Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 136/2026

YS

('l-Ilmentatriċi')

vs

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

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

Seduta tas-06 ta' Novembru 2026

L-Arbitru,

Ra l-Ilment[1] datat 13 ta' Mejju 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi t-telf li sofriet meta sar pagament frawdolenti ta' €4,995 mill-kont tagħha mal-BOV.

Il-pagament sar fid-19 ta' Jannar 2026, fil-ħin ta' 15:11 favur (P...O...S…F…) 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 - 9 b'dokumentazzjoni addizzjonali minn p. 10 - 59

[2]P. 50; 77

- Il-frodist jirnexxielu jippenetra b'mod frawdolenti l-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' 15:05, irċeviet messaġġ fuq it-*thread* '*BOV Mobile'* li kien jgħid li n-numru +35679083647 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://bovportals.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-PIN. Fl-*email* tagħha tal-1 ta' Frar 2026, u fir-rapport tal-Pulizija, jingħad li daħħlet *one-time password*. Il-*website* uriet in-numri li minnhom kienet ser tirċievi telefonata biex tiġi assistita, fosthom, in-numru li minnu kienet tirċievi l-*alerts* tal-Bank.[5]

– Fil-ħin ta' 15:08 irċeviet telefonata min-numru 99180001, li huwa n-numru li minnu kienet tirċievi SMS mill-Bank. Il-frodista, mara li titkellem bil-Malti, ikkonfermatilha isimha, kunjomha, l-indirizz tad-dar u n-numru tal-karta tal-identità tagħha u qaltilha li kien qed isir tentattiv biex jittieħdu €4,995 mill-kont tagħha.[6]

– Il-frodista qaltilha li ser twaqqaf it-tranżazzjoni. Waqt it-telefonata, l-Ilmentatriċi reġgħet daħħlet il-PIN fil-*link* u wara t-telefonata, ma kellhiex aċċess għall-*BOV Mobile App*.[7]

– Il-pagament ta' €4,995 sar fil-ħin ta' 15:11 bis-sistema ta' *Instant Payments*. Fil-ħin ta' 18:17 tal-istess jum, l-Ilmentatriċi rċeviet SMS mill-Bank li l-pagament kien ġie pproċessat.[8]

– Ftit minuti wara t-telefonata, l-Ilmentatriċi ssuspettat li kienet frodi u fil-ħin ta' 16:01 ċemplet lill-*Customer Service Centre* tal-BOV. Il-Bank imblokka l-profil tagħha u l-*cards* u beda l-proċess tar-*recall*.[9]

– Il-Bank irċieva t-talba għar-*recall* fil-ħin ta' 16:12 u fil-ħin ta' 16:29 bagħat *camt.056* lill-bank benefiċjarju. Fl-istess jum, fil-ħin ta' 16:52, l-Ilmentatriċi għamlet rapport lill-pulizija.[10]

[4]P. 54
[5]P. 14; 46;
[6]P. *ibid*.
[7]P. 150; 153 - 154
[8]P. 52;
[9]P. 14 - 15; 72
[10]P. 146; 183

– Fil-21 ta' Jannar 2026, l-Ilmentatriċi rċeviet SMS ta' *Spot the Scam* mill-Bank.[11]

– Fis-6 ta' Frar 2026, il-Bank għalaq il-każ tar-*recall,* u fid-9 ta' Frar 2026, infurma lill-Ilmentatriċi li l-bank benefiċjarju kien irrifjuta r-*recall* għax ma kienx fadal flus.[12]

L-Ilment

L-Ilmentatriċi qed titlob kumpens ta' €4,995 għax skont hija:

> *"I was the target of a fraud attempt in which individuals contacted me using what appeared to be the bank's official communication number. During this interaction, the fraudsters demonstrated access to accurate and sensitive personal information, including my home address and details relating to recent updates made to my bank account. This level of accuracy raises serious concerns regarding how such information became accessible to third parties and calls into question the effectiveness of the bank's data protection and security systems.*
>
> *Despite the seriousness of the incident and the clear indication that fraudsters were impersonating the bank using its own communication channels, I do not believe that the situation was handled with the level of urgency and security response required. In particular, the fact that fraudsters were able to contact clients using the bank's number and provide correct personal details suggests a significant vulnerability. However, I did not receive sufficient reassurance, clear explanations, or evidence of strengthened security measures following my report.*
>
> *As a result of this incident, a total amount of €4,995 was taken from my account. Following this, I was offered a reimbursement that amounted to only a small portion of the total sum lost. In order to receive €999, I was required to sign an agreement stating that, should the fraudster return the stolen funds at any point in the future, the bank would reclaim the portion that had been reimbursed to me. I find this condition to be*

[11] P. 59

[12] P. 36; 147; 183

unreasonable and unfair, particularly given that I was the victim of fraud under circumstances that raise serious concerns about the bank's security procedures.

In addition to this, all of my savings are held with the bank, and I also pay a substantial amount to it through the interest on my home loan. As a result, I reasonably expect a high standard of security, protection, and customer care, which in this case I do not feel has been met.

Overall, this experience has caused significant stress and uncertainty, especially regarding the safety of my personal data and financial assets. The combination of inadequate responses, lack of clear explanations, and the conditions attached to the partial reimbursement has further contributed to a loss of confidence in the bank's ability to protect its customers."[13]

Tkompli tgħid:

"This case highlights a number of serious failings in the bank's duty of care, security response, and customer handling.

Firstly, I received an official alert warning about an ongoing scam only a few days after I had already fallen victim to it. This delay is unacceptable, particularly given that the scam was clearly already known to the bank at the time. A timely warning could have prevented the incident entirely.

Secondly, despite widespread media coverage regarding this fraud scheme — including reports of suspects identified and arrests made — the bank failed to confirm whether my case formed part of this same scam. In contrast, the police authorities have confirmed that I am indeed a victim of this ongoing scheme, which has reportedly been affecting individuals since 2024. The bank's inability or unwillingness to provide this clarity demonstrates a lack of transparency and coordination in handling a known and established fraud pattern.

Most concerning, however, is the financial outcome and the conditions imposed. From the total amount of €4,995 that was taken, I was

[13] P. 3

reimbursed only €999[14] — approximately 20% of the stolen funds. This is wholly disproportionate given the circumstances surrounding the fraud, particularly the use of the bank's own communication channels and the apparent compromise of sensitive personal data.

Furthermore, the requirement to sign an agreement stating that the bank would reclaim the reimbursed amount should the stolen funds be recovered in the future is deeply unreasonable. This effectively removes my right to my own money and shifts the burden of loss onto the victim, rather than reflecting accountability on the part of the institution."[15]

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

"I request a fair and proportionate resolution to this matter - the full amount which I was defrauded, €4995. While I understand that any compensation may need to follow the Arbiter's model, I expect a more equitable outcome reflecting the circumstances of this case, particularly as a loyal client who entrusts all my savings to the bank and contributes substantially through home loan interest.

I request a reassessment of the reimbursement provided, with a view to increasing it beyond the €999 offered, in proportion to the €4,995 lost.

Any settlement should be made without prejudice to future developments, including court decisions or recovery of funds from the fraudsters. In such cases, I expect full entitlement to any amounts recovered directly, without the bank reclaiming previously reimbursed sums. It is not acceptable for the victim to bear further financial disadvantage".[16]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[17] tagħhom ippreżentata fit-3 ta' Ġunju 2026, BOV qalu:

[14] Not clear if this was actually reimbursed or simply offered.
[15] P. 4 - 5
[16] P. 5
[17] P. 62 - 76 u dokumenti annessi P. 77 - 148

*"**II. The Bank's point of view***

5. *Whereas, according to the Bank's records*[18]*, the disputed transaction effected on the 19th January 2026 in the amount of €4,995 was duly authorised at 15:11:21 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;*

6. *Whereas Article 40(1) of Directive 1 of the Central Bank of Malta (which Directive is based on PSD2) provides that a payment transaction is to be regarded as authorised only where the payer has given consent to execute the transaction:*

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

In the present case, the Bank submits that such consent was duly given through the successful use of the Complainant's personalised security credentials within the Bank's secure channels;

7. *Whereas the Bank has implemented the safeguards required under PSD2 and the applicable regulatory framework, including Strong Customer Authentication (SCA), which requires authentication based on two or more independent elements, namely knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is), designed to protect the confidentiality of authentication data:*

> *"**'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*

[18] Doc. A

(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]*"*

8. *Whereas, in addition to SCA, the Respondent applies the principle of dynamic linking in accordance with Commission Delegated Regulation (EU) 2018/389, such that authentication is specifically linked to the amount of the transaction and the beneficiary;*

9. *Whereas the aforesaid Regulation provides that SCA may be exempted for transactions which are considered to present a low level of risk. Notwithstanding this, the Bank consistently applies SCA so as to ensure the highest level of security, even in circumstances where an exemption could otherwise apply. In the present case, the transaction was approved through SCA;*

10. *Whereas the payment was approved using the confidential details of the Complainant. The Bank had no control over the initiation of the transfer, which was affected without its intervention. Once the Bank receives legitimate instructions for a third-party payment through its secure and authenticated channels, it is obliged to execute them, it being reasonably expected that only the account holder has access to such confidential credentials. In the present case, the transaction was duly authorised following successful validation of the Complainant's credentials and without any indication of fraud at the time of processing;*

11. *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

[19]Article 4(30) of PSD2.

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

12. *Whereas the Bank further submits that the disputed transaction fell within the applicable daily and per-transaction limits*[24]*, wherein the maximum permitted for third party payments via personal internet banking is €5,000 per transaction and €5,000 per day. The payment in question, amounting to €4,995, was therefore within such parameters;*

13. *Whereas, without prejudice to the foregoing, even if the Complainant were to allege that the transaction was not authorised*

[20]Doc. B, Page 24.
[21]Doc. B, Page 25.
[22]Doc. B, Page 18.
[23]Doc. B, Pages 23 to 24.
[24]Doc. C (https://www.bov.com/bov-digital-banking-limits)

by her, the Bank is not thereby obliged to refund the same, in circumstances where the transaction was enabled through actions performed using her personalised security credentials. In this respect, the Bank refers to Article 45 of Directive 1 of the Central Bank of Malta, entitled ***'Obligations of the payment service user in relation to payment instruments and personalised security credentials'****, which provides:*

> *"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."*

14. *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".*

15. *Whereas the Bank rejects the Complainant's allegation that the Bank failed to provide adequate or timely warnings concerning spoofing and other forms of fraud, or that the risks associated with such scams were only brought to her attention after the incident in question. In her complaint, the Complainant expressly alleges that the scam alert message received from the Bank was sent two days after the disputed transaction and therefore, according to her, provided no preventative value. She further alleges that*

inconsistencies in the Bank's communications caused uncertainty as to what constituted legitimate contact from the Bank;

16. *Whereas these allegations are not borne out by the evidence. On the contrary, the Bank is in possession of evidence showing that, well before the events of 19th January 2026, the Complainant had been sent a series of fraud awareness SMS communications to her registered mobile number as part of the Bank's ongoing anti-fraud and customer awareness campaigns;*

17. *Whereas the following warnings were issued to the Complainant prior to the incident:*

    (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) *6th 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) *26th 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."*

18. *Whereas these warnings were not isolated or incidental. They were issued periodically over a prolonged period and conveyed a clear, repeated and consistent message: that customers should not click on links received by SMS, should not disclose personal or security credentials, and should not act upon unsolicited communications requesting sensitive information or urgent payment-related action;*

19. *Whereas the Bank further submits that, as a voluntary user of the Bank's internet banking and mobile banking services, the*

Complainant knew, or in any event ought reasonably to have known, that such services are accessed exclusively through the Bank's official website or through the authorised BOV Mobile Application, and not by means of hyperlinks received through SMS messages or through directions provided in unsolicited telephone calls;

20. *Whereas the Bank emphasises that it has never required the Complainant, nor any of its customers, to access internet or mobile banking services through hyperlinks sent by SMS, nor to disclose sensitive information following unsolicited telephone calls purporting to originate from the Bank. On the contrary, the Bank expressly informed the Complainant in writing that it may send informational SMS or email communications, but that it never requests passwords, full card details, CVV, PIN or one-time passwords by SMS or telephone, nor does it ask customers to click on links in order to "secure" their account. The Bank further clarified that its legitimate card-activation SMS process does not require disclosure of security credentials and cannot be equated with the type of fraudulent communication complained of by the Complainant;*

21. *Whereas this distinction is important, because the Complainant's own version of events is that she clicked on a link contained in a message which purported to originate from the Bank, was redirected to a website resembling the Bank's online banking platform, and thereafter received a telephone call from a person claiming to be a Bank representative, who purported to guide her in relation to an alleged unauthorised transaction;*

22. *Whereas in those circumstances, the very conduct on which the fraud depended, namely, following a link received by SMS, accessing a purported banking portal through that link, and engaging with an unsolicited caller claiming to act on the Bank's behalf, was conduct against which the Complainant had already been repeatedly and expressly warned;*

*23. Whereas the Bank further submits that the warnings referred to above formed part of an ongoing and sustained educational campaign which the Bank has been conducting over a number of years in order to raise customer awareness of fraud and scam-related risks. Besides direct SMS warnings, the Bank also disseminates anti-fraud information through public awareness initiatives and other communications intended to educate customers as to the nature of spoofing and similar scams. A comprehensive list of the relevant awareness material up to September 2025 is being produced as "**Doc. D**";*

24. Whereas moreover, the Bank notes that awareness of such risks is not confined to warnings issued by the Bank alone. Guidance of a similar nature has also been made available by public authorities and regulators concerned with the protection of consumers of financial services. Such guidance consistently stresses the importance of using only genuine banking channels, of avoiding access through unverified links, and of safeguarding passwords, verification codes and other confidential credentials. 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.*

25. Whereas in light of the above, the Bank submits that the risk of SMS spoofing, fraudulent hyperlinks and unsolicited calls purporting to originate from the Bank was neither novel nor unforeseeable at the time of the events in question. On the contrary, it had been repeatedly and clearly brought to the attention of the Complainant through direct warnings issued to her over an extended period prior to the incident;

26. Whereas accordingly, the Complainant's assertion that she was misled, inadequately warned, or left insufficiently protected by reason of any omission on the part of the Bank is unfounded and is contradicted by the evidence;

III. Chronology of events

27. Whereas on the 19th January 2026, the Complainant fell victim to a spoofing scam, following which the disputed payment in the amount of €4,995 was executed from her account at approximately 15:11. Shortly thereafter, at approximately 16:01, the Complainant contacted the Bank's Customer Service Centre (CSC) and reported that she had accessed a link received via SMS and had disclosed her banking credentials, including authentication details, as recorded in the Bank's call logs[25]. The Bank immediately took action by blocking the Complainant's 24x7 user profile and stopping her cards and, at that stage, it was confirmed that the disputed transaction had already been executed. An urgent request for cancellation and recall of funds was immediately initiated. On the same day, the Complainant contacted the Bank again at approximately 16:24 to enquire whether the payment had been cancelled and was informed that, given that this was a SEPA Instant payment, it had already been processed and could not be stopped[26]. Further to the Complainant's report, at approximately 16:12 onwards, the Bank's Payments Investigations Unit (PIU) formally received the recall request and proceeded to issue the necessary recall messages to the

[25]Call Recording 1.

[26]Call Recording 2.

beneficiary bank, including a fraud recall request through the appropriate channels. These actions were taken promptly following notification by the Complainant;

28. *Whereas on the 20th January 2026, the Complainant provided the Bank with a more detailed account of the incident, confirming that she had clicked on a link received via SMS, accessed a website resembling the Bank's platform and entered a one-time password, after which she received a follow-up call from an individual purporting to be a Bank representative*[27]*. The Complainant also submitted the relevant police report in support of the recall request, and the Bank continued to process the matter accordingly;*

29. *Whereas in the days that followed, the Bank continued to pursue the recall of funds*[28] *procedure, including sending reminders to the beneficiary bank and monitoring the status of the request. However, given that the transaction was affected by means of SEPA Instant payment, the funds were transmitted and made available almost immediately, thereby significantly reducing the possibility of recovery;*

30. *Whereas by early February 2026, the Bank was informed that no funds remained available, and the recall of funds could therefore not be successfully completed. The Complainant was informed accordingly."*[29]

Seduti

Fl-ewwel seduta tat-2 ta' Lulju 2026, l-Ilmentatriċi xehdet hekk:

"Il-każ beda fid-19 ta' Jannar 2026 fejn għall-ħabta tat-3.00 p.m. irċevejt telefonata bin-numru reġistrat kif jidħol is-soltu tal-BOV. Il-mobile tiegħi mqabbad mal-Google contacts, u meta jċempluli l-BOV, inkun naf li mill-BOV u, jiġifieri n-numru kien proprju tal-BOV.

[27]Doc. E
[28]Doc. F
[29]P. 64 - 73

Ngħid li rajt il-messaġġ u t-telefonata flimkien. L-ewwel daħal il-messaġġ imbagħad daħlet it-telefonata.

Fil-messaġġ ma kienx hemm li qed jippruvaw jittieħdu xi flus. Fil-messaġġ kien hemm miktub li ġie miżjud numru fl-account tiegħi. Dan in-numru li żdied kien scam għax kemm-il darba kelli bżonn nagħmel xi changes jew niftħu joint account, eċċ., kull darba kelli mmur il-bank biex niffirmaw.

Ngħid li t-telefonata daħlet wara li għafast il-link. Irċevejt dan il-messaġġ, għafast il-link u mbagħad daħlet it-telefonata.

Ngħid li għafast il-link għax ovvjament ħadt qatgħa għax is-soltu biex nagħmel xi changes fl-account tiegħi tal-bank kull darba kelli mmur hemmhekk.

Ma stajtx nifhem kif din ġrat barra min-normal tal-proċeduri tas-soltu biex iżżid u tagħmel changes.

Il-call imbagħad daħlet min-numru tal-bank wara li għafast il-link u x'ħin għafast il-link, qaltli biex nidħol fil-Mobile App imma jiena ma kellix aċċess biex nużaha. Meta ppruvajt nidħol fl-account tiegħi tal-Mobile App qisha ġiet iffriżata mill-ewwel.

F'din it-telefonata qaltli li qed jippruvaw jittieħdu €4995 mill-account tiegħi. F'mument ta' paniku staqsejtha jekk kinux qed jipprovaw jidħlu l-flus jew jittieħdu. U qaltli li qed jippruvaw jittieħdu u jien, billi moħħi mistrieħ li min-naħa tal-bank, tlabtha biex twaqqaf kollox u, through that, kif ippruvajt nidħol fil-Mobile App, nassumi li ħadet il-PIN minn hemmhekk, u ġiet confirmed it-transaction.

Qed ngħid li nassumi li ħadet il-PIN minn hemmhekk għax hi qaltli biex nidħol fil-Mobile Application. U jien biex nidħol irrid nagħmel l-erba' numri. Ngħid li jien ma daħħalt l-ebda code. Nassumi li l-code li ġie generated, l-iscammer kienet qed tarah ukoll. B'hekk imbagħad ma kellix aċċess aktar għall-mobile. Imma ma daħħaltx il-code li ġie generated b'dawk il-four codes jiena.

Jien qed nassumi li hi ħadet il-PIN tiegħi u bih iġġenerat il-code. Qed nassumi li hi ħadet il-PIN mill-App u mbagħad iġġenerat il-code mil-link li bagħtitli jew mingħand il-persuna li ntbagħtet.

Qed jingħad li mit-telefonati jiena ma ċħadtx li daħħalt l-informazzjoni kollha li talbitni.

Ngħid li l-PIN jiena stess daħħaltu, però, codes aktar minn hemmhekk, ma daħħaltx jiena.

Sadanittant, jien moħħi mistrieħ għax kienet call proprja bħal tal-bank, jiġifieri bl-affarijiet kollha li bdiet tgħidli u dettalji li tat lili fuq l-address tad-dar tiegħi, eċċ., li dik qajmet ftit concern kif kellha dawk id-dettalji tiegħi meta ma tajtx dettalji jiena. Kulma kellha n-number tiegħi u minn hemmhekk ikkonfermatli ismi, l-address tad-dar, eċċ."[30]

Fil-kontroeżami qalet:

"Nikkonferma li kont irċevejt SMS li allegatament qalli li ġie miżjud mobile number ġdid mal-kont tiegħi.

Nikkonferma li f'dak l-SMS kien hemm link.

Mistoqsija qabel ma għafast il-link ipprovajtx inċempel lill-bank fuq in-numru uffiċjali biex nivverifika jekk kienx ġenwin, ngħid li la ġie mit-thread tal-bank, jiena dak il-ħin kont għaddejja minn affarijiet personali li m'għandhomx x'jaqsmu, imma fil-panic tal-mument, għafast il-link għax rajt li kien mit-thread sħiħa ta' meta nagħmel il-withdrawals u, allura, moħħi qalli li ġie mill-bank.

Mistoqsija ġaladarba kelli riskju li kont ser niġi scammed darb'oħra, dan ma qajjimli l-ebda suspett, ngħid li billi kienu scams differenti ngħid li, le, għax din kienet ċemplitli mingħajr email, mingħajr messaġġ, eċċ., u tatni d-dettalji tagħha bħal kull call normali mill-bank u qaltli li ser tibgħatli Docusign biex niffirmah għax id-dettalji tiegħi kienu ilhom ma jiġu updated minn February 2023. X'ħin bagħtitli d-Docusign rajtu

[30] P. 149 - 150

suspettuż għax is-soltu ġejja u sejra l-bank anke sempliċiment biex niftaħ il-BOV App.

U għidt possibbli ser tagħmilli update tad-dettalji through Docusign? U rċevejt l-emails over fifty times u għidt mela scam.

Nikkonferma li dħalt fil-link tal-SMS li ntbagħat f'dan il-każ.

Ngħid li meta dħalt fil-link, il-webpage kienet proprja l-Internet Banking tal-BOV. Mistoqsija x'talbitni ndaħħal, ngħid il-PIN biex inkun nista' nidħol fl-account; il-User ID u l-PIN.

Mistoqsija jekk il-PIN kienx il-One-Time Password, ngħid li, le, ma kienx il-One-Time Password. Kien il-PIN li nidħol bih is-soltu (Hawn l-Ilmentatriċi qed turi fuq il-mobile tagħha fejn iddaħħal il-PIN).

U fil-pront, ċempel in-number.

Mistoqsija meta ċempluli xi staqsew minni, jekk talbunix nagħmel xi ħaġa, ngħid li erġajt daħħalt il-PIN f'din il-link.

Qed jingħad li jien għidt fl-ilment tiegħi li ġejt mitluba ndaħħal il-One-Time Password.

Ngħid li x'ħin dħalt fil-link, u daħħalt il-User ID u l-PIN, jista' jkun li ġie ġġenerat il-One-Time Password, però, ngħid il-verità, wara sitt xhur dak id-dettall ma nistax niftakru.

Qed jingħad li ser jistrieħu fuq l-ilment tiegħi fejn ngħid li daħħalt il-One-Time Password (paġna 14 tal-proċess).

Barra minn hekk, qaltli d-dettalji tiegħi: ismi, kunjomi, l-address u l-ID Card number, u qaltli li ser twaqqaf it-transaction. U jien għidtilha biex tagħlaqli l-card ukoll għax ovvjament kont mingħalija li qed nitkellem ma' xi ħadd mill-BOV.

U hi qaltli li ma kienx hemm għalfejn għax il-flus ittieħdu direttament mill-account. U għidtilha li jien nibża' ħafna u li aħjar tagħlaqli kollox. Nassumi li ma kellhiex dik il-faċilità li tagħlaqli l-card u l-card ma ingħalqitx ovvjament għax mhux min-naħa tal-bank.

Imma, other than that, ma ġejt mitluba nagħmel xejn iżjed.

Le, ma talbitni nagħmel xejn fuq il-Mobile App innifsu. L-unika ħaġa li qaltli kienet li ma kienx ser ikolli aċċess għall-Mobile App u li ridt immur il-BOV biex jerġgħu jiftħuhieli. Infatti, ma stajtx nidħol biex nara l-flus hux veru naqsu.

Ngħid li l-messaġġ irċevejtu filgħaxija li telqu €4,995 mill-account. U erġajt ċempilt lill-BOV biex nikkonferma li ma kinux €4,995 oħra.

Mistoqsija rċevejtx mill-bank, mill-BOV Mobile, matul din it-telefonata messaġġ b'xi kodiċi, ngħid, safejn naf jien, le.

Qed niġi referuta għal dak li għidt fix-xhieda tiegħi li meta dħalt fuq l-App kienet iffriżata. Ngħid li ma stajtx nużaha.

Mistoqsija meta ċemplitli kinitx diġà ffriżata, ngħid li jien kont mingħalija li qiegħda fl-App mil-link. Imma kif imbagħad qatgħet, u ppruvajt nidħol biex nara minn liema kont inqatgħu, ma stajtx nużaha l-App. Kienet qisha frozen, fis-sens li ma stajtx indaħħal PIN, ma stajt nagħmel xejn.

Mistoqsija kemm damet din it-telefonata, ngħid li ma damitx aktar minn five minutes. Rather, three minutes. Ma nafx. Sakemm jien kont qed nippanikja u ngħidilha biex tagħlaqli kollox għax nibża, dik l-iżjed ħaġa li damet għaddejja. Ngħid li matul dan il-proċess kollu jien ma kelli l-ebda suspett sakemm kont qed nitkellem mal-boyfriend għax l-affarijiet li bdiet tgħidli, proprju bħalma meta jkolli komunikazzjoni mal-bank, anke l-mod kif għalqet it-telefonata, tatni isimha, tatni kollox.

Qed niġi referuta għal lista ta' SMSs annessa mar-risposta tal-bank li l-bank bagħatli fuq il-mobile tiegħi bl-aħħar wieħed tat-22 October 2025 ta' Spot the Scam.

Mistoqsija nikkonferma jekk irċevejtx dawn il-messaġġi, ngħid li jien ippreżentajt log bħala parti mill-evidenza tiegħi. Ngħid li jien rajt li rċevejt messaġġ jumejn wara li ġrat l-iscam.

Mistoqsija rċevejtx il-messaġġi ta' qabel dan, ngħid li fuq il-mobile tiegħi ma sibthomx.

Qed jingħad li hemm lista ta' ħdax-il SMS.

Mistoqsija niftakarx irċevejtx wieħed minn dawn il-ħdax, ngħid mhux ser ngħid le, però, minn October sa January, qatt ma ħsibt li ser tiġri l-ħaġa.

Mistoqsija rċevejtx l-SMS t'Ottubru, ngħid, però, mhux qiegħed fil-logs tiegħi għax kieku kont insemmih. Ngħid li le, t'Ottubru ma nafx li rċevejtu.

Mistoqsija niftakarx jekk irċevejtx mill-bank SMS minn dawn il-ħdax, jgħidli biex noqgħod attenta, ngħid li fil-mobile tiegħi ma kellix allura ma nistax ngħid li rajtu. Mistoqsija niftakarx jekk irċevejtx dan it-tip ta' SMS, ngħid li, le.

Nikkonferma l-mobile number tiegħi li hu 79xxxx20.

Mistoqsija nikkonferma li l-bank jibgħatli SMSs oħra fuq dan in-numru meta, eżempju, nagħmel xi pagament, ngħid kif semmejt mill-istess thread li rċevejt l-iscam kont nirċievi withdrawal, xi ħadd sent you …

Nikkonferma li nirċievi SMSs mill-bank fuq il-mobile tiegħi irreġistrat.

Nikkonferma li nsegwi s-social media.

Qed jingħad li l-bank u banek oħra jwissu kontra dawn it-tipi ta' scams u l-BOV ilu għaddej bil-kampanja Spot the Scam.

Mistoqsija jekk ġielix rajt xi posts, xi videos fuq dan, ngħid li jiena nuża social media; Facebook ma tantx nużah, però, kemm-il darba wżajtu qatt ma telali post hekk. Qed jingħad li mhux fuq Facebook biss qiegħda ssir din il-kampanja imma anke fuq TV.

Ngħid li fuq billboard rajt, imma l-istess, xi ġimagħtejn wara li ġrat l-iscam jiena u nieżla minn Ħaż-Żebbuġ.

Ngħid li l-messaġġ daħal fl-istess thread tal-BOV. Il-frodisti ċempluli min-numru 9918 00001.

Qed jingħad mill-Arbitru, issa li kkonfermajt li stajt tajt il-kodiċi biex tidħol fil-kont tiegħi, minn hemm jien m'għamilt xejn iżjed.

Nikkonferma li m'għamilt xejn iżjed, le."[31]

Mistoqsija dwar SMS b'*activation code* li rċeviet fl-24 ta' Jannar 2026, qalet li dan kien wasal għax kellha tmur il-Bank biex terġa' jkollha aċċess għall-flus tagħha, u li ma kinitx irċeviet SMS bħal dan waqt li kienet għaddejja l-frodi.[32]

Fil-15 ta' Lulju 2026, il-Bank ippreżenta l-i*statement* tal-kont tal-Ilmentatriċi minn fejn sar il-pagament ilmentat, għall-perjodu mill-1 ta' Jannar 2025 sal-31 ta' Jannar 2026, hekk kif mitlub mill-Arbitru. Dan ġie mmarkat bħala Doc. G.[33]

Xhieda tal-Fornitur tas-Servizz

Fis- seduta tal-10 ta' Settembru 2026, il-Bank ressaq ix-xhieda ta' Keith Vella, *Deputy Money Laundering Reporting Officer* u *Head AFC Transaction Monitoring and Proactive Analysis* tal-BOV, li kkonferma bil-ġurament l-*affidavit* tiegħu.[34]

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.[35]

Waqt is-seduta qal:

"Ngħid li f'dan il-każ, fid-19 ta' Jannar 2026, mill-kont tal-klijenta ġiet executed tranżazzjoni ta' €4,995, lejn istituzzjoni finanzjarja oħra Maltija, il-Moneybase, ġewwa Malta stess.

Din hija istituzzjoni finanzjarja Maltija reputabbli, ġo pajjiż reputabbli li hu low risk, fejn ma kien hemm l-ebda restrizzjoni fuq il-pagament biex jiġi executed kemm min-naħa tar-remitter, li f'dan il-każ hija l-klijenta, u kemm min-naħa tal-beneficiary ma kien hemm l-ebda ħjiel li any of the parties jista' jkun involut f'financial crime jew xi azzjoni oħra illeġittima.

Ngħid li t-Transaction Monitoring System, jekk neħduh fl-ambitu ta' risk-based approach li l-bank japplika fis-sistemi tiegħu skont kif mitlub mill-

[31] P. 152 - 155
[32] P. 155
[33] P. 158 - 166
[34] P. 172 - 174; 180
[35] P. 172 - 173

FIAU u mil-liġijiet oħra internazzjonali jew minn standards oħra internazzjonali, dan il-pagament bl-ebda mod ma kien hemm red flags li dan kellu jitwaqqaf mis-sistemi tagħna."[36]

Fil-kontroeżami qal:

"Qed jingħad li l-Ilmentatriċi qatt ma għamlet pagamenti daqshekk kbar u banek oħra fejn għandha kontijiet magħhom normalment tirċievi telefonata jew tkun avżathom qabel li ser isir pagament kbir anke taħt il-€5,000.

Qed jingħad ukoll li l-Ilmentatriċi rċeviet notification mill-Mobile App li kien hemm transaction, 3 hours, 17 minutes wara.

Mistoqsi għalfejn in-notification waslet daqshekk tard jekk it-tranżazzjoni ma setgħetx titwaqqaf għax kienet meqjusa normali, ngħid li ma nistax nirrispondi fuq kif wasal il-messaġġ jiena.

Mistoqsi kif ma jitqajjimx suspett lill-bank li hemm pattern differenti meta l-Ilmentatriċi qatt m'għamlet tranżazzjonijiet daqshekk kbar fl-aħħar sena u anke qabel, ngħid li kif spjegajt, il-bank jutilizza r-risk-based approach, jieħu diversi fatturi in konsiderazzjoni: il-method of payment, l-ammont tal-payment, il-jurisdiction fejn saret it-transaction u diversi fatturi oħra in solidum biex naraw jekk it-transaction hijiex suspettuża jew le.

Ngħid li f'dan il-każ, it-transaction ma kienet bl-ebda mod suspettuża.

Ma jfissirx li għax ma tagħmilx transactions within the same band, jew viċin, bilfors it-transaction trid tieqaf. Jew inkella jekk qatt ma għamilt transaction lejn IBAN partikolari, bilfors transaction trid tieqaf. Jew inkella jekk qatt ma għamilt transaction lejn post jew istituzzjoni finanzjarja partikolari bilfors trid titwaqqaf. Il-bank jutilizza a risk-based approach.

Mistoqsi ġaladarba din l-iscam kienet ilha għaddejja 'l fuq minn sentejn, ma jkunx hemm concern li jkun hemm xi ħaġa ħażina ġaladarba l-IP

[36] P. 180

> ***address ma jkunx tal-klijenta, ngħid li jittieħdu diversi fatturi in consideration.***
>
> ***F'dan il-każ, is-sistema ma ħassitx li kellha bżonn twaqqaf dak il-pagament, dejjem on a risk-based approach."***[37]

Xehed ukoll Michael Gatt, *Senior Manager* fid-Dipartiment tal-*Electronic Payments* tal-BOV, li kkonferma bil-ġurament l-*affidavit* tiegħu.[38]

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 l-*Login ID*, l-*One-Time Password*, l-*Activation Code* jew kodiċijiet oħra ta' awtentikazzjoni permezz ta' SMS, *email* jew telefonata.[39]

Waqt is-seduta qal:

> ***"Ngħid li f'dan il-każ, il-pagament ġie awtorizzat bl-istess serial token number li intuża fil-passat mill-klijent. B'xi mod jew ieħor, konxjament jew inkonxjament, il-klijent għadda d-dettalji tat-Transaction Signing, jiġifieri l-code, lill-frodista u, mbagħad, ġie esegwit il-pagament.***
>
> ***Ngħid li forsi differenti minn każijiet oħrajn fejn il-frodista ħa over il-Mobile App tal-klijent.***
>
> ***Nikkonferma li biex sar dan il-pagament il-frodist kellu bżonn ċertu informazzjoni li jkollu biss il-klijent, Ms YS, f'dan il-każ. L-ewwel, l-informazzjoni biex tidħol fl-Internet Banking u, mbagħad, l-informazzjoni biex tawtorizza l-pagament speċifiku. Dan mhuwiex wieħed minn dawk li kien hemm Activation Code li biddlet it-token; dan baqa' bl-istess serial number.***

[37] P. 180 - 181

[38] P. 170 - 171; 181

[39] P. 170 - 171

> ***Nikkonferma li apparti li għafset il-link biex daħlet f'website frawdolenti, imbagħad riedet kodiċi li jiġi ġġenerat mit-token li mingħajr dak il-kodiċi ma setax jiġi awtorizzat il-pagament."***[40]

Fir-rieżami qal:

> ***"L-Ilmentatriċi stqarret li daħħlet il-User ID u l-PIN.***
>
> ***Mistoqsi x'jagħmlu l-User ID u l-PIN, ngħid li meta int qed iddaħħal biss il-Login ID u l-PIN, int għandek biss aċċess għall-Internet Banking. Hemmhekk qed tara l-kontijiet, qed tara t-tranżazzjonijiet, però, ma tistax tesegwixxi tranżazzjoni.***
>
> ***L-Ilmentatriċi stqarret ukoll li daħħlet il-One-Time Password.***
>
> ***Mistoqsi x'relevanza għandha l-One-Time Password, ngħid li l-One-Time Password biex tilloggja fl-Internet Banking, però, kif għidt qabel, biex inti tesegwixxi tranżazzjoni, trid tmur f'Payment to Third Parties u tagħti d-dettalji kollha, imbagħad, mhux il-One-Time Password, għandek is-Signature 2 u hemmhekk jiġi ġġenerat Challenge Code, iddaħħal dan il-code u ġaladarba ddaħħal dan il-code, jiġi esegwit il-pagament."***[41]

Fil-kontroeżami, ix-xhud ċaħad li l-frodista setgħet tieħu s-*Signatures* meta l-Ilmentatriċi daħħlet il-PIN biex tidħol fil-kont tagħha, għax dik hija informazzjoni li jafha l-klijent biss. Qal ukoll li l-Bank kien ser jiċċekkja jekk dak il-ħin kienx hemm xi problemi li għalihom l-*App* ma baqgħetx taħdem, iżda l-frodista ma kellha ebda aċċess biex twaqqaf l-*App* jew tibblokka l-kont tal-Ilmentatriċi.[42]

L-Arbitru rrefera għal Doc. A, li juri li l-proċess beda fil-ħin ta' 15:06 u l-pagament sar fil-ħin ta' 15:11.[43] Mistoqsi mill-Arbitru għalfejn in-notifika tal-pagament intbagħtet tliet sigħat wara, ix-xhud qal li jista' jkun li l-SMS intbagħat wara, iżda l-Bank xorta kien konformi mad-Direttiva PSD għax mhux obbligat jibgħat SMS.[44]

[40] P. 181
[41] P. 181 - 182
[42] P. 182
[43] *Ibid*.
[44] P. 182 - 183

Xehed ukoll Luke Cutajar, *Senior Coordinator* fid-Dipartiment tal-*Payments Investigations* tal-BOV, li kkonferma bil-ġurament l-*affidavit* tiegħu.[45]

Qal li l-Bank irċieva t-talba għar-*recall* fid-19 ta' Jannar 2026 fil-ħin ta' 16:12, bagħat *camt.056* fil-ħin ta' 16:29 u, ftit minuti wara, bagħat ukoll messaġġ *SWIFT* lill-bank benefiċjarju. Fi żmien anqas minn ġimagħtejn, il-Bank bagħat tliet *SWIFT reminders* u tliet *email reminders*. Fis-6 ta' Frar 2026 il-Bank għalaq il-każ. Ix-xhud qal ukoll li qatt ma rċevew risposta.[46]

Fil-kontroeżami kkonferma li l-IBAN tal-benefiċjarju u l-bank benefiċjarju kienu Maltin.[47]

Sottomissjonijiet Finali

L-Ilmentatriċi ma ppreżentatx nota ta' sottomissjonijiet finali, kif kellha dritt.[48]

Il-Fornitur tas-Servizz ippreżenta n-nota tiegħu fid-19 ta' Ottubru 2026, fejn bażikament sostna l-pożizzjoni tiegħu kif esibita fir-risposta u fix-xhieda waqt is-seduti. Il-Bank issottometta li l-kondotta tal-Ilmentatriċi tammonta għal *gross negligence* u talab li l-ilment jiġi miċħud fl-intier tiegħu.[49]

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.

[45] P. 175 - 176; 183
[46] P. 183
[47] P. 184
[48] P. 184 - 186
[49] P. 187 - 196

Analiżi u konsiderazzjoni

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

Għal dan il-għan, l-Arbitru qed jannetti ma' din id-deċiżjoni mudell li ppubblika u li ser jiġi 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*[50] 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.

Fuq kollox, il-PSD 2 tagħmilha ċara[51] 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.[52][53]

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.

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

[51] Article 64 of PSD 2

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

[53] 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	(20%)	20%
TOTAL FINALI	**(40%)**	**(60%)**

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 60% tal-piż u l-40% 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-PIN fil-*website* frawdolenti u, waqt it-telefonata mal-frodista, reġgħet daħħlet il-PIN fl-istess *link*.

L-Ilmentatriċi stess ammettiet li:

"Ngħid li meta dħalt fil-link, il-webpage kienet proprja l-Internet Banking tal-BOV. Mistoqsija x'talbitni ndaħħal, ngħid il-PIN biex inkun nista' nidħol fl-account; il-User ID u l-PIN."[54]

U wkoll:

"Mistoqsija meta ċempluli xi staqsew minni, jekk talbunix nagħmel xi ħaġa, ngħid li erġajt daħħalt il-PIN f'din il-link."[55]

Fl-*email* tagħha tal-1 ta' Frar 2026 lill-Bank, l-Ilmentatriċi kitbet:

"I was prompted to enter a one-time password, supposedly so that BOV could contact me with guidance to stop the unauthorised activity."[56]

Fis-seduta qalet li ma tiftakarx dan id-dettall:

"Ngħid li x'ħin dħalt fil-link, u daħħalt il-User ID u l-PIN, jista' jkun li ġie ġġenerat il-One-Time Password, però, ngħid il-verità, wara sitt xhur dak id-dettall ma nistax niftakru."[57]

L-Ilmentatriċi ċaħdet li daħħlet xi kodiċi apparti l-PIN u qalet li tassumi li l-frodista ħadet il-PIN u bih iġġenerat il-kodiċi.[58]

Iżda s-Sur Gatt ikkonferma li l-pagament ġie awtorizzat bl-istess *serial token number* li kienet tuża l-Ilmentatriċi, li t-*token* ma nbidilx, u li l-pagament ma setax

[54] P. 152 - 153
[55] P. 153
[56] P. 14
[57] P. 153
[58] P. 150

jiġi awtorizzat mingħajr kodiċi ġġenerat mit-*token*.[59] Ċaħad ukoll li l-frodista setgħet tieħu s-*Signatures* meta l-Ilmentatriċi daħħlet il-PIN.[60]

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-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 ċirkostanza speċjali li timmerita li l-Ilmentatriċi jitnaqqsilha l-piż ta' negliġenza grossolana b'doża ta' 30%[61], jiġifieri 10% aktar mill-20% normalment spjegati fil-mudell.

Dan huwa każ fejn 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, l-isem, il-kunjom, l-indirizz tad-dar u n-numru tal-karta tal-identità tal-Ilmentatriċi. It-telefonata dehret li waslet mill-istess numru li minnu l-Ilmentatriċi kienet tirċievi SMS ġenwini mill-Bank.[62]

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.

Il-Bank ippreżenta lista ta' ħdax-il twissija li bagħat lill-Ilmentatriċi permezz ta' SMS, l-aħħar waħda fit-22 ta' Ottubru 2025, jiġifieri fit-tliet xhur ta' qabel il-frodi.[63]

[59]P. 181

[60]P. 182

[61]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'20%, iżda f'dan il-każ ma kienx hemm bdil fit-*token*. Ara p. 181.

[62]P. 46; 52; 149; 153

[63]P. 68 - 70

L-Ilmentatriċi qalet li ma sabitx dawn it-twissijiet fuq il-*mobile* tagħha u li ma tafx li rċeviet dik tat-22 ta' Ottubru 2025. Iżda kkonfermat in-numru tal-*mobile* tagħha u li fuqu tirċievi SMS mill-Bank.[64]

Għalhekk, l-Arbitru huwa sodisfatt li t-twissija tat-22 ta' Ottubru 2025 intbagħtet fuq in-numru irreġistrat tal-Ilmentatriċi fit-tliet xhur ta' qabel il-frodi. It-twissija tal-21 ta' Jannar 2026, intbagħtet wara l-frodi u, għalhekk, l-Arbitru mhux qed jieħu konjizzjoni tagħha.[65]

Mill-i*statement* ippreżentat (Doc. G) jirriżulta li fit-12-il xahar ta' qabel il-frodi, l-Ilmentatriċi ma għamlitx pagamenti lil terzi mill-kont minn fejn sar il-pagament ilmentat. Għalhekk, skont il mudell, dan inaqqas il-ħtija tal-Ilmentatrici b'20%.

L-Arbitru ma jsib ebda nuqqas da parti tal-BOV dwar *transaction monitoring* peress li din kienet tranżazzjoni unika fil-limitu ta' pagamenti akkordat ta' €5,000, lejn kont ma' istituzzjoni finanzjarja Maltija.[66]

[64] P. 154
[65] P. 59
[66] P. 180 - 181

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	(30%)	30%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(20%)	20%
TOTAL FINALI	**(50%)**	**(50%)**

B'kollox, għalhekk, l-Ilmentatriċi hija intitolata għal kumpens ta' 50% tat-telf li sofriet mill-pagament frawdolenti li ġie ddebitat fil-kont tagħha mal-Bank.[67]

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, erba' mija u sebgħa u disgħin ewro u ħamsin ċenteżmu (€2,497.50).

[67] 50% ta' €4,995

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.65% fis-sena[68] 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 50% għall-BOV u 50% 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-data tan-notifika ta' dik l-interpretazzjoni jew il-kjarifika jew il-korrezzjoni hekk kif provdut taħt l-artikolu 27(3) tal-Att.

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

Kull talba għal kjarifika tal-kumpens jew talba għall-korrezzjoni ta' xi żbalji fil-komputazzjoni jew klerikali jew żbalji tipografiċi jew żbalji simili mitluba skont l-artikolu 26(4) tal-Att, għandhom isiru lill-Arbitru, b'notifika lill-parti l-oħra, fi żmien ħmistax (15)-il ġurnata min-notifika tad-Deċiżjoni skont l-artikolu msemmi.

Skont il-prattika stabbilita, id-Deċiżjoni tal-Arbitru tkun tidher fis-sit elettroniku tal-Uffiċċju tal-Arbitru għas-Servizzi Finanzjarji. Dettalji personali tal-Ilmentatriċi/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.