl-*affidavit* spjega li s-sistema ta' monitoraġġ tat-tranżazzjonijiet tal-Bank hija bbażata fuq ir-*Risk-Based Approach* u li tranżazzjonijiet ma jiġux imwaqqfa, miċħuda jew soġġetti għal investigazzjoni addizzjonali fin-nuqqas ta' indikazzjonijiet jew fatturi ta' riskju li jiġġustifikaw tali intervent.[43]

Mistoqsi mill-Ilmentatriċi, ix-xhud qal:

"Qed niġi riferut mill-Ilmentatriċi għall-istatement tiegħi, fejn jissemma r-risk-based approach. Mistoqsi jekk, peress li ma kienx hemm tranżazzjonijiet iktar minn dak l-account, ta' dak l-ammont jew kważi lanqas kien hemm tranżazzjonijiet minn dak l-account li ħarġu l-flus, il-Bank ma identifikax li din kienet xi ħaġa mhux normali, ngħid li fis-7 ta' Ottubru 2025 l-Ilmentatriċi bagħtet €5,000 lil MeDirect Bank, suppost f'kont tagħha stess. Jiġifieri din it-tranżazzjoni li l-Ilmentatriċi qed tgħid li kienet frawdolenti kienet tal-istess ammont u kienet sejra wkoll lejn istituzzjoni finanzjarja Maltija. Jiġifieri kienet taqa' within your same profile.

Mistoqsi dan meta kien, ngħid 7th October 2025.

L-Arbitru jirreferi għall-istatement u jgħid li 2nd October. Ngħid li hemm waħda żgur 7th October 2025.

L-Arbitru jirreferi għal tranżazzjoni msemmija fl-istatement li hija 2nd October ta' €5,000 li tgħid '24/7 transfer between own accounts MeDirect'. L-Ilmentatriċi tikkonferma li din id-data tidher fil-kont tagħha.

Ngħid li fir-rapport tiegħi fis-2nd October qiegħda mniżżla.

[41] P. 143 - 144

[42] P. 145

[43] Affidavit ta' Keith Vella, p. 137 - 139

L-Arbitru jgħid li peress li mhux qed tidher imniżżla fl-istatement, probabbilment hemm xi żball fir-rapport tas-Sur Vella. Iżda l-argument mhuwiex fuq id-data.

Ngħid li, saritx fis-2nd jew 7th, still... it-transaction telqet mill-Bank tagħna u marret ġo kont ieħor ġo financial institution Maltija tal-istess ammont €5,000. Jiġifieri qed ngħidu qisu xahrejn, tlieta xhur qabel it-transaction allegatament frawdolenti.

L-Ilmentatriċi tgħid li din kienet transaction waħda minn numru ta' transactions li ġeneralment ikunu dejjem qed jidħlu fil-kont u mhux joħorġu mill-kont.

L-Arbitru jgħid li x-xhud wieġeb din il-mistoqsija.

Ngħid ukoll li qabel dik it-transaction allegatament frawdolenti fin-19th January, ftit ħin qabel, mill-kont tal-Ilmentatriċi seħħet transaction oħra tal-istess ammont li kienet indirizzata lejn istituzzjoni finanzjarja l-Irlanda. Il-Bank hemmhekk waqqafha u rriġettaha mal-ewwel. Imbagħad, konsegwentament, saret din it-transaction allegatament frawdolenti lil Moneybase ġewwa Malta. Ngħid li dan juri kemm taħdem tajjeb ir-risk-based approach; l-Ilmentatriċi, għal ċertu tali żmien qabel din it-transaction ma kinitx qed 'titransactja' jew tibgħat flus ġo kontijiet barra minn Malta. Hemmhekk, is-sistema ndunat li seta' kien hemm xi ħaġa ħażina b'dik it-transaction, waqqfitha u rriġettatha.

L-Arbitru jinnota li din mhijiex imniżżla fl-istatement. Ngħid li hemmhekk mhijiex ser tidher għaliex la t-transaction ma tkunx għaddiet ma tkunx ħarġet mill-kont.

L-Arbitru jinnota iżda li lanqas fir-risposta tal-Fornitur tas-Servizz ma ġiet rapportata din. Dr Theuma tgħid li qed jixhed issa s-Sur Vella.

Mistoqsi mill-Ilmentatriċi, jekk il-Bank waqqaf l-ewwel transaction ta' €5,000 ġo bank ġewwa l-Irlanda, għala t-tieni tranżazzjoni ma twaqqfitx ukoll la kienet eżatt warajha, ngħid li għax kienet within your profile. Ma kien hemm xejn ħażin fiha. L-ewwel waħda twaqqfet għax kienet not within your profile.

> ***Mistoqsi għalfejn, la kienu tal-istess ammont, u kienet reġgħet follow-up qisha tal-ewwel waħda, ma kienx hemm forsi telefonata biex il-Bank jaċċerta, kif ġieli jsiru, li din it-tranżazzjoni qed tiġi awtorizzata mill-persuna li qed tagħmel it-tranżazzjoni, ngħid għaliex it-transaction monitoring ma ħassitx li għandha twaqqafhom. Allura, it-transaction baqgħet għaddejja u ma kienx hemm għalfejn ikun hemm kuntatt mal-klijent f'dak il-ħin."***[44]

Qal ukoll:

> ***"Mistoqsi għalfejn ma ġiex revedut dak il-limitu ta' 5k jekk it-transactions kienu jaqgħu kollha taħt il-limit tal-5k, ngħid li ma nkunux qed nobdu r-risk-based approach li aħna obbligati li nimxu miegħu skont il-liġijiet Maltin u anke internazzjonali. Ma nistgħux inwaqqfu kull transaction li tkun taħt il-5,000; nifqgħu s-sistemi tal-Bank u plus li l-customer experience, l-operations tagħna tal-Bank, jiġifieri impossibbli twaqqaf kull transaction ta' kull klijent under 5,000, skont ir-risk-based approach. Impossibbli."***[45]

Xehed ukoll Luke Cutajar, *Senior Coordinator* fid-Dipartiment tal-*Payments Investigations* tal-BOV, li kien inkarigat mir-*recall* tal-pagament. Qal li l-Bank irċieva t-talba għar-*recall* fil-21 ta' Jannar 2026 fil-ħin ta' 09:40 u bagħat *camt.056* erba' minuti wara, flimkien ma' messaġġ *SWIFT* u *email* lill-bank benefiċjarju. Wara diversi *reminders*, fil-5 ta' Frar 2026, il-bank benefiċjarju informah li ma kienx fadal flus fil-kont tal-benefiċjarju.[46]

Nota tal-Fornitur tas-Servizz u Doc. G

Fit-22 ta' Settembru 2026, il-Bank ippreżenta nota ta' kjarifika flimkien ma' *statement* ta' kont ieħor tal-Ilmentatriċi, immarkat bħala Doc. G.[47] Fin-nota, il-Bank qal:

> *"1. Illi waqt is-seduta tad-9 ta' Settembru 2026, is-Sur Keith Vella xehed li fis-7 t' Ottubru 2025 l-Ilmentatriċi kienet bagħtet €5,000 lil MeDirect Bank*

[44] P. 145 - 146
[45] P. 147
[46] *Affidavit* ta' Luke Cutajar, p. 140 – 141
[47] P. 149 - 154

f'kont tagħha stess u spjega li, għaldaqstant, it-tranżazzjoni kkontestata kienet taqa' fil-profil tagħha. F'dan ir-rigward, L-Onor. Arbitru rrefera għal "Doc. F" li kien ippreżenta l-Bank u osserva li l-istatement kien juri tranżazzjoni ta' €5,000 datata t-2 t' Ottubru 2025;

2. Illi ai fini ta' kjarifika, il-Bank qiegħed jippreżenta statement ta' kont ieħor li jappartjeni lill-Ilmentatriċi li jispiċċa bin-numri 2981[48]*, hawn anness u mmarkat bħala* ***"Doc. G"****;*

3. Illi "Doc. F" juri t-trasferiment ta' €5,000 li sar fit-2 ta' Ottubru 2025 mill-kont tal-Ilmentatriċi li jispiċċa bin-numri 6944 għall-kont tagħha li jispiċċa bin-numri 5981. "Doc. G" juri kemm il-kreditu ta' dan l-istess ammont fil-kont li jispiċċa bin-numri 5981 fit-2 ta' Ottubru 2025, kif ukoll it-tranżazzjoni separata ta' €5,000 li saret fis-7 ta' Ottubru 2025 mill-istess kont."[49]

Fl-24 ta' Settembru 2026, l-Ilmentatriċi oġġezzjonat għall-preżentata ta' Doc. G u qalet:

"Nixtieq nirrimarka li, skont il-verbal tas-smigħ ta' l-ewwel seduta, l-Arbitru talab lill-Bank sabiex jippreżentalu kopja tal-istatement tal-kont minn fejn sar il-pagament, li tkopri t-tnax-il xahar qabel ma seħħet il-frodi. Dan il-kont jispiċċa bin-numri 6994[50] *u ġie ppreżentat lill-Arbitru mill-Bank bħala 'Doc F'. F''Doc F' tidher tranżazzjoni ta' €5,000 datata 2 ta' Ottubru 2025.*

Il-Bank ippreżenta nota u 'Doc G' wara t-tieni seduta. Kif ġie stipulat fin-nota tal-Bank, 'Doc G' jirreferi għal tranżazzjonijiet ta' kont bankarju ieħor. Għalkemm nifhem li 'Doc G' qed jiġi ppreżentat bħala kjarifika fir-rigward tax-xhieda tas-Sur Keith Vella, dan id-dokument jikkostitwixxi evidenza ġdida u, għaldaqstant, m'għandux jiġi kkunsidrat."[51]

L-Arbitru qed jiċħad din l-oġġezzjoni. Doc. G ma jikkostitwixxix evidenza ġdida iżda jsostni x-xhieda li s-Sur Keith Vella ta bil-ġurament waqt is-seduta tad-9 ta' Settembru 2026, meta xehed li fis-7 ta' Ottubru 2025, l-Ilmentatriċi bagħtet

[48] In-numru jispiċċa 5981 p. 151
[49] P. 150
[50] In-numru jispiċċa 6944
[51] P. 155

€5,000 lil MeDirect Bank f'kont tagħha stess.[52] Din ix-xhieda ngħatat fil-preżenza tal-Ilmentatriċi, li kellha l-opportunità tagħmel il-mistoqsijiet tagħha lix-xhud.

Il-Bank ippreżenta Doc. G għax, waqt dik is-seduta, l-Arbitru osserva li t-tranżazzjoni ta' €5,000 li tidher f'Doc. F kienet datata t-2 ta' Ottubru 2025 u mhux is-7 ta' Ottubru 2025.[53] Doc. G jikkjarifika din id-diskrepanza: it-trasferiment tat-2 ta' Ottubru 2025 sar bejn żewġ kontijiet tal-Ilmentatriċi, filwaqt li l-pagament tas-7 ta' Ottubru 2025 sar mill-kont l-ieħor tagħha li jispiċċa bin-numri 5981.[54] Barra minn hekk, Doc. G intbagħat ukoll lill-Ilmentatriċi fejn għamlet il-kummenti tagħha dwaru.[55]

Għaldaqstant, Doc. G qed jiġi aċċettat u kkunsidrat.

Sottomissjonijiet Finali

Fis-sottomissjonijiet finali, il-partijiet bażikament sostnew il-pożizzjoni tagħhom kif esibita fl-ilment, fir-risposta u fix-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 jippersonifika l-Bank u 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

[52] P. 145
[53] *Ibid*.
[54] P. 133; 151 - 152
[55] P. 149; 155

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 jemfasizza 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 jkun jidher li ġejjin mill-bank konċernat fuq il-mezz li normalment juża l-bank biex jibgħat messaġġi lill-klijenti.

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

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

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

Il-Qorti Ewropea tal-Ġustizzja (CJEU) fil-każ ta' *Wind Tre and Vodafone Italia*[56] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara każijiet fejn l-Ilmentaturi faċilment jaqgħu f'din il-kategorija.

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

Fuq kollox, il-PSD 2 tagħmilha ċara[57] 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/Ilmentatriċi. 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/Ilmentatriċi, jagħmel awtorizzazzjoni speċifika tal-pagament *a favur* tal-frodist.

Dan il-fatt huwa wkoll inkluż fil-mudell.

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

Il-mudell għandu wkoll għarfien dwar jekk l-Ilmentatriċi tkunx midħla tas-sistemi ta' pagamenti *online* mal-Bank billi tkun għamlet 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.[58] [59]

Deċiżjoni

L-Arbitru jiddeċiedi skont kif provdut f'Artikolu 19(3)(b) tal-Kap. 555 tal-Liġijiet ta' Malta b'referenza għal dak li, fil-fehma tiegħu, ikun ġust, ekwu u raġonevoli fiċ-ċirkostanzi u merti sostantivi tal-każ.

[57] Article 64 of PSD 2

[58] (EU) 2018/389 tas-27 ta' Novembru 2017 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)

[59] PSD 2 UE 2015/2366 Artikolu 68(2).

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

	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	(50%)	50%
Żieda għax l-Ilmentatriċi kkoperat b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax tkun irċeviet 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-Ilmentatriċi għandha ġġorr 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-pagament ilmentat sar wara li l-Ilmentatriċi daħħlet il-*User ID* u l-*One-Time Password* fil-*website* frawdolenti u, waqt it-telefonata mal-frodista, daħħlet il-kodiċi fil-funzjoni tat-*Transaction Signing* tal-*BOV Mobile App*.

L-Ilmentatriċi stess ammettiet li:

> ***"Ngħid li at a certain point, daħħalt il-User ID u l-One-Time Password."***[60]

U wkoll:

> ***"Ngħid, iva, kien hemm żewġ numri fuq l-iscreen, u qaltli biex nidħol bit-Transaction Signing mill-App, u ddaħħal iż-żewġ codes. Naħseb Transaction 2 kienet. Ngħid li ma rċevejtx messaġġi."***[61]

Is-Sur Gatt ikkonferma li t-*token* ma nbidilx u li l-kodiċi li awtorizza l-pagament ġie ġġenerat mill-*mobile app* tal-Bank fuq il-*mobile* tal-Ilmentatriċi.[62]

In vista ta' din ix-xhieda u tal-fatt li din l-informazzjoni kienet biss fil-pussess tal-Ilmentatriċi u setgħet tiġi a konoxxenza tal-frodista biss jekk l-Ilmentatriċi żvelathomlha, l-Arbitru jikkonkludi li l-Ilmentatriċi kkoperat mal-frodista billi għaddiet kull informazzjoni li kienet meħtieġa biex jiġi approvat il-pagament ilmentat.

L-Ilmentatriċi kkonfermat li rċeviet it-twissija tal-Bank tat-22 ta' Ottubru 2025,[63] li ntbagħtet fit-tliet xhur ta' qabel il-frodi.[64] It-twissija tal-21 ta' Jannar 2026 intbagħtet wara l-frodi u għalhekk l-Arbitru mhux qed jieħu konjizzjoni tagħha.

Mill-i*statements* ippreżentati jirriżulta li fid-9 ta' Diċembru 2025, l-Ilmentatriċi għamlet pagament lil terzi mill-istess kont minn fejn sar il-pagament ilmentat, u li fis-7 ta' Ottubru 2025, għamlet pagament ta' €5,000 mill-kont l-ieħor tagħha lejn kont f'isimha ma' istituzzjoni finanzjarja Maltija oħra.[65] Għalhekk, l-Arbitru ma jarax li għandu jsir tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar.

[60] P. 126
[61] P. 128
[62] P. 143 - 144
[63] P. 130
[64] P. 52
[65] P. 133; 145; 150; 152

L-Arbitru jifhem li waqt it-telefonata konvinċenti mas-suppost rappreżentanta tal-Bank, l-Ilmentatriċi setgħet naqqset jew warrbet is-salvagwardji soliti għax mill-informazzjoni li bdiet tagħtiha dehret telefonata ġenwina.

Għalhekk l-Arbitru jħoss li f'dan il-każ hemm ċirkostanzi speċjali li jimmeritaw li l-Ilmentatriċi jitnaqqsilha l-piż ta' negliġenza grossolana b'doża ta' 40%[66], jiġifieri 20% aktar mill-20% normalment spjegati fil-mudell.

Dan huwa każ fejn:

1. Il-frodist mhux biss bagħat SMS qarrieq iżda sostna l-kredibbiltà tal-SMS permezz ta' telefonata konvinċenti minn persuna titkellem bil-Malti li tat informazzjoni li l-Bank biss seta' jkollu, fosthom in-numru tal-kont u l-indirizz tad-dar tal-Ilmentatriċi. It-telefonata waslet minn numru li jixbah ħafna lin-numru li minnu l-Ilmentatriċi kienet tirċievi SMS ġenwini mill-Bank.

   L-Arbitru jifhem li meta l-Ilmentatriċi ġiet iffaċċjata minn xi ħadd li jippersonifika 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.

2. L-Arbitru jara nuqqas da parti tal-BOV dwar *transaction monitoring* minkejja li din kienet tranżazzjoni unika fil-limitu ta' pagamenti akkordat ta' €5,000, lejn kont ma' istituzzjoni finanzjarja Maltija, u kienet tal-istess ammont tal-pagament li l-Ilmentatriċi għamlet fis-7 ta' Ottubru 2025.

   L-Arbitru jinnota li, skont ix-xhieda tas-Sur Vella, ftit qabel il-pagament ilmentat is-sistema tal-Bank waqqfet tentattiv ieħor ta' pagament ta' €5,000 lejn istituzzjoni finanzjarja fl-Irlanda għax ma kienx fil-profil tal-Ilmentatriċi.[67] Dan it-tentattiv ma ssemmiex fir-risposta tal-Bank, iżda l-*log* tal-*Internet Banking* juri żewġ awtorizzazzjonijiet ta' pagament, fil-ħin ta' 10:37:03 u fil-ħin ta' 10:39:33.[68]

[66]F'każijiet oħra fejn il-frodi saret permezz ta' *activation code* li bidel it-*token*, l-Arbitru żied id-doża ta' responsabbiltà fuq il-Bank b'30%, iżda f'dan il-każ ma kienx hemm bdil fit-*token*. Ara P. 143.
[67]P. 146
[68]P. 57

Meta f'affari ta' żewġ minuti, wara li jkun żamm pagament suspettuż, issir talba biex l-istess pagament isir lejn IBAN differenti, *it-transaction monitoring system* għandha tkun sensittiva biżżejjed biex tissuspetta li hemm xi ħaġa stramba biżżejjed biex il-pagament jinżamm sa ma jsir kuntatt mal-klijent. Il-Bank jaf, jew imissu jaf, kif il-frodisti jużaw aġenti magħrufa bħala *'mules'* differenti biex iduru mas-sistemi tal-banek.

Għalhekk il-mudell qed jiġi rivedut hekk:

	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	(50%)	50%
Żieda għax l-Ilmentatriċi kkoperat b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax tkun irċeviet 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-Ilmentatriċi hija intitolata għal kumpens ta' 40% tat-telf li sofriet mill-pagament frawdolenti li ġie ddebitat fil-kont tagħha mal-Bank.[69]

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' elfejn ewro (€2,000).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.65% fis-sena[70] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.

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 rnexxielhom jimblukkaw 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 possibbiltà 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-Ilmentatriċi.

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-

[69] 30% ta' €5,000

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

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