Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 082/2026

ZQ and UT

('l-Ilmentatur(i)')

vs

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

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

Seduta tal-25 t'Awwissu 2026

L-Arbitru,

Ra l-Ilment[1] datat 04 Marzu 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi t-telf li sofriet meta saru żewġ pagamenti frawdolenti mill-kont tagħha mal-BOV li b'kollox jammontaw għal €4,940 u spejjeż relatati ta' €26.

Fil-fatt, dawn il-pagamenti kollha saru nhar l-4 t'Awwissu 2025 kif spjegat fit-tabella:

Ħin	Ammont €	Referenza
15:16:40	500	p. 179; 212
15:17:55	4,440	p. 179; 212
TOTAL	**4,940**	

[1]Paġni (P.) 1 - 8 b'dokumentazzjoni addizzjonali minn p. 9 - 195.

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'.*

- 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*),

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

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:

- Fl-4 t'Awwissu 2025, fil-ħin 11:55, irċeviet dan il-messaġġ SMS fuq BOV Mobile *chat* fejn normalment jikkomunika magħha l-Bank:

  "We sent you a message. View & login https://ref29551bov.com 6603"[3]

- Billi emmnet li dan kien messaġġ ġenwin, għafset il-*link* u daħlet f'*site* li dehret identika għal tal-BOV u hemm tat kredenzjali sigrieti biex tidħol fis-*site* ta' *internet banking*.

- Kompliet issegwi l-istruzzjonijiet u daħlet fis-*Signature 1* fejn jidher li talbet *authentication code li l-Bank bagħtilha permezz ta' SMS fil-ħin ta' 15:12 li kien jgħid:*

  "Here is your activation code. Please use it within 1 hour to activate your BOV Mobile App:G98b8b10"[4]

- Jidher li dan ġie kkomunikat lill-frodist għax ftit minuti wara irċeviet notifiki permezz ta' SMS dwar il-pagamenti ilmentati kif spjegat fit-tabella hawn fuq.[5]

- Biex setgħu jsiru dawn il-pagamenti kien hemm trasferiment mill-*joint account* ta' €2,000 għal kont persunali tal-Ilmentatriċi u trasferiment ieħor ta' €600 mill-kont *savings* għall-kont kurrenti tagħha. Dan jispjega għaliex l-ilment sar miż-żewġ ilmentaturi għalkemm l-Ilmentatur spjega li hu ma kienx involvut fil-messaġġi li rċeviet biss l-Ilmentatriċi.

[3] P. 178
[4] *Ibid.*
[5] P. 179

- Kif indunat bil-frodi, irrapportat il-każ lill-Bank li beda proċess ta' *recall* fil-ħin ta' 15:33.[6] Il-Bank irċieva risposta mill-bank barrani fil-ħin ta' 16:45 fejn talbu kopja tar-rapport tal-pulizija li sar fil-ħin 18:37.[7]

- Ir-*recalls* ma rnexxewx għax il-bank barrani informa li "*we cannot withdraw the funds because our customer is unlocatable*."[8]

- Il-Bank offra rimbors ta' 50% skont il-mudell tal-Arbitru (dettalji aktar 'l isfel) iżda ma aċċettatx għax ippretendiet irkupru totali.

L-Ilment

L-Ilmentatriċi qed titlob kumpens totali ta' €4,966 li jinkludi €26 spejjeż tar-*recall* u ħruġ ta' *cards* ġodda. Hi spjegat:

> *"The Bank has let me down for the following reasons:*
>
> *1. Failure to adequately prevent or detect suspicious transactions*
>
> *The fraudulent transactions arose from a sophisticated impersonation scam whereby the SMS appeared within the Bank's official communication thread. This significantly reduced my ability to detect the fraud. Furthermore, the transactions in question (€500 and €4,440) were untypical of my normal account activity and, in my view, should have triggered enhanced transaction monitoring or intervention before the funds left my account.*
>
> *2. Insufficient weight given to material mitigating factors*
>
> *In assessing liability under the Arbiter's model, I believe the Bank did not appropriately weigh relevant circumstances, including:*
>
> *• my status as a new customer and the existence of an ongoing home loan application at the time, constituting a special circumstance; and*
>
> *• my immediate action in contacting the Bank, blocking my cards, and filing a police report on the same day.*

[6] P. 265
[7] P. 191
[8] P. 265

I would also like note that I was advised by the Bank's Customer Care team to file the police report on the following day. However, I proceeded to file it on the same day in order to act as swiftly as possible.

3. Timeliness of the Bank's response

Although I reported the incident immediately on 4 August 2025, I understand that the recall process was only initiated on the following day. Given the time-sensitive nature of such fraud recovery actions, I believe this may have been a factor as to why the recall process was unsuccessful.

4. Disproportionate allocation of responsibility

The Bank has concluded that I should bear 50% of the responsibility. I think that this allocation does not proportionately reflect the relative responsibilities of the parties (as noted in point 2 above).

5. Prolonged handling of the case

The incident occurred on 4 August 2025. Despite my immediate reporting and cooperation, several months elapsed before a settlement position was communicated. As a direct consequence of the fraudulent transactions, I was left with no available funds in my bank account for approximately one month, until my next salary was credited. This placed me in a financially difficult position."[9]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[10] tagħhom datata 24 Marzu 2026, il-BOV qalu:

"3. Whereas the Bank's records[11] *show that the disputed payments were duly authorised by (Complainant) on the 4th August 2025 at 15:16:40 and 15:17:55, following successful authentication through the Bank's secure digital banking channels. Both transactions were authorised using (Complainant's) personalised security credentials and were confirmed through Strong Customer Authentication ("SCA"), applied in accordance with the Bank's security framework and the requirements of Directive (EU)*

[9] P. 4
[10] P. 199 - 210 u dokumenti annessi p. 211 - 256
[11] Doc. A

2015/2366 ("PSD2"). At the time of processing, the transactions were executed in the ordinary course through authenticated sessions, and there were no objective indicators that they were unauthorised or fraudulent;

4. Whereas Article 40(1) of Directive No. 1 of the Central Bank of Malta, which transposes PSD2 into Maltese law, provides that a payment transaction is considered to be authorised where the payer has given consent to its execution. In the present case, consent was given through the successful completion of the authentication process using credentials associated with (Complainant). The Bank therefore received legitimate and binding payment instructions and, in accordance with the applicable legal framework, bears no obligation to refund the disputed amounts:

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

5. Whereas, in compliance with PSD2, the Bank has implemented robust technical and procedural security measures, including SCA, 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) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data."*[12]

6. Whereas, in addition to SCA, the Bank applies dynamic linking in accordance with Commission Delegated Regulation (EU) 2018/389, ensuring that each authentication is uniquely linked to the specific transaction amount and payee, thereby further reinforcing the integrity and security of the payment authorisation process. Article 5 provides the following:

> *"Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this*

[12] Article 4(3) of PSD2.

Regulation, they shall also adopt security measures that meet each of the following requirements:

a) The payer is made aware of the amount of the payment transaction and the payee;

b) The authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

c) The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

d) Any change to the amount or the payee results in the invalidation of the authentication code generated"

7. Whereas the payments were approved by means of (Complainant's) confidential details. The Bank had no control over them as they were done without the Bank's intervention. Once the Bank receives legitimate instructions for a "third party payment" from the adequate channels, the Bank implemented them, as it is reasonably expected that the only person who has access to such confidential information and systems is the person with whom it is associated. In fact, this is outline in the terms and condition of the Internet Banking system[13] which provide the following:

'You authorise us to act on any instruction that we receive through the Channels which has been, or reasonably appears to have been, sent by you and which, where applicable, has been using your Security Number/s or BOV Mobile PIN or biometric data.'[14]

"All payments, instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your BOV Securekey security number or numbers ("Security Number/s"); or input your BOV Mobile PIN

[13] Doc. B
[14] Doc. B, page 5

("BOV Mobile PIN"), or input your biometric data, are deemed as ***binding*** *on you."*[15]

8. Whereas the Bank respectfully submits that (Complainant) herself confirmed that she disclosed her Internet Banking credentials after interacting with a fraudulent communication. Such disclosure directly undermines the confidentiality of the personalised security credentials which, under PSD2 and the applicable contractual framework, are required to remain strictly personal to the account holder. The execution of the disputed transactions was therefore the direct result of the use of valid credentials following their disclosure, and not of any failure or malfunction within the Bank's systems. In these circumstances, the responsibility for the unauthorised access to the Complainant's account cannot be attributed to the Bank;

B. Transaction limits and risk assessment

9. Whereas it is significant to note that the disputed transactions were also within the applicable transaction limits imposed for third-party payments effected through the Bank's digital banking channels. In the present case, the relevant limit for personal customers using Internet Banking was €5,000[16] *per transaction, as publicly disclosed by the Bank. The disputed third-party payments of €500 and €4,440 therefore did not exceed any system-imposed or disclosed threshold that would, of itself, prevent execution or render the transactions abnormal at the point of processing.*

It is further noted that PSD2 does not impose an obligation on payment service providers to set transaction limits but merely requires that customers be informed where such limits exist. Accordingly, the execution of the disputed transactions within the applicable limits was fully consistent with both the Bank's disclosed framework and the applicable regulatory requirements;

10. Whereas, while Commission Delegated Regulation (EU) 2018/389 permits payment service providers, in certain circumstances, not to apply

[15] *Ibid*., page 4

[16] Doc. C (Such information is also accessible on the Bank's website: https://www.bov.com/bov-digital-banking-limits)

SCA to low-risk transactions,[17] the Bank consistently applies SCA as a matter of policy in order to maintain the highest possible level of security. In the present case, both disputed transactions were authorised through SCA notwithstanding that the amounts fell within the ordinary and disclosed transaction limits;

C. User obligations and gross negligence

11. Whereas, without prejudice to the foregoing, even if (Complainant) were to allege that she did not subjectively intend to authorise the disputed payments, the Bank is nevertheless not obliged to refund the amounts in question where their execution was enabled (Complainant's) own actions. The applicable legal framework does not turn on subjective intention, but on whether the payment service user complied with her statutory and contractual obligations in relation to the use of the payment instrument and the safeguarding of personalised security credentials. In this regard, Article 45 of Directive No. 1 of the Central Bank of Malta, entitled "Obligations of the payment service user in relation to payment instruments and personalised security credentials", provides that the payment service user must use the payment instrument in accordance with its terms and take all reasonable steps to keep personalised security credentials safe:

> *'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.'*

12. Whereas Article 50(1) of the same Directive further provides that the payer shall bear all losses relating to unauthorised payment transactions where such losses are incurred as a result of the payer acting fraudulently

[17] Article 18 of Regulation (EU) 2018/389

or failing to fulfil one or more of the obligations set out in Article 45 with intent or gross negligence:

> *'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.'*

13. Whereas (Complainant) acted in breach of both the statutory obligations referred to above and the contractual obligations set out in the Bank's terms and conditions governing the use of the Bank's Internet Banking service, which provide the following:

> *'You must take all the reasonable precautions to prevent the loss, theft or fraudulent use of the BOV Securekey, the Security Number/s, the BPV Securekey PIN, and/or the BOV Mobile Application, the BOV Mobile Authentication Software, biometric data, the BOV Mobile PIN, as applicable. You undertake not to record your BOV Securekey PIN and/or BOV Mobile PIN in an easily recognizable form and to keep said PINs separate from the BOV Securekey and/or the mobile device. You must take every effort to prevent the BOC Securekey, the Security Number/s, the BOV Securekey PIN and/or the BOV Mobile Application; the BOV Mobile Authentication Software, the BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party.'*[18]

14. Whereas, as a voluntary user of the Bank's Internet and Mobile Banking services, (Complainant) knew, or ought reasonably to have known, that access to such services may only be effected through the Bank's official website or mobile application, and that the Bank does not request customers to disclose personalised security credentials or to access Internet Banking through links received by SMS, social media or other unsolicited communications. This forms part of the basic conditions governing the use of the Bank's digital banking services;

[18] Doc. B, page 7

15. Whereas notwithstanding this, (Complainant) proceeded to act in a manner inconsistent with the standard of care reasonably expected of a prudent payment service user, by clicking on a link received by SMS and providing her personalised security credentials on a website impersonating the Bank;

D. Warnings, awareness campaigns and the Complainant's conduct

16. Whereas, in addition to contractual and technical safeguards, the Bank has for several years implemented a comprehensive, structured and sustained programme of customer warnings and scam awareness initiatives as part of its operational and risk mitigation framework, specifically aimed at preventing spoofing, smishing and impersonation fraud. These initiatives are delivered through a combination of direct customer communications and continuous public-facing campaigns across digital and traditional media;

17. Whereas, prior to the incident complained of, the Bank sent (Complainant) a direct SMS warning on the 15th of July 2025, expressly stating that the Bank would never request customers to transfer money or disclose card details, PINs, verification codes or passwords via phone calls or SMS/email links, and warning customers to remain vigilant against such scams:

> *'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.'*

18. Whereas the content of the said SMS warning was clear, direct and unambiguous, and specifically addressed the precise fraud typology encountered in this case, namely impersonation through unsolicited SMS communications containing links and urgent instructions;

19. Whereas the said SMS warning formed part of a broader and continuous scam-awareness programme implemented by the Bank throughout 2025,[19] consisting of frequent educational posts, videos, reels and boosted campaigns warning customers against clicking on links

[19] Doc. D

received by SMS, responding to urgent payment requests, or disclosing personalised security credentials;

20. Whereas these scam-awareness campaigns were disseminated regularly throughout the year, including in the months immediately preceding and following the 4th of August 2025, and were published across multiple channels, including Facebook, Instagram, TikTok, YouTube, television, radio and print media. Several such posts achieved significant reach and engagement, demonstrating that the warnings were actively circulated and accessible to customers;

21. Whereas the Bank further reinforced these warnings through boosted posts, reels and public campaigns focusing on SMS impersonation, fraudulent links, urgent payment requests and credential disclosure. These initiatives were aimed at ensuring repeated exposure to scam-prevention messaging and reinforcing customer vigilance;

22. Whereas accordingly, the Bank submits that (Complainant) was not only contractually bound to safeguard her personalised security credentials, but was also operating in an environment in which clear, frequent and well-publicised warnings regarding precisely the type of fraud encountered were consistently issued by the Bank prior to the incident complained of;

23. Whereas, in addition to the Bank's own warnings, guidance warning consumers against accessing banking services through links received by SMS or email, and emphasising the need to safeguard personalised security credentials, is likewise consistently issued by the Malta Financial Services Authority (MFSA). Of particular relevance is the MFSA's publication 'The MFSA's Guide to Secure Online Banking',[20] which reiterates that customers should only access banking services through genuine channels and must protect all confidential access data:

> *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*

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

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.

24. Whereas, notwithstanding the foregoing (Complainant) nonetheless proceeded to click on a link received by SMS, disclose her personalised security credentials on a third-party website impersonating the Bank, and manually authenticated multiple transactions using SCA;

25. Whereas by engaging in such conduct, (Complainant) acted in breach of the terms and conditions governing the use of the Bank's digital banking services and failed to comply with her obligations under Article 45(1) and 45(2) of Directive 1 of the Central Bank of Malta, in that she did not take reasonable steps to safeguard her personalised security credentials. It is reasonably expected that a consumer is aware of, and adheres to, the terms regulating the contractual relationship by which he is bound;

26. Whereas it is well-established that no system of safeguards, whether contractual, technical or educational, can prevent losses where a customer voluntarily discloses confidential banking credentials or authentication codes or inputs such information on fraudulent websites. In the present case, the Complainant's own actions directly enabled the execution of the disputed transactions;

27. Whereas therefore, the Bank respectfully submits that any alleged fraud arose as a direct consequence of (Complainant) voluntary participation in the authentication process, in disregard of clear, repeated and explicit warnings issued by the Bank. Such conduct goes beyond mere inadvertence or error and constitutes gross negligence, thereby excluding any obligation on the part of the Bank to bear the resulting loss;

III. Timeline of Events

28. Whereas on the 4th of August 2025, (Complainant) informed the Bank that she had fallen victim to a scam after clicking on a fraudulent link and providing her Internet Banking credentials. She reported that two payments, in the amounts of €4,440 and €500, had been executed from her account ending 3057, with payment references 25216010550760000[21] and 25216010550010000[22] respectively. On the same day, the matter was immediately referred to the Bank's Payments Investigations Unit and Customer Resolutions, and recall requests were initiated in respect of both payments;

29. Whereas on the 5th of August 2025, the Bank formally acknowledged the complaint and confirmed to (Complainant) that recall of funds had been initiated for both transactions. She was also requested to provide a copy of the police report and screenshots of the fraudulent communications,[23] which were submitted;

30. Whereas on the 3rd of October 2025, Payments Investigations received confirmation from the beneficiary bank that the recall of the €4,440 payment had been declined due to no funds remaining. (Complainant) was informed accordingly;[24]

31. Whereas on the 10th of October 2025, a similar confirmation was received indicating that the recall of the €500 payment had likewise been declined. Complainant was informed accordingly;[25]

32. Whereas on the 13th of October 2025, the Bank informed (Complainant) that both recall attempts had been unsuccessful and advised her of the possibility to apply for a partial refund under the Arbiter's model, providing her with a copy of the applicable framework. The Complainant confirmed her wish to proceed under the said model;[26]

[21] Doc. E
[22] Doc. F
[23] Page 009 of the Complaint
[24] Page 014 to 015 of the Complaint
[25] Page 017 of the Complaint
[26] *Ibid*.

33. Whereas on the 28th of January 2026, following completion of the internal assessment and application of the Arbiter's model, the Bank approved and communicated a without prejudice offer of 50% compensation, amounting to €2,470, to (Complainant);[27]

34. Whereas on the 20th of February 2026, (Complainant) was reminded to indicate whether she accepted the Bank's offer;

35. Whereas on the 27th of February 2026, (Complainant) informed the Bank that she was declining the offer and intended to refer the matter to the Office of the Arbiter for Financial Services. The case was thereafter closed from the Bank's end;[28]

36. Whereas in view of the above, the Bank respectfully submits that the incident was reported immediately on the same day the disputed transactions occurred, the Bank maintained ongoing engagement with (Complainant), providing updates and documentation as developments arose; and the outcome of the recall process was ultimately dependent on the beneficiary bank's control, whose cooperation was required and whose responses determined the success or otherwise of the recall efforts;"[29]

Seduti

Fl-ewwel seduta tal-20 t'April 2026, l-Ilmentatrici spjegat il-każ kif diġà riprodott hawn fuq u kkonkludiet hekk:

"Jiena nħoss li 50% mhumiex biżżejjed peress li kont għadni klijenta ġdida u kelli dik il-home loan application, jiġifieri s-suspett tiegħi ma setax ikun għoli.

Ngħid li dwar il-home loan kont nitkellem mal-bank fiżikament. Kienu jibagħtu emails ukoll. Ġieli irċevejt xi email b'encrypted message. U, allura, ħsibt li din kienet xi ħaġa simili.

[27] Page 024 to 025 of the Complaint
[28] Page 077 of the Complaint
[29] P. 200 - 209

Nixtieq insemmi wkoll li meta għafast il-link, in no way ma kont naf li qed nagħmel xi pagament. Qatt ma telali xi valur ta' xi flus jew currency sign jew beneficiary name."[30]

Fil-kontroeżami qalet:

"Mistoqsija allura naqbilx li l-argument ma jreġix li jien nassumi li kien mill-bank għax ma kontx qed nikkomunika permezz ta' SMS u lanqas permezz ta' dak in-numru, ngħid li mhux eżatt għax għalija x'ħin rajt messaġġ BOV Mobile assumejt li dak komunikazzjoni mill-bank.

Qed jingħad li qatt ma kont ikkomunikajt fuq l-account opening u fuq il-home loan application permezz ta' SMS. Ngħid, eżatt.

Qed jingħad li meta dħalt fil-link tal-SMS, idderiġieni għal fuq website. Ngħid, eżatt. Kienet bħall-BOV Log In normali.

Mistoqsija xi staqsieni eżatt fuq il-website, ngħid li ilu ftit xhur imma kelli biex indaħħal il-User ID, li daħħalt tiegħi personali u, mbagħad, code u dak il-code iġġenerajtu mill-app. Dan kien il-One-Time Password.

Qed jingħad li sussegwentement, anke kif jidher mill-iscreenshot li ppreżentajt, irċevejt activation code u mistoqsija x'għamilt, jekk daħħalthiex fuq il-website, ngħid li ma niftakarx eżatt imma nassumi li fil-web page baqgħet tippromptjani u daħħaltha fil-website.

Mistoqsija nifhimx li b'dawk il-passi li ħadt setgħu isiru l-pagamenti lill-iscammer, ngħid li issa iva.

Mistoqsija jekk qabel dan l-inċident kontx naf li l-bank qatt ma jitlob lill-klijenti biex jagħtu l-kredenzjali tagħhom permezz ta' SMSes, ngħid li kont klijenta ġdida, u għalija, as such, ma talabnix il-kredenzjali. Għalija qisni dħalt ġo link u ħa nagħmel log in fil-website tal-bank biex nara l-messaġġ, jiġifieri ma kont naf li qed nagħti dik id-data.

Ngħid li ma kontx naf li l-bank qatt ma jitlob kredenzjali għax għalija dawk ma kinux kredenzjali.

[30] P. 258

Mistoqsija naqbilx li l-bank għamel kampanji estensivi kif ukoll bagħatli SMS dirett, ngħid li naqbel imma l-kampanja mhux neċessarjament kulħadd jaraha.

Qed jingħad li fl-ilment tiegħi stqarrejt li l-bank dam ma ħa azzjoni, però, waqt din is-seduta għidt ukoll li dakinhar stess ibblokkjawli l-card u l-għada bdew ir-recall requests.

Ngħid eżatt. Jien għar-recall requests kont qed nirreferi li damu.

Qed jingħad li r-recall request mhuwiex dependenti fuq il-bank imma hu dependenti fuq il-beneficiary bank.

Mistoqsija naqbilx li min-naħa tal-bank għamel minn kollox sabiex ikun jista' jipprova jidderiġili l-flus lura li kont tlift, ngħid li iva, naqbel."[31]

Fit-tieni seduta li nżammet fis-17 ta' Ġunju 2026, il-Bank ressaq ix-xhieda ta' Michael Gatt, espert fis-sistema tal-pagamenti elettroniċi tal-BOV. Spjega kif f'għajnejn il-Bank, il-pagamenti ilmentati dehru awtorizzati mill-Ilmentatriċi u dan skont ir-regoli Ewropej dwar pagamenti.

Spjega li f'dan il-każ jidher li l-Ilmentatriċi ikkoperat mal-frodist billi daħħlet il-kodiċi mitluba, li hija biss kellha, fis-*Signature 1 panel* tas-sistema, u dan ippermetta lill-frodist jieħu f'idejh iċ-ċavetta li jawtorizza pagamenti daqslikieku kienet l-Ilmentatriċi li qed tawtorizzahom.

Spjega:

"Ngħid li l-bank qatt ma jitlob lill-klijenti tiegħu biex jagħtu l-kredenzjali tagħhom permezz ta' SMS, email jew telefonata.

Nikkonferma li l-Ilmentatriċi irċeviet dawn il-warnings qabel ma ġara l-inċident.

L-Arbitru jiġbed l-attenzjoni li l-Ilmentatriċi hija klijenta ġdida tal-bank u kienet irċeviet warning wieħed biss li kien xi xahar qabel.

L-Ilmentatriċi tikkonferma li kienet irċeviet dan il-warning.

[31] P. 259 - 260

L-Ilmentatriċi tikkonferma li hi ma kinitx għamlet pagamenti qabel dan l-inċident.

Kontroeżami:

Qed jingħad li l-Ilmentatriċi ma kinitx taf li qiegħda tagħmel pagament għax hi ma daħħlet l-ebda ammont.

Ngħid li ġaladarba klijent jagħti l-informazzjoni kollha li spjegajt qabel, awtomatikament il-frodista ħa over l-Internet Banking tal-klijent. It-tranżazzjonijiet għamilhom il-frodista."[32]

Xehed ukoll Keith Vella, *Deputy MLRO* u Head ta' *Transaction Monitoring and Pro-active Analysis* tal-BOV, li spjega l-*monitoring payments system* li jopera l-Bank biex jippreveni l-frodi. Qal li skont ir-*risk-based approach* tas-sistema, iż-żewġ pagamenti ma kienx hemm għalfejn jiġu mwaqqfa.[33]

Fil-kontroeżami qal:

"Qed jingħad li fit-Termini u Kundizzjonijiet tal-Bank hemm li pagament jista' jiġi rifjutat jew imwaqqaf jekk jidher mhux tas-soltu meta mqabbel mal-mod ta' kif il-klijent normalment juża l-kont tiegħu.

Mistoqsi għalfejn f'dan il-każ ma ġewx imwaqqfa jew soġġetti għal verifiki addizzjonali meta l-Ilmentatriċi qatt ma kienet għamlet pagament online ta' din in-natura jew ammont simili u meta t-tranżazzjonijiet żvojtawlha l-kontijiet kollha tagħha, ngħid li fit-Terms and Conditions hemm 'jista'' jiġifieri mhux kull transaction trid tieqaf. U jekk inwaqqfu kull tranżazzjoni nkunu qed niksru l-liġi aħna stess ta' bank għax qed immorru kontra kull prinċipju fil-liġijiet tal-Anti-Money Laundering kif ukoll bir-recommendations li joħorġu kemm ir-regolatur Malti kif ukoll regolaturi internazzjonali kif ukoll standarde setters f'dan il-kuntest.

Kif għidt, is-sistema taħdem fuq a risk-based approach. Ma jfissirx li għax qatt ma għamilt pagament bħalma ġraw b'dawn iż-żewġ pagamenti, is-sistema gġandha bilfors twaqqafhom. Hemm diversi red

[32] P. 262
[33] P. 262 - 264

> ***flags li s-sistema tieħu in konsiderazzjoni imma ma jfissirx li persuna jew klijent jagħmel tranżazzjoni l-ewwel darba kif qed jagħmilha issa, ifisser li bilfors is-sistema trid twaqqafha.***
>
> ***Apparti minn hekk, ma jfissirx ukoll li għax klijent ma jkun għamel qatt tranżazzjoni barra minn Malta, is-sistema bilfors trid twaqqafha. Is-sistema taħdem within the parameters of the risk-based approach kif aħna mitlubin nagħmlu mir-regolaturi u mil-liġijiet internazzjonali.***
>
> ***F'dan il-każ il-bank uża r-risk-based approach f'dan il-kuntest ukoll u s-sistema ma kellhiex għalfejn twaqqaF dawn iż-żewġ tranżazzjonijiet.***
>
> ***Mistoqsi jekk jinġibed l-ammont kollu li hemm fil-kont fi tranżazzjoni waħda, is-sistema tal-bank ma tqisx dan bħala red flag, ngħid li għalkemm il-kont kien fih kważi €5,000 u dawn inġibdu fi transaction waħda, that's a red flag on its own."***[34]

Xehed ukoll Luke Cutajar, uffiċjal inkarigat mir-*recalls* li jsiru mill-Bank meta jirċievi rapport ta' *scam* biex isir tentattiv li l-fondi jiġu rkuprati qabel ma l-i*scammer* jilħaq jiġbidhom. Qal li r-*recalls* saru fil-ħin ta' 15:33 b'mod tempestiv iżda ma rnexxewx għax il-bank barrani qal li ma jistax jintraċċa lill-klijent tal-kont fejn daħlu l-flus biex jawtorizza r-rimbors.[35]

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

[34] p. 264
[35] P. 265 - 266

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 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 wżat biex jasal għal deċiżjoni dwar kif ser isir '*apportionment'* tal-konsegwenzi tal-frodi. Il-mudell fih ukoll diversi rakkomandazzjonijiet biex il-banek ikomplu jsaħħu l-protezzjoni tal-konsumatur kontra frodisti li kulma jmur dejjem isiru aktar kapaċi u kreattivi.

Iżda l-Arbitru jħoss il-bżonn jemfasizza 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*[36] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara każi fejn l-Ilmentaturi faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[37] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

Għalhekk, il-banek jeħtieġ li jkollhom sistema ta' pagamenti robusta biżżejjed biex il-pagament ma jsirx jekk ma jkunx speċifikament awtorizzat mill-klijent/ilmentatur. Il-banek ma jistgħux ma jerfgħux responsabbilità jekk iħallu toqob fis-sistemi tagħhom li permezz tagħhom il-frodist ikun jista', bla ma jkun hemm aktar involviment tal-klijent/ilmentatur, jagħmlu awtorizzazzjoni speċifika tal-pagament a favur tal-frodist.

Dan il-fatt huwa wkoll inkluż fil-mudell.

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

Il-mudell għandu wkoll għarfien dwar jekk l-ilmentatur ikunx midħla tas-sistemi ta' pagamenti *online* tal-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.[38] [39]

Deċiżjoni

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

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

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

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	(20%)	20%
TOTAL FINALI	**(40%)**	**(60%)**

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 60% tal-piż u l-40% l-oħra iġorrhom il-BOV.

Meta ppubblika l-mudell, l-Arbitru spjega li dan japplika b'mod ġenerali imma l-Arbitru jibqa' ħieles li ma jimxix miegħu f'każijiet speċifiċi li jirrikjedu apprezzament partikolari.

Però, l-Arbitru jiġġustifika, bi spjegazzjonijiet adegwati fid-deċiżjonijiet tiegħu, meta ma jimxix ma' dan il-mudell, fejn applikabbli.

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

F'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatriċi titnaqsilha l-piż ta' negliġenza grossolana b'doża ta' 20%. Dan jieħu kunsiderazzjoni li l-klijenta kienet għadha kif bdiet ir-relazzjoni mal-BOV, kienet irċeviet SMS ta' twissija biex ma tagħfasx *link* u kienet qed tikkomunika mal-Bank dwar self biex tixtri darha.

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

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

L-Arbitru jirrakkomanda li meta jkun hemm reġistrazzjoni ta' *software token* fuq *device* ġdid (li jkun jinvolvi wkoll *unenrolmen*t minn fuq id-*device* ta' qabel għax il-*mobile app* tista' tkun irreġistrata fuq *device* wieħed biss) għandu wkoll ikun hemm eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

L-argument li l-pagamenti setgħu jsiru biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi u għalhekk hemm bżonn ta' konsiderazzjoni profonda biex filwaqt li jinżammu

pagamenti b'xamma ta' frodi, ma jiġux restrittivi b'mod li jiġu mblokkati pagamenti ġenwini li ovvjament huma f'maġġoranza kbira.

Hemm eżempji ta' istituzzjonijiet finanzjarji u banek li għandhom sistemi ta' pagamenti b'teknoloġija avvanzata fejn, f'każ serju ta' dubju, jintbagħat SMS fuq il-*mobile* irreġistrat, jinforma li qed jintalab li jsir pagament u l-klijent jingħata kodiċi li jdaħħal fis-sistema biex jikkonferma l-pagament.

Dan isaħħaħ is-sigurtà u jevita dewmien biex isir kuntatt permezz tat-telefon mal-klijent.[40]

Qed ukoll tiġi skużata b'20% oħra għaliex ma ġiet ippreżentata ebda evidenza li l-Ilmentatriċi kienet għamlet pagamenti *online* bħal dawn fl-aħħar 12-il xahar.

B'kollox, għalhekk, l-Ilmentatriċi hija intitolata għal kumpens ta' 40% tat-telf li sofriet mill-pagamenti frawdolenti li ġew iddebitati fil-kont tagħha mal-Bank.[41]

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' elf, disa' mija u sitta u sebgħin ewro (€1,976).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[42] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[43]

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

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

[41] 40% ta' €,4940

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

[43] [43] 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.

Rakkomandazzjoni

Peress li waqt il-proċess il-Bank kien offra kumpens ta' 50%, l-Arbitru jirrakkomanda, iżda bla obbligu min-naħa tal-Bank, li jżid il-kumpens dekretat (li jżomm konsistenza ma' deċiżjonijiet f'każijiet simili) skont l-offerta li kienet saret qabel ma ġie rreġistrat l-ilment.

_____

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

<u>Nota ta' Informazzjoni relatata mad-Deċiżjoni tal-Arbitru</u>

Dritt ta' Appell

Id-Deċiżjoni tal-Arbitru legalment torbot lill-partijiet, salv id-dritt ta' appell regolat bl-artikolu 27 tal-Att dwar l-Arbitru għas-Servizzi Finanzjarji (Kap. 555) ('l-Att'), magħmul quddiem il-Qorti tal-Appell (Kompetenza Inferjuri) fi żmien għoxrin (20) ġurnata mid-data tan-notifika tad-Deċiżjoni jew, fil-każ li ssir talba għal kjarifika jew korrezzjoni tad-Deċiżjoni skont l-artikolu 26(4) tal-Att, mid-data tan-notifika ta' dik l-interpretazzjoni jew il-kjarifika jew il-korrezzjoni hekk kif provdut taħt l-artikolu 27(3) tal-Att.

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

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