**Quddiem l-Arbitru għas-Servizzi Finanzjarji**

**Każ ASF 069/2026**

**CA**

**('l-Ilmentatur')**

**vs**

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

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

**Seduta 25 t'Awwissu 2026**

**L-Arbitru,**

Ra l-Ilment datat 23 ta' Frar 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi tal-anqas 50% tat-telf li sofra meta saru tliet pagamenti frawdolenti mill-kont tiegħu mal-BOV li b'kollox jammontaw għal €4,950 li minnhom €500 ġew irkuprati.

Fil-fatt, dawn il-pagamenti kollha saru nhar it-13 t'Ottubru 2025, kif spjegat fit-tabella:

| Ħin | Ammont € | Referenza |
|---|---|---|
| 18:12:28 | 1,950 | p. 63; 10 |
| 18:14:36 | 2,500 | p. 63; 10 |
| ~18:27 | 500 | p. 11 |
| Rkupru | (500) | p. 8 |
| | | |
| **TOTAL** | **4,450** | |

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[1] 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*),

[1] L-Uffiċċju tal-Arbitru wkoll 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:

- Fit-13 t'Ottubru 2025, fil-ħin 17:46, irċieva dan il-messaġġ SMS:

  *'A new phone number has been added, If NOT authorised visit https://deskhelp-bov.com For other queries call +35621234821'*[2]

- Billi emmen li dan kien messaġġ ġenwin, għafas il-*link* u daħal f'*site* li dehret identika għal tal-BOV u hemm ta kredenzjali sigrieti biex jidħol fis-*site*.

- Kompla jsegwi l-istruzzjonijiet u daħal fis-*Signature* 1 fejn jidher li talab *authentication code* li eventwalment ġie kkomunikat lill-frodist u b'hekk, il-frodist seta' jittrasferixxi l-*mobile app* fuq *device* ikkontrollat minnu u, bla aktar ħtieġa ta' involviment tal-Ilmentatur, għamel il-pagamenti lmentati.

- Irċieva SMS notifiki ta' tliet pagamenti kif indikat fit-tabella t'hawn fuq.[3]

- Mal-ewwel intebaħ li kien ġie ffrodat u qabad mal-Bank jirrapporta u b'hekk saru *recalls* urġenti li ma rnexxewx, iżda l-aħħar pagament ta' €500 laħaq inżamm.

- Il-Bank offrielu rimbors ta' 30% skont il-mudell tal-Arbitru (dettalji aktar 'l isfel) iżda ma aċċettax għax ippretenda tal-anqas nofs it-telf.

- Sar rapport lill-pulizija nhar l-14 t'Ottubru 2025.[4]

L-Ilmentatur qed jitlob kumpens ta' €2,225 li, kif ġie spjegat qabel, jammonta għal 50% tat-telf sostnut peress li jsostni li l-BOV għandu jġorr nofs it-tort peress li huwa qatt ma kien għamel pagamenti tal-ammonti in kwistjoni li saru fi żmien tempestiv wieħed wara l-ieħor.

[2] P. 10
[3] P. 10 - 11
[4] P. 36

**L-Ilment**[5]

L-Ilmentatur spjega li:

> *"This complaint concerns the Bank's statutory obligations under Directive (EU) 2015/2366 (PSD2) and Commission Delegated Regulation (EU) 2018/389 (the Regulatory Technical Standards on Strong Customer Authentication and Secure Communication, hereafter 'RTS').*
>
> *A key legal standard is set out in Article 2(1) RTS, which requires payment service providers to maintain transaction-monitoring mechanisms 'that enable them to detect unauthorised or fraudulent payment transactions' by analysing payment transactions taking into account elements 'which are typical of the payment service in the circumstances of a normal use of the personalised security credentials.' The regulatory standard is therefore behavioural and contextual: it requires an assessment of whether a given transaction fits the normal pattern of use for that service and that customer. It is not satisfied merely by showing that the same payment function (e.g. 'Pay Third Party') has been used at least once before.*
>
> *Article 2(2) RTS further specifies minimum risk factors that must be incorporated into transaction monitoring. In particular, Article 2(2)(b) requires consideration of 'the amount of each payment transaction,' while Article 2(2)(c) requires consideration of 'known fraud scenarios in the provision of payment services.'*
>
> *An objective comparison between my historic account behaviour and the fraud pattern demonstrates notable dissimilarities which should have been detected by the banks' monitoring system. Historically, I had used the 'Pay Third Party' feature exclusively for local transfers, with my maximum outgoing payment being €626. I had never executed rapid sequence payment, same-day priority third-party transfers, payments to foreign accounts or large outgoing third-party payments. Additionally, payments were usually performed once a month with the shortest interval between payments being 13 days apart. Table 1 shows a log of the account payments made in the 12 months prior to the fraud incident. By*

[5]Paġni (P.) 1 - 7 b'dokumentazzjoni addizzjonali minn p. 8 - 44.

*contrast, the fraudulent transactions consisted of two same-day priority third-party payments of €1,950 and €2,500, executed in rapid succession, together with a €10,000 internal transfer between my own accounts into account ending 6164 to extract more funds.*

*Table 1. Transactions from account ending 6164 in the 12 months prior to the fraud incident.*

| ***Date of transaction*** | ***Amount in Euro*** |
|---|---|
| *06/12/24* | *106.2* |
| *19/2/25* | *276* |
| *12/03/25* | *75* |
| *03/04/25* | *154* |
| *06/05/25* | *626* |
| *04/06/25* | *102* |
| *08/07/25* | *465* |
| *11/08/25* | *541* |
| *04/09/25* | *350* |
| *17/09/25* | *110.25* |

*I had no prior history of transferring €10,000 internally between accounts. Internal transfers between my own accounts were typically modest and always occurred outwards from account ending 6164.*

*The escalation in transaction magnitude alone is significant. The two fraudulent third-party payments of €1,950 and €2,500 represented approximately 3–4 times my historical maximum third-party payment of €626, and they were executed back-to-back on the same day. The €10,000 internal transfer substantially exceeded my prior internal transfer behaviour. Under Article 2(2)(b) RTS, the amount of each payment transaction is a mandatory risk consideration. A deviation of this scale from established behavioural norms cannot reasonably be classified as 'typical of the normal use' of my personalised security credentials within the meaning of Article 2(1).*

*Moreover, the use of same-day priority execution constituted an additional risk amplifier. I had never previously utilised priority processing for third-party transfers. Priority execution materially reduces recovery opportunities and is widely recognised within the banking sector as a high-risk fraud vector. When combined with the sudden increase in transaction size and rapid sequencing, this pattern aligns with known authorised push payment (APP) fraud typologies. Article 2(2)(c) RTS expressly requires banks to factor known fraud scenarios into their monitoring mechanisms.*

*PSD2 Article 68(2) further provides that a payment service provider may block a payment instrument for objectively justified reasons relating to suspicion of unauthorised or fraudulent use. The regulatory framework does not require certainty of fraud; it requires objectively justified suspicion. The cumulative indicators present in this case — significant escalation in amount, first-time use of priority processing, rapid consecutive execution, and unprecedented internal reallocation of €10,000 — collectively created objective grounds for suspicion. The fact that the smallest transaction was successfully recalled confirms that intervention was possible within the processing window, had appropriate suspicion been triggered earlier.*

*The mere fact that I had previously used the 'Pay Third Party' feature does not render a fourfold escalation in amount, combined with first-time priority usage and abnormal internal fund movement, typical of normal use.*

*On an objective assessment of my historic behavioural baseline and the fraud pattern, the transactions were materially atypical. Accordingly, the Bank's classification of these payments as 'similar transactions' does not align with the regulatory standard governing transaction monitoring obligations under PSD2 and Commission Delegated Regulation (EU) 2018/389. On this basis, a higher proportion of responsibility should be allocated to the Bank than the 30% refund it has offered and should be changed to 50%."*[6]

[6] P. 42 - 44

**Risposta tal-Fornitur tas-Servizz**

Fir-risposta[7] tagħhom datata 17 ta' Marzu 2026, il-BOV qalu:

> ***"A. Authorisation of the transactions and compliance with PSD2***
>
> *5. Whereas the Bank's records[8] show that the disputed payments were duly authorised by the Complainant on the 13th October 2025 at 18:12:28 and 18:14:36, following successful authentication through the Bank's secure digital banking channels. Both transactions were authorised using the 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) 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;*
>
> *6. 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 the 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.'*
>
> *7. Whereas, in compliance with PSD2, the Bank has implemented robust technical and procedural security measures, including SCA, defined as:*

[7] P. 49 – 62 u dokumenti annessi p. 63 - 132
[8] Doc. A

> *'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.'*[9]

8. *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;*

9. *Whereas once the Bank receives a third-party payment instruction through its secure and authenticated channels that has been properly authorised using valid personalised security credentials, it is obliged to process such instruction. It is reasonably expected that access to and use of such credentials rests exclusively with the account holder. In this case, the payments were duly authorised following successful validation of the Complainant's credentials, and there was no indication of fraud at the point of execution. This position is expressly reflected in the Bank's General Terms and Conditions governing the use of Internet and Mobile Banking, effective as from the 5th October 2025, which provide that:*

> *'All payments, Instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your security credentials while using a Hardware Token, BOV Mobile Authentication Software or BOV ebanking (generate Login OTP/scan Cronto) are deemed as binding on you. You authorise us to act on any Instruction that we receive through the Channels and declare and confirm that any information given by you to us is true and correct and you are responsible for the authenticity and*

[9] Article 4(3) of PSD2

*correctness of the information given.' (Section 2.22 – Any Instructions to us)*[10]

***B. Transaction limits and risk assessment***

10. *Whereas 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*[11] *per transaction, as publicly disclosed by the Bank. The payments of €1,950 and €2,500 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 oblige payment service providers to impose transaction limits but merely requires that customers be informed where such limits exist;*[12]

11. *Whereas, while Commission Delegated Regulation (EU) 2018/389 permits payment service providers, in certain circumstances, not to apply SCA to low-risk transactions*[13]*, 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***

12. *Whereas, without prejudice to the foregoing, even if the Complainant were to allege that he 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 by the Complainant's own actions. The applicable legal framework does not turn on subjective intention, but on whether the payment service user complied with his statutory and*

[10] Doc. B, page 24
[11] Doc. C (Such information is also accessible on the Bank's website: https://www.bov.com/bov-digital-banking-limits)
[12] Article 28(2) of Directive 1 of the Central Bank of Malta which reflects article 52(2) of the PSD2
[13] Article 18 of Regulation (EU) 2018/389

*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.'*

13. *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 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.'*

14. *Whereas the Complainant acted in breach of both the statutory obligations referred to above and the contractual obligations set out in the Bank's General Terms and Conditions governing the use of Internet and Mobile Banking, effective as from 5th October 2025, which expressly require customers to take all reasonable precautions to safeguard their personalised security credentials and*

*to prevent such credentials from being disclosed to, or coming into the possession or knowledge of, third parties. In particular, the said General Terms and Conditions provide that:*

> *'You must take all the reasonable precautions to prevent dissemination, loss, theft or fraudulent use of the BOV Securekey, the Security Number/s, the BOV Securekey PIN, and/or the BOV Mobile Application, the BOV Mobile Authentication Software, biometric data, the BOV Mobile PIN, BOV ebanking as applicable.' (Section 2.23 – Security Notice)*[14]

15. *Whereas, as a voluntary user of the Bank's Internet and Mobile Banking services, the 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 credentials or to access Internet Banking through links received by SMS, social media or other unsolicited communications. The Bank has consistently and repeatedly warned customers against precisely such conduct. The General Terms and Conditions expressly state that:*

> *'It is your obligation to ensure that you access the correct and official BOV social media and website links. If you follow a fraudulent link, your Bank card details or personal information or financial information might be used by fraudsters and you may end up losing money. We will never send you text messages or messages via social media asking you for personal or financial information, passwords, PINs, card numbers or images with your card details.' (Section 10 – Social Media Channels)*[15]

16. *Whereas notwithstanding these clear and well-known warnings, the Complainant proceeded to act in a manner wholly inconsistent*

[14] Doc. B, page 24
[15] Doc. B, page 33

*with the standard of care reasonably expected of a prudent payment user;*

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

17. *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 measures include, inter alia, the direct transmission of SMS alerts to customers warning them of the risks associated with fraudulent communications;*

18. *Whereas, prior to the incident complained of, the Bank sent the Complainant multiple direct SMS communications expressly warning that the Bank never sends links by SMS, never requests customers to disclose credentials, and never asks customers to authorise transactions through unsolicited communications. These warnings were sent repeatedly between November 2023 and September 2025 and included, inter alia, the following messages:*

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

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

(v) *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) *4th September 2025 – 'Il-Bank of Valletta qatt ma jibghatlek SMS b'links biex taghfas fuqhom. Taghfashomx ghax tista tigi misruq! Jekk tigi f'dubju, cempel lill-Bank fuq 21312020.'*

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

20. *Whereas the said SMS warnings were not isolated communications but formed part of a broader and structured customer education programme implemented by the Bank on a continuous basis. In this regard, the Bank consistently issued scam awareness communications throughout the relevant period, addressing spoofing, smishing and impersonation fraud, including fraudulent SMS messages containing links and urgent instructions purporting to originate from the Bank;*

*21. Whereas during 2025, including in the months preceding and surrounding the incident of the 13th October 2025, the Bank conducted an ongoing programme of public awareness initiatives, disseminated throughout the year via various channels, with a specific focus on warning customers against clicking on links received by SMS and against disclosing credentials or authorising transactions following unsolicited communications. These initiatives included, inter alia, a public webinar on scams and phishing awareness, educational articles addressing financial crime and fraud risks, and other public-facing informational materials;*

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

*23. Whereas the Bank also utilised social media platforms to extend the reach of its scam awareness messaging, including the publication of posts specifically warning about spoofed SMS messages and fraudulent links during August and October 2025, that is, in close temporal proximity to the incident complained of;*

*24. 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',*[17] *which reiterates that customers should only*

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

*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 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, notwithstanding the foregoing warnings, which were directly communicated to the Complainant, repeated over a prolonged period, and specifically addressed the precise fraud typology encountered in this case, the Complainant nonetheless proceeded to click on a link received by SMS, disclose his personalised security credentials on a third-party website impersonating the Bank, and manually authenticate multiple transactions using SCA;*

26. *Whereas by engaging in such conduct, the Complainant acted in breach of the terms and conditions governing the use of the Bank's digital banking services and failed to comply with his obligations under Article 45(1) and 45(2) of Directive 1 of the Central Bank of Malta, in that he did not take reasonable steps to safeguard his 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;*

27. *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;*

28. *Whereas therefore, the Bank respectfully submits that any alleged fraud arose as a direct consequence of the Complainant's 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*

29. *Monday 13th October 2025 –*

    (i) *The Complainant authenticated two third-party payments in the amounts of €1,950 and €2,500, which were approved at 18:12:28 and 18:14:36 respectively, following successful Strong Customer Authentication. Both transactions were processed as immediate payments in accordance with the Bank's digital banking procedures. The Bank's Terms and Conditions provide that where a customer requests an immediate payment, the payment instruction becomes irrevocable once received and cannot be cancelled or amended. This is consistent with Article 80 of Directive PSD2, entitled 'Irrevocability of a payment order';*

    (ii) *Later, the Complainant contacted the Bank's Electronic Banking Unit and reported that he had fallen victim to a scam after clicking on a link received by SMS and providing his internet banking login credentials. The Complainant advised that the payments of €2,500 and €1,950 had been affected from his account;*

*(iii) The matter was immediately brought to the attention of the relevant internal units in order to assess the situation and take the necessary safeguarding and recovery steps;*

*(iv) The Bank also identified that a further payment in the amount of €500 had been processed. This payment was likewise treated as potentially fraudulent and included in the recovery process;*

*(v) The Bank's Payments Investigations Unit ('PIU') initiated recall requests in respect of the disputed payments[18] through the applicable interbank recall channels, following the Complainant's report;*

*(vi) PIU confirmed that the payment in the amount of €500 had been successfully returned to the Bank. The funds were credited back to the Complainant's account ending 6146 on the same day;*

*30. Tuesday 14th October 2025 –*

*(i) The Bank formally acknowledged the Complainant,[19] confirmed that the €500 had been returned and credited, and advised that the recall requests in respect of the remaining payments of €1,950 and €2,500 were still ongoing. On the same date, the Complainant was requested to provide screenshots of the fraudulent messages received and a copy of the police report, both of which he subsequently supplied;*

*31. Tuesday 28th October 2025 –*

*(i) The Bank confirmed that the recall requests in respect of the payments of €1,950 and €2,500 were being declined due to no funds remaining in the beneficiary account;[20]*

[18] Doc. E and Doc. F
[19] Page 008 of the Complaint
[20] Page 021 of the Complaint

*(ii) The Bank informed the Complainant accordingly and advised him of the possibility to apply for a percentage refund under the Arbiter's model, without prejudice to the Bank's position;*[21]

*32. Whereas the Bank respectfully submits that the successful recovery of the €500 payment demonstrates that the Bank took prompt action and pursued all available recovery channels within its control upon being notified of the suspected fraud. The inability to recover the remaining amounts arose from the unavailability of funds at the receiving bank, a circumstance beyond the Bank's control;"*[22]

**Seduti**

Fl-ewwel seduta tat-28 t'April 2026, l-Ilmentatur spjega l-każ kif diġà riprodott hawn fuq u kompla jgħid:

***"Ir-raġuni hi għax jien inħoss li l-monitoring tat-transactions tiegħi, min-naħa tal-BOV, ma kinux adekwati għax il-pattern tal-pagamenti kien atypical, ma kienx tas-soltu.***

***Dawn it-tliet pagamenti saru f'perjodu ta' 14-il minuta, li saru immedjatament wara li sar log in fuq device kompletament ġdid u wara li saru interactions ġodda li qatt ma kienu saru qabel min-naħa tiegħi.***

***Ngħid li dan l-account, storikament, kien intuża minni biex nagħmel pagamenti lokali, third-party payments, li tipikament kienu jsiru bejn wieħed u ieħor kull sitt jew tmien ġimgħat, u li kienu jkunu ta' ammonti ta' valuri żgħar ħafna.***

***Ngħid li dawn il-pagamenti kont nagħmilhom billi nidħol fil-BOV App u kont nagħmel Pay Third Party u kont indaħħal id-dettalji tal-business li kont ser inħallas.***

***Dawn ma kinux isiru b'SCT Instant Payments u l-pagamenti frawdolenti saru bl-SCT Instant Payments.***

[21] *Ibid*.
[22] P. 50 - 60

> ***Jien inħoss li din il-kumbinazzjoni ta' login ġdida minn device ġdida, l-użu tal-ewwel darba ta' Enhanced Authentication Methods u dan l-eżempju ċar ta' pagamenti kbar li qatt ma saru qabel, u t-timeframe, jiġifieri l-ammont qasir taż-żmien li saru fih, huwa ovvju li mhux is-soltu li jsir hekk.***
>
> ***Allura, nħoss li l-bank kellu jkollu monitoring system to flag these payments u nħoss li kieku kellu dan, ma kinux isiru t-tieni jew it-tielet pagament.***
>
> ***Ngħid li meta tagħmel pagamenti through Third-Party Payments, dawn ma jsirux bis-Signature 1 jew bis-Signature 2. Ngħid li s'issa għadni ma nafx għalxiex dawn jintużaw."***[23]

Mistoqsi jekk irċeviex SMS bl-*Activation Code* qal li ma jiftakarx,[24] u wara qal li forsi irċevih imma ma sabux.[25]

Fil-kontroeżami qal:

> ***"Nikkonferma li fit-13 t'Ottubru 2025, irċevejt SMS li jien ħsibt li ġej mill-bank.***
>
> ***Nikkonferma li dak il-ħin il-mobile kien dejjem fil-pussess tiegħi.***
>
> ***Qed jingħad li fuq dak l-SMS kien hemm link u mistoqsi x'għamilt wara li għafast il-link, ngħid li kif għafast il-link infetħet awtomatikament website li dehret bħal tal-BOV u jiena daħħalt il-User ID u l-User Code. Nikkonferma li l-User Code hija l-password li jiġġenera l-App.***
>
> ***Ma niftakarx eżatt x'ġara għax kollox ġara daqsxejn malajr u issa għadda naqra żmien. Naħseb kont irċevejt xi messaġġ ieħor imma ma nafx fuq liema channel. Ma nistax nikkonferma 100% kienx l-Activation Code, imma naħseb hekk ġara. Jista' jkun li ktibtu fuq il-BOV App imma m'inix 100% żgur fuqha l-affari.***

[23] P. 134
[24] P. 135
[25] P. 139

> ***Mistoqsi nifhimx li l-informazzjoni li daħħalt kienet kunfidenzjali u sensittiva, ngħid li iva.***
>
> ***Mistoqsi ppruvajtx inċempel il-bank fuq in-numru uffiċjali qabel għafast il-link u daħħalt id-dettalji, ngħid li le.***
>
> ***Mistoqsi jekk qabel dan l-inċident kontx intiż tal-fatt li l-bank qatt ma jibgħat messaġġi, SMSes b'links jew biex tagħti dettalji kunfidenzjali, ngħid li in retrospect iva, għax kont irċevejt messaġġ b'warning, iwissi fuq dawn l-affarijiet.***
>
> ***Qed jingħad li f'paġni 55 u 56 tar-risposta tal-bank hemm lista u mistoqsi naqblux li mhux warning wieħed kien bagħatli l-bank imma kien bagħat diversi warnings, ngħid li iva, naqblu.***
>
> ***Mistoqsi minkejja dawn l-SMSes jien xorta ma ġinix suspett u niċċekkja mal-bank, ngħid li le għax ħassejt li l-SMSes kienu jkunu generic u parti mill-promotional material tal-BOV, affarijiet li tirċievi li ma jkunux indirizzati lejk speċjalment li ħafna drabi tispiċċa tinjora sfortunatament."***[26]

Fit-tieni seduta li nżammet fis-17 ta' Ġunju 2026, il-Bank ressaq ix-xhieda ta' CA, espert fis-sistema tal-pagamenti elettroniċi tal-BOV. Spjega kif f'għajnejn il-Bank, il-pagamenti lmentati dehru awtorizzati mill-Ilmentatur u dan skont ir-regoli Ewropej dwar pagamenti. Spjega li f'dan il-każ jidher li l-Ilmentatur ikkopera mal-frodist billi daħħal il-kodiċi mitluba, li huwa biss kellu, fis-*Signature 1 panel* tas-sistema, u dan ippermetta lill-frodist jieħu f'idejh iċ-ċavetta li jawtorizza pagamenti daqslikieku kien l-Ilmentatur li qed jawtorizzahom.

Spjega li:

> ***"F'dan il-każ, ġie ġġenerat minn fuq l-Internet Banking. Jiġifieri l-proċess telaq minn fuq il-mobile, fejn ġie disclosed il-Login ID u l-One-Time Password. U minn hemmhekk, il-frodista daħal fl-Internet Banking tal-klijent, mar fuq il-function tal-Activation Code, ġie iġġenerat l-Activation Code, ġiet iffirmata s-Signature 1. Dak l-Activation Code intbagħat fuq il-mobile number li jkun irreġistrat mal-bank li b'xi mod ġie ikkomunikat***

[26] P. 135 - 136

***lill-frodista. Minn hemm 'l hemm, il-frodista jista' jissettja l-Mobile App fejn għandu kontroll fuqha kompletament.***

***U minn hemm 'l hemm, beda jagħmel it-tranżazzjonijiet il-frodista.***

***Jiġifieri, minn hemm 'l hemm, il-klijent tilef il-kontroll tal-Internet Banking tiegħu u ħa over il-frodista.***

***Mill-perspettiva tal-bank, il-klijent beda jesegwixxi dawn il-pagamenti.***

***Ngħid li l-bank qatt ma jitlob lill-klijenti biex jagħtu l-kredenzjali tagħhom jew kodiċi permezz ta' SMSs u telefonati.***

***Nikkonferma li f'dan il-każ speċifiku, l-Ilmentatur intbagħtulu diversi SMSs ta' warnings. Ngħid li kull tliet xhur nibagħtuhom."***[27]

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head 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, it-tliet pagamenti ma kienx hemm għalfejn jiġu mwaqqfa.[28]

Fil-kontroeżami qal:

***"Mistoqsi jekk tkun qed tiġi użata għall-ewwel darba s-Signature 1 jew 2 u immedjatament wara jsir pagament, għandux iqajjem suspett lill-bank, ngħid li min-naħa tal-bank ma jfissirx li għax tuża s-Signature 1 jew tagħmel change in activation code għall-ewwel darba dak ifisser li t-transactions ta' wara trid twaqqafhom bilfors.***

***On a risk-based approach, il-bank ma nistġħux kull darba li jkun hemm change in activation code jew inkella l-klijent għall-ewwel darba jitlob is-Signature 1 jitwaqqfu dawk it-transactions kollha. Aħna nsegwu l-guidance u l-liġijiet internazzjonali. On a risk-based approach, ma jfissirx li għax intalbet l-ewwel darba, jew għax kien hemm change fl-activation code, bilfors li hija red flag. Hemm affarijiet oħra li jiġu kkunsidrati.***

***L-Ilmentatur jgħid li saru tliet tranżazzjonijiet u t-tielet tranżazzjoni saret waqt li kien mal-Customer Support jirrapporta l-frodi u wkoll kien hemm***

[27] P. 138
[28] P. 140

***moviment ta' €10,000 minn kont tal-Ilmentatur għal kont ieħor tiegħu biex ikomplu jiġu misruqin il-flus.***

***Mistoqsi x'seta' qajjem suspett lill-bank li dawn it-tranżazzjonijiet kienu frawdolenti, ngħid li fis-sistema ma kienx hemm bżonn li jitwaqqfu l-pagamenti għax ma kien jidher xejn sa dak il-ħin li kien hemm xi ħaġa suspettuża. On a risk-based approach, is-sistema ma ħassitx li twaqqaf dawn it-transactions.***

***Qed niġi mistoqsi li kieku kien hemm aktar flus, kieku kienu jibqgħu jinġibdu l-flus sakemm jispiċċaw?***

***L-Arbitru jiċċara li din it-tielet tranżazzjoni ta' €500, kienet għaddiet u twaqqfet biss għaliex ir-rapport tal-attività kien laħaq daħal u l-bank irnexxielu jżommha milli titlaq 'il barra.***

***Ngħid li iva.***

***L-Arbitru jkompli jgħid li l-mistoqsija tal-Ilmentatur rigward jekk il-flus kinux jibqgħu għaddejjin jgħid li hemm żewġ elementi illi jikkontrolla dan. Inti għandek daily limit li ġeneralment ikun ta' €5,000, jiġifieri jekk tagħmel pagament ta' €5,000 probabilment is-sistema twaqqfu. Mhix kwistjoni ta' transaction monitoring. Hija a built-in system biex jekk inti trid tagħmel pagament ta' €5,000, ikollok tikkomunika mal-bank.***

***Il-mistoqsija tal-Ilmentatur għandha relevanza dwar il-fatt li saru tliet pagamenti within the €5,000 limit f'ċertu ħin limitat, dik fiha innifisha ma setgħetx tat red light lill-bank li l-affarijiet ma kinux kif suppost?***

***U l-Arbitru fehem li s-Sur Vella qed jgħid li le għax is-sistema tagħhom mhijiex sensittiva daqshekk li għax saru tliet pagamenti b'ammonti relattivament żgħar, is-sistema ser twaqqafhom.***

***L-Arbitru jistaqsini jekk fehemx sew.***

***Ngħid li, le, jien m'għidtx hekk. Jiena qed ngħid li għal dawn it-tliet transactions, even though they were transacted within a span of fifteen minutes, ma jfissirx li s-sistema tal-bank ma kinitx sensittiva biżżejjed, ma kienx hemm għalfejn is-sistema twaqqafhom. Plus hekk, mill-analiżi li għamilna aħna, meta bdejna naraw kemm kien l-ammont ta' klijenti u***

> ***kemm ammont ta' transactions qed jgħaddu within a span of a few minutes, li imbagħad jirriżultaw li huma fraudulent, il-perċentaġġ kien veru negliġibbli.***
>
> ***Jiġifieri on a risk-based approach, is-sistema qed taħdem sewwa u within the parameters of the legislation."***[29]

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-*iscammer* jilħaq jiġbidhom.

Qal li r-*recalls* saru fil-ħin ta' 18:28, tliet minuti wara li rċevew ir-rapport, iżda r-*recalls* ma rnexxewx.[30]

**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

[29] P. 140 - 142
[30] P. 142 - 143

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

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

Fuq kollox, il-PSD 2 tagħmilha ċara[32] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

Għalhekk, il-banek jeħtieġ li jkollhom sistema ta' pagamenti robusta biżżejjed biex il-pagament ma jsirx jekk ma jkunx speċifikament awtorizzat mill-klijent/Ilmentatur. Il-banek ma jistgħux ma jerfgħux responsabbilità jekk iħallu toqob fis-sistemi tagħhom li permezz tagħhom il-frodist ikun jista', bla ma jkun hemm aktar involviment tal-klijent/Ilmentatur, 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.[33][34]

**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.

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

[32] Article 64 of PSD 2
[33] (EU) 2018/389 tas-27 ta' Novembru 2017 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[34] PSD 2 UE 2015/2366 Artikolu 68(2).

| | **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-Ilmentatur għandu jġorr 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-mudell isib li l-fatt li l-Ilmentatur ikkopera mal-frodist billi għaddielu kull informazzjoni li kienet meħtieġa biex jiġu approvati l-pagamenti inkluż b'mod partikolari l-*activation code* biex jinbidel id-*device* li fuqu hemm l-APP li tapprova pagamenti.

F'dan il-każ, hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jitnaqqaslu l-piż ta' negliġenza grossolana b'doża ta' 20%. Dawn il-pagamenti saru ftit ġranet wara li daħlet is-sistema *Instant Payments*. Din is-sistema għandha ħafna benefiċċji iżda għandha wkoll riskji li l-pagamenti jsiru b'mod kważi immedjat. Dan jitlob li s-sistema ta' monitoraġġ ta' pagamenti tal-banek jeħtieġ tiġi rfinuta biex toffri monitoraġġ '*real time*' għax jekk il-flus jilħqu jitilqu, diffiċli li xi *recall* jirnexxi kif huwa evidenti f'dan il-każ.

L-Arbitru qed inaqqas il-piż ta negliġenza tal-Ilmentatur b'20% għal din ir-raġuni:

> Opinjoni li diġà esprima f'deċiżjoni ta' każ ASF 116/2023 li meta jiġi rreġistrat *device* ġdid, irid isir proċess sħiħ ta' rikonferma mill-Bank li dan sar fuq talba ġenwina tal-klijent.
>
> F'dan il-każ, iżda, l-Arbitru jinnota li filwaqt li ma kienx hemm bidla tal-*mobile device* u l-istess numru baqa' rreġistrat mal-Bank, fil-proċess kien hemm bidla fis-*software token* li jawtorizza l-pagamenti.
>
> L-Arbitru jirrakkomanda li meta jkun hemm reġistrazzjoni ta' *software token* fuq *device* ġdid (li jkun jinvolvi wkoll *unenrolment* minn fuq id-*device* ta' qabel għax il-*mobile app* tista' tkun irreġistrata fuq *device* wieħed biss), għandu wkoll ikun hemm eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

> L-argument li l-pagamenti setgħu jsiru biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi u, għalhekk, hemm bżonn ta' konsiderazzjoni profonda biex filwaqt li jinżammu pagamenti b'xamma ta' frodi, ma niġux restrittivi b'mod li jiġu mblukkati 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.[35]

L-Arbitru ma jaqbilx mal-argument tal-Ilmentatur li on a *'risk-based approach'* dawn il-pagamenti kellhom karatteristiċi strambi biżżejjed biex il-Bank seta' issuspetta li ma kienx kollox normali, speċjalment rigward it-temp ta' madwar ftit minuti li matulhom saru tliet pagamenti atipiċi għall-istorja tal-kont.

L-ammonti, għalkemm atipiċi, kienu taħt il-limitu ta' pagamenti ta' €5,000 li l-Ilmentatur għażel għal pagamenti f'jum wieħed.

Qed ukoll jiġi skużat b'20% oħra għaliex ma ġiet ippreżentata ebda evidenza li l-Ilmentatur kien għamel pagamenti *online* bħal dawn fl-aħħar 12-il xahar, li huma differenti mill-pagamenti li l-Ilmentatur kien jagħmel lil terzi mill-*Mobile App*.

B'kollox, għalhekk, l-Ilmentatur huwa intitolat għal kumpens ta' 40% tat-telf li sofra mill-pagamenti frawdolenti li ġew iddebitati fil-kont tiegħu mal-Bank.[36]

**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' elf, seba' mija u tmenin ewro (€1,780).**

[35] Dan it-tip ta' sistema diġà qed jopera permezz ta' *3D Secure* f'każ ta' pagamenti bil-*card* lill-*merchants* għal xiri *online*.
[36] 40% ta' €4,450

**Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[37] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.** [38]

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

**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.

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

[38] [38] 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.