Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 033/2026

YU

('l-Ilmentatur')

vs

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

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

Seduta tal-15 ta' Ġunju 2026

L-Arbitru,

Ra l-Ilment[1] datat 12 ta' Diċembru 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €8,549.01[2] rigward tliet pagamenti li saru mill-kont li l-Ilmentatur għandu mal-BOV favur terzi li wara rriżulta li kien frawdolenti. L-Ilmentatur qed jitlob kumpens ta' €8,499.01 u jaċċetta li jsofri €50 kif provdut mir-regolamenti.

L-Arbitru ġew quddiemu diversi ilmenti ta' dan it-tip li filwaqt li jvarjaw fuq ċerti dettalji, fihom ħafna affarijiet komuni bejniethom:

- Il-pagament ikun għal ammont ġeneralment taħt il-€5,000 biex ma jinżammx minħabba li jeċċedi d-*'daily limit'* ta' pagamenti li jkun maqbul bejn il-Bank u klijent tat-tip *'retail'.*

[1]Paġni (P.) 1 - 10 b'dokumentazzjoni addizzjonali minn P. 11 - 46.
[2] L-ammount tal-pagament kien ta' €9700 (4700+3000+2000) iżda il-Bank irkupra €700.99+€450.

- Il-frodist jirnexxielu jippenetra b'mod frawdolenti il-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *e-mail.*

- Il-frodist jagħti *link* fil-messaġġ tiegħu u jistieden lill-klijent biex jagħfas fuq il-*link* biex jagħmel '*validation'* jew '*re-authentication'* tal-kont tiegħu.

- Minkejja diversi twissijiet[3] maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-bank ma jibgħatx *links* fil-messaġġi tiegħu, u li l-klijent għandu jikkomunika mal-bank biss tramite l-App u/jew il-*website* uffiċjali u dan permezz tal-kredenzjali li l-bank ikun ta lill-klijent, il-klijent b'nuqqas ta' attenzjoni jagħfas il-*link*.

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

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

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

- Fil-15 t'Ottubru 2025, fil-ħin ta' 20:30, l-Ilmentatatur xtara biljett tal-ajru tal-*KM Airlines* billi uża *BOV Gold Card* permezz ta' *Google Wallet*.[4]

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

[4] P. 40

- Ħames minuti wara, fil-ħin 20:35 rċieva SMS[5] fuq in-numru 99180001 li fuqu normalment jirċievi messaġġi mill-BOV. Dan il-messaġġ (li wara rriżulta li kien frawdolenti) kien jgħid:

  'New number has been added , if NOT authorised visit https://24x7-loginbov.com For further enquiries call +35621234821'.

- Kif għafas il-link daħal f'*website* li dehret identika għal dik ta' BOV u ġie mitlub jagħti n-numru tal-mobajl tiegħu. Ġie nfurmat li kienu ser jikkuntattjawh dalwaqt.

- Fil-ħin ta' 21:47, irċieva telefonata fuq l-istess numru, 99180001, fejn persuna femminili introdućiet ruħha bħala '*BOV agent'* kellmitu bil-Malti u qaltlu li kien sar attentat biex jeħdulu xi flus u talbitu jidħol fil-BOV Internet Banking biex isir '*security check'*. Daħal fl-*Internet Banking* bħas-soltu permezz tal-*USER ID* u l-*One-Time Password* (OTP) u '*BOV Agent'* qaltlu li s- *security check* kien għadda u li ser tkompli moniteraġġ u jerġgħu jikkuntatjawh filgħodu. Hemm intemmet it-telefonata.

- Irriżulta li fil-ħin ta' 21:54 daħallu wkoll SMS fuq *BOV Mobile* (distint minn dak 99180001) li infurmah:

  'Here is your activation code Please use it within 1 hour to activate your BOV Mobile APP:XNHGEm9'.

  L-Ilmentatur isostni li dan il messaġġ ma ndunax bih għax kieku kien jissuspetta li kien hemm frodi. Isostni li dan il-*code* ma daħħlux fil-*website* u ma kkomunikah lil ħadd.

- Minkejja dan jidher li l-is*cammer* uża l-*activation code* biex irreġistra l-*BOV mobile app* fuq *device* ikkontrollat minnha u b'hekk setgħet tagħmel il-pagamenti ilmentati bla ma jkun hemm bżonn aktar interventi min-naħa tal-Ilmentatur. Billi l-*BOV Mobile App* tista' tkun fuq *device* wieħed biss bilfors li kien hemm *unenrolement* minn fuq id-*device* tal-Ilmentatur u *enrolment* fuq device tal-is*cammer.*

[5] *Ibid*.

- Imbagħad saru it-tliet pagamenti[6] ilmentati:
    - €4700 *instant SEPA payment* għal kont *Revolut Ireland* fil-ħin ta' 22:23 tal-15 t'Ottubru 2025
    - €2,000 *instant SEPA payment* għal kont *AIB Ireland* fil-ħin ta' 01:54 tas-16 t'Ottubru 2025
    - €3,000 *instant SEPA payment* għal kont *AIB Ireland* fil-ħin ta' 02:09 tas-16 t'Ottubru 2025.
- Saru wkoll transferimenti mill-kont tal-mara tal-Ilmentatur għall-kont tal-Ilmentatur biex ikun hemm fondi biżżejjed biex isiru l-pagamenti ilmentati. L-Ilmentatur qal li saru żewġ attentati oħra biex isiru transferimenti li ma għaddewx għax jidher li ma kienx hemm flus biżżejjed.[7] [8]
- Sar rapport lill-pulizija fis-16 t'Ottubru 2025 fil-ħin ta' 09:07,[9] u minn dan ir-rapport jirriżulta li SMS għall-pagamenti ilmentati waslu fil-ħin ta' 07:03 u minn hemm induna bil-frodi.
- Il-każ ġie rrapportat lil BOV qabel 07:38 tas-16 t'Ottubru 2025 u l-BOV immedjatament fetaħ *recalls* u dawn ipproduċew €700.99 dakinhar stess u €450 fit-30 t'Ottubru 2025.[10]

L-Ilment

L-Ilmentatur qed jitlob kumpens ta' €8,499.01, kif ġie spjegat qabel.

L-argument prinċipali tal-Ilmentatur huwa li huwa qatt ma kkomunika l-*activation code* lil ħadd, anzi jsostni li lanqas biss kien induna bl-SMS. U għalhekk huwa ma jistax jifhem kif il-frodist seta' għamel il-pagamenti ilmentati li huwa ma awtorizzax u li lanqas kixef l-*Activation Code* li bih il-frodist seta' jikkontrolla l-*BOV mobile App* u jagħmel il-pagamenti bla ma huwa japprovahom.

[6] Ħinijiet meħuda mil-*logs* ta' BOV p. 59
[7] P. 138
[8] P. 143 juri li wara l-aħħar pagament kien fadal €2,160.14 fil-kont. Aktar probabbli li ġew imwaqqfa peress li intlaħaq il-limitu ta' trasferimenti li jsiru f'ġurnata ta' €5,000. L-ewwel pagament ta' €4,700 għadda fil-15 u żewġ pagament għal €5,000 għaddew fis-16 t'Ottubru 2025.
[9] P. 36 -38
[10] P. 95 - 102

BOV offrewlu kumpens ta' 60% iżda huwa ma aċċettax u qed jinsisti għal irkupru sħiħ ħlief għal €50.

Fl-ilment ikkwota diversi ksur tar-regolamenti taħt id-direttiva tal-EU magħrufa bħala PSD 2[11] u peress li jsostni li huwa la kien negliġenti u lanqas kien awtorizza l-pagamenti jinsisti li għandu dritt għal rimbors sħiħ ħlief għal €50.

Fl-Ilment tiegħu qal li l-Bank għandu jġorr il-piż ta' dan il-frodi għal dawn ir-raġunijiet:

1. *"Failure to prevent and detect fraudulent transactions*

   The Bank failed to implement effective real-time or near-real-time transaction monitoring, despite regulatory obligations under PSD2, the EBA Guidelines on Fraud Risk Management, and the Instant SEPA Credit Transfer framework. The transactions executed were unusual for my account profile and should have triggered immediate fraud alerts. No preventative action was taken before the funds were irreversibly transferred.

2. *Failure to promptly notify me of Instant SEPA transactions*

   The Bank delayed sending SMS notifications for Instant SEPA payments until the following morning, despite the transactions being executed within seconds. This delay prevented me from taking timely action to mitigate losses and is inconsistent with the heightened notification obligations associated with instant, irrevocable payments.

3. *Processing transactions without my consent*

   A total of six transactions were executed without my authorisation. I did not provide explicit consent for any of these transactions. Under PSD2, the Bank bears the burden of proving that valid consent and authentication were obtained. No such proof has been provided.

4. *Breakdown of authentication and security controls*

   An Activation Key was generated without my completion of the required Signature 1 (challenge code). This indicates a serious failure in the Bank's

[11] EU Directive 2015/2366

authentication and security mechanisms. The Bank has not explained how this was possible nor demonstrated that its systems functioned correctly.

5. *Lack of transparency and inadequate investigation*

   The Bank provided only minimal information regarding its internal investigation and relied on unsubstantiated references to audit logs without providing technical evidence or a clear explanation. This lack of transparency prevents independent verification and raises concerns regarding possible system vulnerabilities.

6. *Failure to safeguard my account and application access*

   As a result of these failures, the fraudster was able to install the "BOV Mobile App" on another device and gain full control of my accounts. This outcome demonstrates that the Bank did not adequately safeguard my credentials, devices, or account access as required by PSD2."[12]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[13] tagħhom, il-BOV qalu:

"The Bank's Point of View

1. *Whereas the pecuniary loss claimed relates to the three Instant SEPA payments executed from (The Complainant's) account. The Complainants' own "Financial Loss and Remedy Sought" quantify the outstanding loss and request reimbursement in (Co name only. Mrs. XXX's account activity forms part of the factual sequence but does not constitute a separate head of loss. Thus, the Bank respectfully submits that her role is that of an interested party and not claimant;*

2. *Whereas according to the Bank's records*[14]*, the three disputed payments were duly processed through the Bank's mobile banking using valid credentials and authenticated successfully;*

[12] P. 6
[13] P. 50 – 58 u dokumenti annessi p. 59 - 135
[14] Doc. A

3. *Whereas the logs in question show a complete and uninterrupted session flow, confirming that the transactions were initiated and authorised by the user. The transactions were authorised on the 15th and the 16th October 2025 at 22:23, 01:54, and 02:09;*

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

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

5. *Whereas the Bank's General Terms and Conditions[15] stipulate 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 correctness of the information given."[16]*
>
> *"You shall be considered to have given payment consent when […] you confirm authorisation of any Payment Instructions*

[15] Doc. B
[16] Doc. B, 2.22 'Any Instruction to Us', Page 24.

through our Channels using your BOV Channel Credentials. "[17]

6. *Whereas immediately upon notification on the 16th October 2025, the Bank initiated recall requests for all three payments*[18] *whereby partial returns of €700.99 and €450 were received and credited to (Complainant's) account. The beneficiary institutions declined the outstanding balances on the basis that no or insufficient funds remained;*

7. *Whereas without prejudice to the above, if (Complainant) is alleging that these transactions were not authorised by him, then the Bank is still not obliged to refund him, since even if he did not have the intention to approve a payment, he still performed the necessary actions which enabled its' approval. In this respect the Bank refers to article 45 of Directive 1 of the Central Bank of Malta, particularly to the article entitled 'Obligations of the payment service user in relation to payment instruments and personalised security credentials' which provides the following:*

> *"(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"*

8. *Whereas article 50(1) of the Directive provides that:*

[17] Doc. B, 2.18(q)(ii), Page 14.
[18] Doc. C, Doc. D, Doc. E

> *"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".*

9. *Whereas (Complainant's) conduct, engaging with an unsolicited link, disclosing authentication elements, and enabling the activation/ takeover of the mobile token subsequently used to authorise the payments, contravenes the security obligations in the Bank's General Terms and Conditions which require the customer to:*

> *"[…] 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".*[19]

10. *Whereas as a voluntary user of the internet banking service, (Complainant) knows or ought to have known that this service can only be accessed from the Banks' website or from the BOV Mobile App. Whereas the Bank never before requested (Complainant) (or any other customer) to access their internet/mobile banking from a link in a SMS, because it has the adequate systems for this service to be accessed. In fact, the Bank warns customers to be careful what information they disclose, particularly on links;*

11. *Whereas, prior to the incident, the (Complainant's) registered number (79309263) received ten anti-fraud SMS warnings between the 11th November 2023 and the 4th September 2025, consistently instructing*

[19] Doc. B, 2.23 'Security Notice', Pages 24 to 25.

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

(i) *11th November 2023 – "SPOT THE SCAM. Please be vigilant. BOV never sends links by SMS. DONOT click on any links and do not provide personal information, passwords or card details."*

(ii) *5th February 2024 – "SPOT THE SCAM. BOV will NEVER send you an sms/email with web links that ask you to provide card details, PIN, verification codes or on-line banking passwords."*

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

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

(v) *22nd October 2024 – "SPOT THE SCAM. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests."*

(vi) *20th January 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links."*

(vii) *15th April 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links."*

(viii) *15th July 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links."*

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

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

12. *Whereas the above-mentioned warnings are part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. Besides these SMSs, the Bank also publishes information regarding scams to which customers may be vulnerable to. In fact, in May 2023 the Bank published a page entitled 'Spot the Scam: Bank impersonation Scams' which explains that scammers may use a technique called 'Spoofing' where "scammers manipulate caller ID or email addresses, so they appear to be from reputable companies such as banks. It can be tough to identify and misleading because it makes people think they are communicating with a trustworthy source. Ask yourself what a bank will NEVER ask you for over the phone.''[20] It also explains what personal details such scam may ask for which indicates that the communication is not genuine;*

13. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams. 'Doc. G1' shows a comprehensive list of the posts made by the Bank in 2024. Moreover, the Bank coordinated TV appearances where Bank employees explained what spoofing is and how to identify it. These programmes aired on the 10th of April 2023, 27th of April 2023 and September 2023. The Bank also published multiple newspaper articles, on various media as can be seen from the attached list marked as 'Doc. G2';*

14. *Whereas besides information provided by the Bank, there are various entities which make educational campaigns in order to raise awareness concerning fraud which may be directed to consumers of financial services. These include the Malta Financial Services Authority (MFSA) who provide information on how a person can identify a system where a payment is to be made. Of particular relevance is the page*

[20] Doc. F

'The MFSA's Guide to Secure Online Banking' which provides the following:

> *Use the genuine internet website of the bank. Never access the bank's website through links contained in emails or SMS, unless you are sure of the identity of the sender. It is always best to access the bank's website by typing in the web address, as provided by the bank, directly in the browser.*
>
> *Follow the information and guidelines provided by your bank on how to use digital banking services.*
>
> *Take the necessary time to read the terms and conditions provided by your bank.*
>
> *Ensure that you always protect all personal details such as card details, passwords, and other confidential data to access the bank's online platform or mobile app.*

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

16. *Whereas, in breach of his obligations under Article 45(2) of CBM Directive No. 1 and as reinforced by the Bank's General Terms & Conditions, (Complainant) failed to take all reasonable steps to keep his personalised security credentials safe, instead engaging with a link and disclosing authentication elements to a third party; this conduct is further aggravated by the fact that he worked at the Bank for thirty-eight (38) years (indicating professional familiarity with banking security) and had received ten pre-incident anti-fraud SMS warnings, all of which reinforces the Bank's submission that his actions meet the threshold of gross negligence;*

I. ***Conclusion***

17. *For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and law.*

18. *Chapter 555 of the Laws of Malta vests the Honourable Arbiter with the authority to decide a case on the basis, inter alia, of the Complainants' legitimate expectations and what they deem fair and equitable in the circumstances of the case. The Bank very respectfully submits that such element of fairness and a customer's legitimate expectations are founded and pivot on a balance between rights and obligations whereby a customer most certainly has rights but also an inherent interest and obligation to faithfully abide with all terms, conditions as well as guidelines issued by the Bank, as these are ultimately intended to serve and protect the customer.*

19. *The Bank reserves the right to bring oral and documentary evidence in order to substantiate the defences raised in this reply, as well as to make submissions both verbally and in writing pursuant to the provisions of Chapter 555 of the Laws of Malta.*

20. *The Bank reserves all rights/actions pertaining to it at law and respectfully requests the Arbiter to reject and dismiss the complaint's claims."*[21]

Seduti

Fl-ewwel seduta tas-16 ta' Marzu 2026, l-Ilmentatur spjega l-każ tiegħu kif diġà riprodott hawn fuq.

Meta l-Arbitru staqsih għandux idea kif il-frodist skopra l-*activation code* la huwa lanqas biss kien induna bl-SMS, l-Ilmentatur qal:

"***Ngħid li ma nafx. Jiena bqajt insostni u nistaqsi l-activation code fejn qiegħed? Għax bqajt nimmoniterja n-numru 9919 8001.***

[21] P. 51 - 58

Jiena nibqa' nsostni mija fil-mija li l-activation code irċevejtu fuq il-BOV Mobile tal-mobile tiegħi u mhux biss ma tajtux lill-frodist biex ikun jista' jaqleb il-mobile fuqu, imma lanqas indunajt bih."[22]

Fil-kontroeżami kompla jgħid:

"***Naqbel li l-ewwel SMS li irċevejt kien card alert normali li kkonferma ħlas li jien għamilt ta' €531.06 li ma kien fih l-ebda link u ma talab l-ebda azzjoni ta' sigurtà. Kien in-normali li nirċievu aħna s-soltu.***

Qed jingħad li wara irċevejt SMS ieħor separat li kien fih il-link u jien għafast fuq dan il-link. Ngħid li hekk hu.

Qed jingħad li jien din rajtha suspettuża. Ngħid li hekk hu."[23]

Fit-tieni seduta li nżammet fil-21 t'April 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 deheru 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:

"Nispjega li biex inti tagħmel request għal Activation Code, tista' tmur fi branch, jew iċċempel il-Customer Service Centre jew inkella tilloggja inti stess fl-Internet Banking bis-security features kollha u tagħmel request għal Activation Code.

Dment li jiġi rikjest l-Activation Code, jintbagħat permezz ta' SMS fuq il-mobile number tal-klijent u, mbagħad, tista' tiġi rreġistrata app ġdida.

Ngħid li, ovvjament, b'xi mod jew ieħor, il-klijent kellu diġà konoxxenza ta' dan l-Activation Code.

Jekk lill-frodist ġie kkomunikat il-Login ID u l-One-Time Password,dan hemmhekk illoggja fl-Internet Banking. U s'hemmhekk ma jiġri xejn għax

[22] P. 138
[23] P. 138 - 141

s'hemmhekk kulma qed jara huwa l-bilanċ. Imma, mbagħad, mar fil-function tal-Activation Code u għamel Activation Code request u biex titla' din l-Activation Code request trid tiġi ffirmata, jiġifieri jrid ikun hemm Transaction Signing bis-Signature 1. Hekk kif jitla', jintbagħat SMS fuq il-mobile number tal-klijent.

Nikkonferma li f'dan il-każ, il-pagamenti ġew awtentikati.

Ngħid li biex jiġi awtentikat pagament, trid tmur fit-Third Party Screen, timla d-dettalji kollha imbagħad tmur fit-Transaction Signing, tiffirma t-transactions u jitilqu.

F'dan il-każ kienu instant payments.

Nikkonferma li l-bank qatt ma jibgħat links jew jitlob lill-klijenti biex jagħtu kredenzjali bħall-One-Time Password jew Activation Codes waqt telefonata jew permezz ta' SMS.

Ngħid li l-bank jibgħat on a regular basis SMS alerts lill-klijenti tiegħu fejn javżahom fuq frodi li jkunu għaddejjin biex ma jagħtux informazzjoni, bħal Login ID to third parties.

L-Arbitru jgħid li l-pagamenti saru b'token li nbidel ftit wara li ħareġ dak il-messaġġ tal-Activation Code.

Ngħid li iva, is-serial number kien inbidel qisu ġie rreġistrat device ġdid, bħal meta titlef il-mobile jew tibdel il-mobile."[24]

Fil-kontroeżami, ix-xhud ikkonferma li:

"Jien nibqa' nsostni li l-Activation Code li ntbagħat fuq il-mobile irreġistrat tal-Ilmentatur kieku b'xi mod dan ma ġiex ikkomunikat lill-frodist, kieku l-pagamenti ma setgħux isiru."[25]

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head ta' Transaction Monitoring and Pro-active Analysis* tal-BOV, li fuq dan il-każ qal:

"F'dan il-każ qed nitkellmu fuq tliet tranżazzjonijiet li telqu mill-bank fis-16 t'Ottubru 2025. Tranżazzjoni minnhom kienet ta' €3,000; oħra ta' €2,000 u l-oħra kienet ta' €4,700.

[24] P. 170
[25] P. 171

It-tranżazzjonijiet ta' €3,000 u €2,000 marru ġo kont f'AIB Bank, l-Irlanda.

It-tranżazzjoni ta' €4,700 marret ġo kont fir-Revolut, l-Irlanda.

Ngħid li s-sistema, kemm fil-Pre- u kemm fil-Post-, on a risk-basis approach, ma ħassitx li kellha tifflaggja dawn it-tliet tranżazzjonijiet. Ma kien hemm xejn li jabbinahom ma' xi ħaġa illeġittima jew xi financial crime. U għaldaqstant, is-sistema ma kellhiex għalfejn twaqqafhom biex jiġu analizzati minn human analyst.

Ngħid li dawn it-tranżazzjonijiet marru l-Irlanda li huwa meqjus bħala pajjiż low risk jurisdiction; u l-ammonti, jekk inħarsu lejhom in a holistic way, huma modesti wkoll meta mqabblin mat-tranżazzjonijiet.

Ngħid li l-klijent kien għamel dawn it-tranżazzjonijiet biss cross border imma bħala ammonti, meta tiġi biex tagħmel transaction kemm għal Malta u kemm għal barra minn Malta, tintuża l-istess proċedura – tidħol fis-sistema u kemm iddaħħal id-dettalji u s-sistema fiha nnifisha tagħżel fejn trid tmur it-tranżazzjoni. Dak in the background imma a front-facing user qed jagħmel l-istess proċess kemm biex jibgħat tranżazzjoni barra minn Malta u kemm jekk qed jibgħat tranżazzjoni lejn benefiċjarju lokali.

Ngħid li dawn it-tranżazzjonijiet nistgħu inqisuhom within the profile of the client għar-raġuni li kemm f'Ġunju tas-sena 2023 u anke jekk immorru lura għal Jannar tas-sena 2021, il-klijent kien għamel żewġ tranżazzjonijiet li kellhom l-ammonti viċin, waħda ta' €3,501 u l-oħra ta' €1,917 li marru lejn benefiċjarji f'Malta."[26]

Fil-kontroeżami qal:

"Mistoqsi għalfejn ma telgħux red flags għat-tranżazzjonijiet li għamel l-Ilmentatur għal minn Malta u b'dawk l-ammonti meta mhumiex fil-profil tiegħu, ngħid li ma jfissirx li għax qatt m'għamilt tranżazzjoni għal barra minn Malta ma jkollokx bżonn jew jiġi dak il-bżonn li tagħmel tranżazzjoni barra minn Malta u tistenna li l-bank ma jimxix mar-regoli stabbiliti u guidance li nirċievu mingħand ir-regolatur li nwaqqfu kull tranżazzjoni għax il-klijent abbażi li qatt m'għamel tranżazzjoni għal barra aħna nwaqqfu dejjem l-ewwel tranżazzjoni li ssir mill-klijent għal barra minn Malta.

[26] P. 172 - 173

Din mhijiex fil-guidance li nirċievu mir-regolatur u mhijiex il-guidance u regolamenti li nsegwu on a risk-basis approach, skont il-liġijiet Maltin u d-direttivi li joħorġu mill-Ewropa fuq money laundering. Jiġifieri fl-ebda guidance li jirċievi l-bank bħala subject person ma jiġi mitlub li għax klijent għamel l-ewwel tranżazzjoni barra minn Malta, bilfors irridu nwaqqfu t-tranżazzjoni.

Hemm diversi kriterji li jridu jittieħdu in konsiderazzjoni fit-Transaction Monitoring u dawn huma skont ix-scenarios li hemm skont il-guidelines u r-regolamenti u liġijiet li aħna rridu nsegwu bħala subject persons.

Mistoqsi naqblix li hawn intużat l-InstaSEPA system, ngħid li naqblu.

Mistoqsi naqbilx li din bdiet tintuża fl-1 t'Ottubru, ngħid li mill-bidu t'Ottubru imma ma nafx il-ġurnata eżatt.

Qed jingħad li dawn kienu l-ewwel ftit ġranet li l-bank kien qed joffri din il-function lill-klijenti tiegħu.

Ngħid iva, biex nobdu d-direttiva."[27]

Sottomissjonijiet Finali

Fis-sottomissjonijiet finali, il-partijiet bażikament sostnew il-pożizzjoni tagħhom kif esibita fl-ilment, fir-risposta u fix-xhieda waqt is-seduti**.**

L-Ilmentatur kompla jisħaq li la huwa ma ta l-*Activation Code* lil ħadd, u lanqas biss kien induna bih, allura sta għall-Bank jispjega kif l-i*scammer* seta' jirreġistra l-BOV Mobile APP fuq *device* tiegħu u jibqa' sejjer jagħmel it-tliet pagamenti ilmentati daqslikieku kien qed jagħmilhom huwa stess.

Isostni li dawn il-pagamenti ma humiex awtorizzati bi *Strong Customer Authentication* (SCA) skont id-direttiva PSD2 u, għalhekk, dawn huma pagamenti mhux awtorizzati li huwa ma għandux ikun responsabbli għalihom.

Jakkuża wkoll lil BOV li naqas fl-obbligi tiegħu fil-moniteraġġ tal-pagamenti għaliex il-każ jittratta:

[27] p. 173 - 174

"The disputed transactions consisted of:

- *three Instant SEPA Payments;*
- *executed within a short timeframe during the night;*
- *directed to foreign beneficiaries; and*
- *inconsistent with my recent account behaviour.*

In the twelve months preceding the fraud, I had not executed transactions of this nature.

The Bank is therefore invited to explain how these transactions could reasonably have been classified as being 'within the customer profile'.

Reference is also made to PSD2 Article 68 and the requirement for payment service providers to maintain effective fraud prevention and transaction monitoring mechanisms based on relevant and recent behavioural analysis.

Reliance on isolated transactions dating back three to five years cannot reasonably justify treating the disputed transactions as normal customer behaviour."[28]

Jakkuża wkoll lil BOV li dam wisq biex jibgħat notifika b'SMS dwar il-pagamenti, għax kieku kien jintebah mill-ewwel u kien jevita li jsiru t-tieni u t-tielet pagament.[29]

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.

[28] P. 179
[29] *Ibid*.

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*[30] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha

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

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

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

Deċiżjoni

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

Qabel ma japplika l-mudell għaċ-ċirkostanzi partikolari ta' dan il-każ, l-Arbitru irid jasal għal ġudizzju dwar il-bilanċ tal-probabbilita' tal-argumenti opposti tal-partijiet dwar kif l-*Activation Code*, li mingħajru l-iscammer ma setax jawtorizza pagamenti, ġie a konoxxenza tal-frodist. Irid jiġġudika jekk kinetx mgħoddija

[31] Article 64 of PSD2
[32] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[33] PSD 2 Eu 2015/2366 Artiklu 68(2).

mill-Ilmentatur billi daħħal l-informazzjoni fil-*website* frawdolenti jew ikkomunikah verbalment, jew jekk kif isostni l-Ilmentatur, li dan l-*Activation Code* lanqas biss kien induna bih u, għalhekk, sta għal BOV jispjega kif l-i*scammer* sar jaf bih.

Fl-assenza ta' spjega aktar kredibbli, l-Arbitru jara probabbilità li kien l-Ilmentatur li b'xi mod, għalkemm b'aljenazzjoni u mhux b'intenzjoni, ikkomunika l-*Activation Code* lill-i*scammer.*

L-Arbitru jieħu kunsiderazzjoni li persuna bi 38 sena esperjenza fil-Bank u li rċieva b'mod regolari twissijiet biex ma jagħfasx *links* li jirċievu f'SMS anke jekk jidhru li ġejjin mill-Bank, ma kellux jaqa' biex jagħfas il-*link* fuq l-SMS frawdolenti ħlief b'aljenzzjoni ovvja.

Ma hemmx spjega oħra għalfejn għafas din il-*link* għax ***'ġietni kurżità nara eżatt x'ġara'.***[34]

Persuna bl-esperjenza tal-Ilmentatur mhux biss messu ma jagħfasx il-*link* u jagħti n-numru tal-mobajl (li kien ġa rreġistrat mal-Bank) iżda messu ntebaħ mill-ewwel li din kienet frodi u seta' ċempel lill-*contact centre* tal BOV biex jikkonferma magħhom li kienet frodi. Trid tkun altru aljenat biex temmen li l-Bank irreġistra numru ġdid bla ma int tkun għamilt ebda talba f'dan ir-rigward.

Għalhekk l-Arbitru jasal għall-konkluzjoni fuq bażi ta' probabbilità akbar u fl-assenza ta' xenarju aktar kredibbli, li kien l-Ilmentatur li baqa' jikkopera b'aljenazzjoni biex mhux biss għafas il-*link* frawdolenti iżda ta poter lill-i*scammer* biex jawtorizza l-pagamenti daqslikieku kien awtorizzahom hu stess.

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

[34] P.136

	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 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-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.

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

Għalhekk l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jitnaqqaslu l-piż ta' negliġenza grossolana b'doża ta' 50%, jiġifieri 30% aktar mill-20% normalment spjegati fil-mudell.

Dan huwa każ fejn il-frodist mhux biss bagħat SMS qarrieq iżda sostna l-kredibbilità tal-SMS permezz ta' telefonata konvinċenti minn persuna titkellem bil-Malti li tat informazzjoni li l-Bank biss seta' jkollu.

L-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat minn xi ħadd li jippersonifika b'mod espert lill-Bank permezz ta' telefonata '*live*', allura, l-SMS bil-*link* frawdolenti tidher anqas suspettuża minkejja t-twissijiet li l-Bank kien ħareġ.

F'dan l-aġġustament, minħabba ċirkostanzi speċjali, l-Arbitru qed jieħu wkoll kunsiderazzjoni ta' dawn il-fatturi:

A. 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, iżda 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 eżercizzju 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.[35]

B. Taħt is-sistema ġdida ta' *Instant Payments*[36] li daħlet fis-seħħ fid-09 t'Ottubru 2025, il-banek mistennija jkollhom sistema ta' moniteraġġ ta' pagamenti fuq bażi instantanja (*real time*) u li tkun sensittiva għal pagamenti li b'mod sostanzjali ma jkunux konsistenti mal-istorja tal-klijent.

Dawn il-pagamenti kellhom karatteristiċi strambi biżżejjed biex il-Bank seta' issospetta li ma kienx kollox normali speċjalment rigward il-ħin li fih saru l-aħħar żewġ pagamenti lill-istess persuna f'ħin ta' 15-il minuta deskritti bħala rigal (*gift*).

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

[36] *Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro*

C. Fil-futur qarib (2027/2028), tidħol fis-seħħ leġiżlazzjoni ġdida permezz tal-PSR u PSD3[37] li fost provvidementi ġodda, jobbligaw lill-banek biex f'każ ta' pagamenti frawdolenti fejn ikun hemm persunifikazzjoni tal-bank mill-frodist, il-bank jkun obbligat li jagħmel rifużjoni sħiħa lill-vittma.

   L-Arbitru jqis li l-banek għandhom jipprepaw ruħhom kemm jista' jkun malajr għal dan it-tibdil fix-xenarju regolatorju u, b'hekk, bil-mod il-mod qed iżid id-doża ta' ċirkostanzi speċjali meta jkun hemm frodi permezz ta' persunifikazzjoni, speċjalment jekk issir b'aktar minn kanal wieħed bħal dan il-każ (SMS u telefonata).

L-Arbitru qed ukoll jiskuża l-Ilmentatur b'20% għax ma ġiet ipprovduta l-ebda evidenza li li kien għamel xi pagament simili fit-12-il xahar qabel seħħ dan il-każ.

B'kollox, għalhekk, qed jiġi intitolat għal kumpens ta' 70% tat-telf li sofra minn pagamenti frawdolenti li ġie ddebitat lill-kont tiegħu.[38]

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' ħamest elef, disa' mija u erbgħa u tmenin ewro, punt tlieta wieħed (€5,984.31).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[39] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[40]

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

Fl-aħħarnett, l-Arbitru jirreferi għal rapporti mhux konfermati li l-pulizija irnexxielhom jimblukkaw xi fondi misruqa mill-frodisti u, għalhekk, eventwalment jista' jkun hemm xi rkupru minn dan is-sors.

[37] *https://financialregulations.eu/blog/psd3-psr-eu-payment-services-guide*

[38] 70% ta €8,549.01 = €5,984.31

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

[40] [40] 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.

Jekk jirriżulta rkupru bħal dan, biex ma jkunx hemm possibilità ta' arrikkament inġustifikat, l-Arbitru jordna li l-flus ta' xi rkupru jiġu allokati bl-istess mod kif ġie allokat it-telf f'din id-deċiżjoni, jiġifieri 70% għall-BOV u 30% għall-Ilmentatur.

_____

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

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

Dritt ta' Appell

Id-Deċiżjoni tal-Arbitru legalment torbot lill-partijiet, salv id-dritt ta' appell regolat bl-artikolu 27 tal-Att dwar l-Arbitru għas-Servizzi Finanzjarji (Kap. 555) ('l-Att'), magħmul quddiem il-Qorti tal-Appell (Kompetenza Inferjuri) fi żmien għoxrin (20) ġurnata mid-data tan-notifika tad-Deċiżjoni jew, fil-każ li ssir talba għal kjarifika jew korrezzjoni tad-Deċiżjoni skont l-artikolu 26(4) tal-Att, mid-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-Ilmentatrici/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.