Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 126/2026

AR

('l-Ilmentatur')

vs

Bank of Valletta p.l.c.

(C 2833)

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

Seduta 30 ta' Ottubru 2026

L-Arbitru,

Ra l-Ilment[1] datat 06 Mejju 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi t-telf li sofra meta sar pagament frawdolenti ta' €1,900 mill-kont tiegħu mal-BOV.

Il-pagament sar fis-27 ta' Jannar 2026 fil-ħin ta' 13:18 favur 'Adam mc daid' f'kont ma' bank fl-Irlanda.

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 - 8 b'dokumentazzjoni addizzjonali minn P. 9 - 28.

- 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[2] maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-bank ma jibgħatx *links* fil-messaġġi tiegħu, u li l-klijent għandu jikkomunika mal-bank biss tramite l-App u/jew il-*website* uffiċjali u dan permezz tal-kredenzjali li l-bank ikun ta lill-klijent, il-klijent b'nuqqas ta' attenzjoni jagħfas il-*link*.

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

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

- Fis-27 ta' Jannar 2026, fil-ħin ta' 12:41, irċieva messaġġ javżah li n-numru 79020447 kien ġie miżjud.[3] Dan daħal fuq il-kanal ta' SMS fejn normalment jirċievi notifiki mill-Bank.

[2] L-Uffiċċju tal-Arbitru wkoll ħareġ twissijiet – ara: https://www.youtube.com/watch?v=3podDv2R_Jc&t=3s
[3] P. 27

- Wara li ra l-messaġġ frawdolenti, għafas fuq il-*link* tal-messaġġ, daħal ġo *website* li dehret li kienet tal-BOV u daħħal il-kredenzjali kunfidenzjali li bihom kien jaċċessa l-*internet banking.* Il-*website* infurmatu li xi ħadd mill-Bank kien ser iċempillu fuq wieħed minn żewġ numri indikati biex jgħinuh.

- Fil-ħin ta' 13:14, ċemplitlu persuna fuq numru 99676134 u f'konverżazzjoni li damet sitt minuti,[4] infurmatu li kien hemm pagament ta' €1,900 fis-sistema u staqsietu jekk kienx hu li għamlu. Fil-fatt, fil-ħin ta' 13:19, irċieva notifika b'SMS li l-pagament kien sar[5].

- Billi baqa' suspettuża, ċempel il-*fraud section* tal-Bank[6] fejn ġie infurmat li kien vittma ta' *scam* u bblokkjawlu l-*internet banking* u l-*cards* u talbuh imur jagħmel rapport lill-pulizija.

- Ir-rapport l-għassa sar fil-ħin 15:31[7].

- Il-proċess ta' *recall* min-naħa tal-BOV beda fil-ħin ta' 14:13, il-messaġġ lill-Bank Irlandiż sar fil-ħin 14:22, iżda dan ir-*recall* ma rnexxiex għax fis-6 ta' Frar 2026, ġew infurmati li ma kienx hemm flus fil-kont tal-benefiċjarju[8].

- BOV infurmawh li skont il-mudell tal-Arbitru setgħu joffrulu kumpens ta' 20% li jfisser ammont ta' €380.

- Din l-offerta ma ġietx aċċettata u nfetaħ dan l-ilment mal-Uffiċċju tal-Arbitru fejn qed jitlob kumpens sħiħ ta' €1,900 jew offerta aħjar li tirrappreżenta b'mod aktar ekwu kif għandu jinġarr il-piż tal-frodi.

L-Ilmentatur isostni t-talba tiegħu billi jgħid:

> *"I believe the bank has let me down by not providing sufficient protection against this type of fraud.*
>
> *The scam message appeared within an official BOV message thread, making it seem genuine. I was also contacted by someone impersonating*

[4] P. 28
[5] P. 26
[6] L-Arbitru sema' reġistrazzjoni ta' din it-telefonata. P. 110
[7] P. 12 - 14
[8] P. 145; p. 109

a bank employee who used my personal details, making the situation highly convincing.

In addition, the bank's systems failed to detect or stop an unusual and high-value transaction that was not typical of my account activity.

I did not knowingly authorise this payment, and it only occurred because I was misled into believing I was dealing with the bank."[9]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[10] tagħhom datata 25 ta' Mejju 2026, il-BOV qalu:

1. *'Whereas according to the Bank's records*[11]*, the transaction effected on the 27th January 2026 in the amount of €1,900 was duly authorised through the Complainant's Internet Banking channel within an active session in the Complainant's name, following a successful authentication step recorded at 13:18:05, whereby the system confirmed that "your instructions have been processed successfully." The transaction was initiated, processed, and completed through a continuous authenticated session, reflecting the use of valid credentials and authentication codes attributable to the Complainant. 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, including the use of credentials and mobile authentication codes, thereby ensuring that the transaction originated from authentication elements under the Complainant's control. At no point during the transaction flow did the Bank's systems register any anomaly or indicator of fraud, and the transaction accordingly bore all the hallmarks of a validly authenticated and authorised payment at the time of processing;*

2. *Whereas the Complainant's own evidence confirms that the payment was executed following the completion of the Bank's authentication steps. In*

[9] P. 3
[10] P. 32 – 41 u dokumenti annessi p. 42 - 109
[11] Doc. A

the police report, the Complainant admits: "I pressed the link" and "It requested my user ID and code and I entered the numbers"[12];

3. *Whereas the Complainant further confirms that the caller "was instructing [him] step by step in what codes to get from the BOV Mobile app" and that "after a few codes" the transfer "will be seen as processed"[13], while the complaint form similarly states that he was "misled [...] into providing security codes"[14]. These admissions confirm that the Complainant completed the authentication steps required to approve the transaction;*

4. *Whereas the above admissions are entirely consistent with the Bank's records[15], which show that the transaction was executed through the Complainant's Internet Banking sessions following the successful input of credentials and authentication codes. The sequence described by the Complainant, namely the entry of login details and the provision of codes generated via the BOV Mobile application, corresponds directly with the authentication event recorded by the Bank, thereby confirming that the transaction was carried out through a valid and completed authenticated journey;*

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 in the present case, such consent was manifested through the completion of the authentication process using the Complainant's personalised security credentials and authentication codes, as reflected in the Bank's records (Doc. A);*

[12] Page 12 of the Complaint.
[13] *Ibid.*
[14] Page 003 of the Complaint.
[15] Doc. A

7. Whereas the Bank has implemented robust security measures in line with the requirements of the Payment Services Directive 2 (PSD2), including the application of Strong Customer Authentication (SCA), which is defined as:

> *"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)** [...] designed in such a way as to protect the confidentiality of the authentication data[16]".*

8. 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;

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

10. Whereas in this case, the authentication process fulfilled the requirements of SCA, as it involved elements within the Complainant's exclusive control, namely the entry of login credentials and the provision of authentication codes generated via the BOV Mobile application;

11. Whereas the transaction was accordingly executed only after the successful completion of this authentication process, and the Bank had no control over the initiation or execution of the payment once valid instructions were received through its authenticated channels;

12. Whereas Article 45 of Directive 1 provides that:

> *"(1) The payment service user entitled to use a payment instrument shall: use the payment instrument in accordance with the terms*

[16] Article 4(30) of PSD2.

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

14. *Whereas in the present case, the Complainant's conduct directly enabled the execution of the transaction and therefore engages the liability provisions under Article 50;*

15. *Whereas in addition to the applicable regulatory framework, the relationship between the parties is governed by the Bank's terms and conditions*[17]*, which provide that:*

"All payments, Instructions [...] 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.[18]*"*

16. *Whereas the terms and conditions further provide that the customer shall bear responsibility for transactions carried out prior to notification to the Bank where the customer has failed to safeguard their credentials or has acted with gross negligence;*

17. *Whereas the above provisions reflect the fundamental principle that transactions authenticated through the Bank's secure channels using valid credentials are attributable to the account holder;*

[17] Doc. B
[18] Doc. B, Page 24.

18. *Whereas in this case, the transaction was executed following the successful use of the Complainant's credentials and authentication codes within his authenticated session, and therefore falls squarely within the scope of the above contractual provisions;*

19. *Whereas therefore the disputed transaction cannot be considered unauthorised within the meaning of the applicable regulatory and contractual framework, but rather constitutes a transaction carried out following valid authentication and consent provided through the Complainant's own actions.;*

20. *Whereas the Bank further submits that the disputed transaction fell within the daily and pre-transaction limits[19], 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 €1,900, was therefore within such parameters;*

21. *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;*

22. *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 him not to click links and not to disclose passwords, PINs, verification codes or online-banking credentials via SMS/email/phone:*

> *(i) 12th 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."*

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

(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) *24th 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) *23rd 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) *23rd 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) *3rd 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) 21st 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) 20th January 2026 – "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."

23. Whereas the above-mentioned 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 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'****.*

24. 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.

25. *Whereas despite all these warnings, the Complainant still carried out all the necessary actions which enabled the payment to be approved and therefore, he breached the terms and conditions and this against the above-mentioned article 45(1) of the Directive;*

26. *Whereas besides this, he also acted against article 45(2) of the Directive because he did not take all the reasonable steps to keep his bank transfer number safe. It is reasonably expected that a consumer is aware of the terms which regulate the contractual relationship by which they are bound and adhere to them;*

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

III. The Bank's Actions

28. *Whereas the Bank submits that it acted promptly and diligently upon being informed of the alleged fraud;*

29. *Whereas on the 27th January 2026 at 13:50[20], the Complainant contacted the Bank and informed it of the incident;*

30. *Whereas during this call, the Bank informed the Complainant that the activity in question was indicative of a scam and took all necessary precautionary measures to safeguard the Complainant's account, including the blocking of the Complainant's cards and Internet Banking access, in order to prevent any further unauthorised activity;*

31. *Whereas the Bank further initiated recovery measures without delay. In particular, a recall of funds[21] request was received on 27th January 2026 at 14:13, following which a SWIFT recall message (camt.056) was sent at*

[20] Call Recording 1
[21] Doc. E

14:22:23, and a further notification was issued to the beneficiary bank at 14:36:14, requesting the urgent return of the funds;

32. *Whereas the Bank continued to actively pursue the recovery of the funds, including responding to requests from the beneficiary bank and issuing multiple reminders through both SWIFT and email channels;*

33. *Whereas notwithstanding the Bank's prompt intervention and continued follow-up, it was ultimately confirmed on the 6th February 2026 that the funds did not remain in the beneficiary account and could therefore not be recovered;*

34. *Whereas the Bank duly informed the Complainant of this outcome and proceeded to close the case."*[22]

Seduti

Fl-ewwel seduta tal-10 ta' Ġunju 2026, l-Ilmentatur spjega kif ġraw l-affarijiet (kif spjegat aktar 'il fuq) u qal:

"In the meantime, kont qed nitkellem ma' ħabiba tiegħi li taħdem mal-BOV, u bdiet tinsisti li hija scam, però, jiena emmint li kienet il-vera. Ngħid li ma rajt l-ebda red flags. Però, ġieni suspett u dħalt fil-Facebook page tal-BOV u sibt post minn tagħhom ta' Spot the Scam. Kien hemm telephone number imniżżel u ddeċidejt li nċempel biex nivverifika li kollox sew.

Ngħid li dan kollu ġara fl-istess ġurnata; forsi xi għaxar minuti/kwarta wara t-telefonata.

Ċempilt u qbadt answering machine u qbadt ma' persuna li taħdem mal-BOV. Qaltli li taħdem il-BOV u għidtilha li rċevejt messaġġ u li ftaħt il-link u qaltli li kienet scam. Jien bqajt ninsisti biex nirrakkonta l-istorja għax sa dak il-ħin kont għadni qed nemmen li kienet vera.

X'ħin għidtilha mill-bidu sal-aħħar x'ġara, qaltli li din kienet kollha scam.

[22] P. 33 - 40

Qaltli li kellna nwaqqfu l-card, nagħlqu l-Mobile App u li l-ġurnata ta' wara nista' mmur il-branch ta' fejn ftaħt il-kont biex jerġgħu jiftħuli l-Mobile App u tiġi issued card oħra.

Ngħid li l-bank beda jagħmel tracing of funds biex jara fejn marru biex jiena nieħu refund. Il-proċess dam xi ftit u ġew lura b'risposta li huma m'għandhom l-ebda tort f'dan il-każ għaliex jiena tajt l-aċċess u offrewli refund ta' €380.

Jiena nixtieq nieħu l-full refund ta' €1,900 għaliex jiena kont vittma ta' impersonation scam. Jien qatt ma ħsibt li qed nagħti aċċess lil scammers.

Ngħid li mill-bidu sakemm bdejt nitkellem mal-impjegata proprja tal-BOV, emmint li tkellimt ma' impjegata oħra tal-BOV fejn kelli moħħi mistrieħ li ggwidatni fejn bqajt nemmen li r-refund kont ser nirċevih, mentri ma kienx hekk."[23]

Fil-kontroeżami qal:

"Nikkonferma li għafast fuq il-link.

Mistoqsi x'dettalji daħħalt fuq dan il-website li dħalt fih, ngħid li niftakar li talbuni code li jingħataw lill-klijenti tal-BOV once li jiftħu kont. Jidhirli li kien xi six-digit code. Il-User ID. Dan ma jinbidilx. Fil-fatt, ma kontx nafu bl-amment u kelli nfittex fil-karti li kienu tawni meta mort niftaħ il-kont.

Naħseb li dak; ma jidhirlix li daħħalt xi dettalji oħrajn.

Mistoqsi tajtx xi One-Time Password, ngħid li jista' jkun aktar 'il quddiem. Anke meta kont qed nitkellem ma' din it-tfajla fuq it-telefon, talbitni xi tnejn, tlieta.

Nikkonferma li t-telefonata ġiet min-numru 99676134.

Mistoqsi qattx il-bank ċempilli minn dan it-tip ta' numru, ngħid li, le, l-bank qatt ma ċempel minn dan it-tip ta' numru. U lanqas qatt ma kkomunikajt mal-bank bit-telefon minn dan it-tip ta' numru.

[23] P. 112 - 113

Mistoqsi kif allura ma ġinix suspett li xi ħadd qed iċempilli minn numru normali, ngħid li ġieni suspett imma assumejt li qed iċemplu min-naħa tal-BOV u jidhirli li dan in-numru kien imniżżel ukoll fuq il-web page li dħalt fuqha.

Ngħid li, le, qabel ma tajt id-dettalji personali tiegħi ma ċempilt l-ebda numru uffiċjali tal-bank.

Mistoqsi nispjega x'qaltli biex nagħmel din il-persuna li ċemplitli, ngħid li ċemplitli, qaltli li rċeviet ir-request tiegħi. Għidtilha dak kollu li ġara. Jidhirli li bdiet titlobni xi log in One-Time Passwords ukoll biex tkun tista' taċċessa xi affarijiet fejn imbagħad sabet li jien għamilt request ta' transfer ta' €1,900. Jiena għidtilha li ma għamilt l-ebda request. Qaltli li kellha tipproċessah biex imbagħad titlob għar-refund.

Mistoqsi talbitnix nidħol f'xi post fuq il-Mobile App li taqa' taħt il-kategorija ta' Signatures, ngħid li iva.

Mistoqsi dħaltx fi Transaction Signing, ngħid ma niftakarx eżatt, però, fejn jidħlu BOV Signatures, iva. Codes talbitni għal darbtejn, tlieta. Dwar Transaction Signing ma niftakarx.

Ngħid li dħalt fis-Signatures fejn iġġenerajt b'xi mod xi code u mbagħad ikkomunikajtulha. Ngħid li hi bdiet tgħidli, 'Agħfas dik il-buttuna,' u jiena pprovdejtilha l-code biex hi tkun tista' tmexxi.

Ngħid li matul il-konverżazzjoni ma kelli l-ebda suspett. Din it-tfajla kienet Maltija, bdiet tkellimni bil-Malti, ma kien hemm l-ebda delay, l-ebda tlaqliq. Kienet taf x'inhi tgħid, kienet qed tiggwidani bil-Mobile App, jiġifieri tatni x'nifhem li din il-persuna taħdem fuq dawn l-affarijiet.

Ngħid li matul il-konverżazzjoni, damet kemm damet, ma kelli l-ebda suspett.

Qed niġi referut għar-risposta tal-bank għall-ilment tiegħi fejn hemm lista ta' SMSs (paġni 37 u 38 tal-proċess) li l-bank bagħatli bħala warnings li jwissu kontra dawn it-tipi ta' scams.

Mistoqsi nikkontestax li rċevejt dawn il-messaġġi, ngħid li fil-passat kont nirċievi dawn il-messaġġi, però, ma kontx irċevejt qrib ta' dan l-inċident.

Mistoqsi rċevejtx dawn il-messaġġi (mit-12 ta' Novembru 2023 sal-20 ta' Jannar 2026), ngħid li jista' jkun hemm minnhom li ma jidħlux. Ommi wkoll klijenta tal-BOV u f'ċerti istanzi kienet tirċievi messaġġ hi u jien le jew bil-kontra. Jista' jkun li hemm xi messaġġi li jien ma rċevejtx.

Mistoqsi rċevejtx l-aħħar messaġġ qabel dan l-inċident, dak tal-20 ta' Jannar 2026, fuq in-numru 9918 0001, ngħid li le, fuq il-messaġġi tiegħi m'għandi xejn imniżżel.

Nikkonferma li għandi ħabiba li taħdem il-BOV.

Mistoqsi kellimthiex meta bdejt nara dawn l-affarijiet iseħħu, ngħid li iva, wara. Ngħid li meta rċevejt dan il-messaġġ, għidtilha li rċevejt link, però, dak il-ħin, kif għidtilkom, kont qed nistenna l-paga dieħla, kelli xi spejjeż u bdejt nippanikja.

Qed jingħad li jien għidt li kellimtha meta rċevejt din il-link. Ngħid li, iva.

Mistoqsi ħallejthiex tirrispondini, ngħid li, le.

Qed jingħad jiġifieri qbadt u għamilt fattija. Ngħid li, iva.

Mistoqsi qattx rajt fuq social media fuq Spot the Scam, li hawn dawn il-ħafna ta' scams jiġru, ngħid li, iva, rajt ħafna. Però, throughout, kemm il-messaġġi u kemm il-website bil-link li għafast, kemm it-telefonata, fl-ebda mument ma ġieni suspett li din setgħet kienet scam."[24]

Fuq talba tal-Arbitru, il-BOV bagħtu kopja tal-i*statement* tal-kont tal-Ilmentatur minn Jannar 2025 sa Jannar 2026. Dan juri li l-Ilmentatur kien għamel *internet payment* wieħed għal valur ta' €1,484.38 fis-26 ta' Marzu 2025[25].

Fit-tieni seduta li nżammet fl-10 ta' Settembru 2026, il-Bank ressaq ix-xhieda ta' Michael Gatt, espert fis-sistema tal-pagamenti elettroniċi tal-BOV[26]. Spjega kif f'għajnejn il-Bank, il-pagament ilmentat deher awtorizzat mill-Ilmentatur u dan skont ir-regoli Ewropej dwar pagamenti.

[24] P. 113 - 115
[25] P. 120
[26] P. 143 - 144

Spjega li f'dan il-każ jidher li l-Ilmentatur ikkopera mal-frodista billi daħħal il-kodiċi mitluba, li huwa biss kellu, biex seta' jsir *Instant Payment* permezz ta' *Signature 2* fil-*Mobile App.* Il-pagament sar bl-istess *token* li saru pagamenti simili permezz tal-*Mobile App*. Ma kien hemm l-ebda bdil tal-*App* minn *device* għal ieħor permezz ta' xi *Activation Code* kif rajna f'każi oħra t'ilmenti dwar frodi.

Ma sarx kontroeżami.

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head Transaction Monitoring Proactive Analysis fil-BOV*[27].

Huwa qal:

> ***"Ngħid li jien Deputy MLRO u Head tat-Transaction Monitoring Proactive Analysis, fil-BOV u nikkonferma bil-ġurament l-affidavit li ppreżentajt.***
>
> ***F'dan il-każ, din it-transaction ġiet executed fis-27 ta' Jannar 2026, ta' €1,900 mill-kont tal-klijent, l-Ilmentatur, għal ġo kont f'istituzzjoni finanzjarja ġo l-Irlanda, Permanent TSB PLC.***
>
> ***Ngħid li l-Irlanda hija meqjusa bħala pajjiż low risk.***
>
> ***Ngħid li meta l-pagament telaq mill-bank tagħna, u ġie ċċekkjat mill-Payment Screening, la l-istituzzjoni finanzjarja, la l-benefiċjarju li huwa Adam Mc Daid, u lanqas id-dettalji l-oħra li kienu inklużi fil-pagament ma ħabtu jew kien hemm xi match ma' xi adverse media jew ma' xi hit oħra li seta' kien hemm f'dawn il-listi msemmijin fl-affidavit.***
>
> ***Ngħid li l-ammont, bħala Transaction Monitoring, huwa modest ħafna, €1,900, u ta' min jgħid ukoll li l-klijent, fis-26 ta' Marzu 2025, biex nikkomparaw ukoll l-ammonti, kien għadda pagament lokali ta' €1,484.38, jiġifieri bħala ammonti huma bejn wieħed u ieħor viċin xulxin.***
>
> ***Ngħid li l-klijent qatt ma bagħat tranżazzjonijiet barra minn Malta qabel dan il-pagament, imma ma jfissirx li għax il-klijent qatt ma jkun bagħat pagament barra minn Malta, bilfors dan il-pagament irid jieqaf. Hemm diversi riskji li jittieħdu in konsiderazzjoni qabel ma pagament jitwaqqaf***

[27] P. 144 - 145

> ***kemm jekk ser isir għall-ewwel darba għal bank ġdid jew istituzzjoni finanzjarja ġdida u jekk anke ser jiġi trasferit lejn pajjiż barra minn Malta. U anke jekk ser jintbagħat aktar minn darba, jiġifieri hemm riskji li jittieħdu in solidum u mhux just għax klijent qatt m'għamel tranżazzjoni lejn pajjiż barra minn Malta bilfors dik it-tranżazzjoni trid tieqaf.[28]"***

Ma sarx kontroeżami.

Xehed ukoll Luke Cutajar li kien inkarigat mir-*recall* tal-pagamenti u qal li r-recall sar fil-pront iżda ma rnexxiex għax il-flus jidher li ngibdu mill-frodisti qabel ma wasal ir-*recall*.[29]

Ma sarx kontroeżami.

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 għandha tinqasam ir-responsabbiltà tal-frodi bejn il-bank konċernat u l-klijent

[28] P. 144 - 145
[29] P. 145

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*[30] 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.

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

Fuq kollox, il-PSD 2 tagħmilha ċara[31] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

Għalhekk, il-banek jeħtieġ li jkollhom sistema ta' pagamenti robusta biżżejjed biex il-pagament ma jsirx jekk ma jkunx speċifikament awtorizzat mill-klijent/Ilmentatur. Il-banek ma jistgħux ma jerfgħux responsabbilità jekk iħallu toqob fis-sistemi tagħhom li permezz tagħhom il-frodist ikun jista', bla ma jkun hemm aktar involviment tal-klijent/Ilmentatur, 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-Ilmentatur ikunx midħla tas-sistemi ta' pagamenti *online* mal-Bank billi jkun għamel xi pagament simili (ġenwin) fit-12-il xahar ta' qabel. Dan jgħin ukoll biex tiġi ffurmata opinjoni jekk il-*monitoring* tal-pagamenti li l-bank huwa doveruż jagħmel (kif spjegat fil-mudell) huwiex effettiv.[32] [33]

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.

[31] Article 64 of PSD 2
[32] (EU) 2018/389 tas-27 ta' Novembru 2017 RTS *supplement* ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[33] 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-Ilmentatur**
Ilmentatur li jkun wera traskuraġni grossolana	0%	(100%)
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	(50%)	50%
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	20%	(20%)
Sub-total	0%	(100%)
Tnaqqis għal ċirkostanzi speċjali	(20%)	20%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(20%)**	**(80%)**

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

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

F'dan il-każ partikolari, il-pagament ilmentat sar billi b'xi mod il-frodist(a) saret taf il-*USER ID,* il-*One-Time Password* u saħansitra l-kodiċi biex ġie approvat il-pagament ilmentat. L-Ilmentatur ma ċaħadx li huwa żvela dawn il-kodiċi sigrieti għax baqa' jemmen li l-frodista kienet rappreżentanta tal-BOV. Anke fit-telefonata reġistrata meta ċempel lill-BOV *fraud section,* għax beda jiġih dubju, huwa ammetta li kixef il-kodiċi sigrieti għax sa dak il-ħin kien għadu jemmen li t-telefonata kienet ma' rappreżentanta ġenwina li kienet qed tgħinu jwaqqaf u mhux jagħmel pagament frawdolenti.

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

Għalhekk l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jitnaqqaslu l-piż ta' negliġenza grossolana b'doża ta' 30%[34], jiġifieri 10% aktar mill-20% normalment spjegati fil-mudell.

Dan huwa każ fejn il-frodista mhux biss bagħtet SMS qarrieq iżda sostniet il-kredibbiltà tal-SMS permezz ta' telefonata konvinċenti minn persuna titkellem bil-Malti li tat informazzjoni li l-Bank biss seta' jkollu.

L-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat minn 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.

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 u l-Ilmentatur kien għamel pagament simili fix-xhur ta' qabel.

[34] 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*.

Għalhekk il-mudell qed jiġi rivedut hekk:

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatur**
Ilmentatur li jkun wera traskuraġni grossolana	0%	(100%)
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	(50%)	50%
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	20%	(20%)
Sub-total	0%	(100%)
Tnaqqis għal ċirkostanzi speċjali	(30%)	30%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(30%)**	**(70%)**

B'kollox, għalhekk, l-Ilmentatur huwa intitolat għal kumpens ta' 30% tat-telf li sofra mill-pagament frawdolenti li ġie ddebitat fil-kont tiegħu mal-Bank.[35]

[35] 30% ta' €1,900

Għaldaqstant, *ai termini* tal-Artikolu 26(3)(c)(iv) tal-Kap. 555 tal-Liġijiet ta' Malta, l-Arbitru qed jordna lil *Bank of Valletta p.l.c.* iħallas lill-Ilmentatur is-somma ta' ħames mija u sebgħin ewro (€570).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.65% fis-sena[36] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[37]

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 jimblokkaw xi fondi misruqa mill-frodisti u, għalhekk, eventwalment jista' jkun hemm xi rkupru minn dan is-sors.

Jekk jirriżulta rkupru bħal dan, biex ma jkunx hemm 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 30% għall-BOV u 70% għall-Ilmentatur.

_____

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-

[36] Ekwivalenti għall-'*Main Refinancing Operations (MRO) interest rate*' kurrenti stabbilita mill-Bank Ċentrali Ewropew.
[37] Fil-każ li din id-deċiżjoni tiġi appellata, u tali deċiżjoni tkun ikkonfermata fl-appell, l-imgħax pagabbli jiġi kkalkolat mid-data tad-deċiżjoni tal-Arbitru.

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

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

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