Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 043/2026

RB

('l-Ilmentatur')

vs

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

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

Seduta tal-15 ta' Lulju 2026

L-Arbitru,

Ra l-Ilment[1] datat 27 Jannar 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €2,450.90 rigward żewġ pagamenti, li saru mill-kont li l-Ilmentatur għandu mal-BOV, favur terzi li wara rriżulta li kien frawdolenti.

BOV offrew li jirrifondu 70% tat-telf iżda l-Ilmentatur offra li jaċċetta biss telf nominali ta' €200 u għalhekk jitlob kumpens ta' mill-anqas €2,250.90.[2]

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

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

[1] Paġni (P.) 1-10 b'dokumentazzjoni addizzjonali minn P. 11 - 61
[2] P. 13

- 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:

---

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

- Fil-5 ta' Settembru 2025, fil-ħin ta' 11:48, l-Ilmentatur ċemplulu minn fuq numru 991800001[4] u mara titkellem bil-Malti qaltlu li kienet mill-*Customer Service* tal-BOV. Qaltlu li jidher li matul il-lejl saru żewġ tranżazzjonijiet fuq il-kont tiegħu li jidhru suspettużi u, għalhekk, BOV ibblokkjaw il-BOV App biex jipproteġuh milli jsiru tranżazzjonijiet mhux awtorizzati. Għalhekk qaltlu li riedet tgħinu ħalli l-BOV App tiġi restawrata.

  Taha il-OTP (One-Time Password) li talbitu[5] u qaltlu li ser jirċievi messaġġ mill-BOV.

- Fil-ħin ta' 11:52, jidħol messaġġ mill-BOV

  > *"Here is your activation code. Please use it within 1 hour to activate your BOV Mobile APP: ls39shl0"*.[6]

  Dan il-messaġġ kien wieħed ġenwin mill-BOV u l-Ilmentatur qal li

  > *"there was no reason to doubt the authenticity and source of this message."*[7]

- Il-*code* ikkomunikah lill-persuna li kienet ċemplitlu u din infurmatu li kien hemm erba' pagamenti u qaltlu jżur il-fergħa tal-BOV għal aktar informazzjoni. Ftit wara, irċieva SMS mill-BOV jinfurmawh dwar tliet pagamenti li saru ta' €1,000.81, €1,500.19 u €950.71.

- Huwa ċar li meta l-Ilmentatur taha l-OTP, ippermetta lill-frodista tidħol fil-kont tiegħu u tara l-bilanċi. Imbagħad, użat is-sistema tal-*Internet Banking* biex jintalab *activation code* ħalli l-BOV *Mobile App* tiġi *unenrolled* minn fuq il-*mobile* tal-Ilmentatur għal fuq *device* tal-frodista u b'hekk setgħet tawtorizza pagamenti li f'għajnejn il-Bank dehru pagamenti approvati mill-Ilmentatur.

- Wara dan saru rapporti mal-Pulizija[8] u mal-fergħa tal-BOV Naxxar li infurmawh li l-Bank kien imblokka l-pagament ta' €1,000.81 u r-raba' pagament ta' GBP £1,000.41, iżda żewġ pagamenti ta' €1,500.19 u

[4] Dan in-numru jixbaħ in-numru 99180001 li l-Bank kien jibgħat SMS notifiki fuqu.
[5] L-OTP seta' jinġieb biss mill-BOV APP u seta' jinduna li din ma kinetx blokkata.
[6] P. 27
[7] P. 3
[8] P. 35 - 37

€950.71 kienu laħqu għaddew u, għalhekk, kellu jsir *recall* biex jipprovaw jiġu rkuprati.

Fid-9 ta' Settembru 2025, ġie nfurmat li r-*recalls* ma rnexxewx.

L-Ilment

L-Ilmentatur argumenta:

"Throughout this process, I consistently maintained that

- *I did not press a link to any attachment*
- *I neither inputted my User ID, nor divulged this information to the caller. I am prepared to support this statement by an affidavit*
- *Hence my User ID and my personal mobile number could have either been obtained through collusion with bank staff or through penetration of BoV's IT and fraud prevention systems.*
- *I did not request an Activation Code. The fraudster/s success in triggering this request demonstrate complete failure of the Bank's security system as this would normally require the user to input the secret 15-digit code and/or change the user's mobile number on the 24*7 BoV's internet Banking*
- *The fraud was enabled by the Bank's systems allowing activation of the BoV Mobile App and execution of payments without any effective safeguard to prevent third-party misuse.*
- *Despite that APS Bank had corrected this deficiency subsequent to Case 116/2023 it is incomprehensible that no action had been taken by BoV to confirm payment instructions with me following a new BOV App set up.*
- *I was manipulated by social engineering (vishing) carried out by a fraudster impersonating a Bank of Valletta customer service agent;*
- *I did not authorise any of the four payments;*
- *Whereas I never made any payments beyond our shores, in a period of a few minutes the fraudster/s succeeded to effect four payments*
- *The Bank's Transaction Monitoring was completely deficient and ineffective given that the reasons behind two payments were related to "Farming" a complete mismatch with my Profile considering that I work in a bakery. This alone ought to have triggered immediate suspicions on the*

authenticity of the payment instructions and block the payment process pending clarification/confirmation from my end.

- *The front office staff at Naxxar branch was not trained to deal with fraud issues whereas the branch management acted very slowly thus losing precious time to request immediate Recall of Funds resulting in this being requested four days later (owing to weekend and intervening public holiday).*

The fraudster was able to:

(a) successfully spoof a phone number resembling a Bank of Valletta customer service line;
(b) possess illegitimately details of my User ID and mobile number
(c) Trigger or exploit the app re-activation process in a manner that allowed immediate execution of payments without my involvement.

At no point prior to the execution of the disputed payments did I:

- *Intend to authorise any payment;*
- *Know that I was interacting with a fraudster;*
- *Receive a clear and specific warning that the One-Time Password and activation code must never be communicated to any third party, including alleged Bank staff.*

The SMS containing the activation code originated from the same legitimate BoV sender ID as previous genuine banking communications, thereby reinforcing the belief that the interaction was authentic.

I further note that

- *The Bank claims the payments were authorised through Strong Customer Authentication (SCA);*
- *However, SCA in this case was obtained through deception and impersonation, not through my free and informed consent.*
- *Despite multiple representations, the Bank has taken the position that liability rests with me on the basis that I shared the Login One-time Password and by relaying the activation code to the fraudster ignoring*

completely my assertion that I did not input my User ID. authentication credentials.

- *The bank's authentication, monitoring, and fraud-prevention systems completely failed. I refer to Directive (EU) 2015/2366 and, in particular, Articles 64, 72, 73 and 74.*
- *Under Article 64, a payment transaction is authorised only where the payer has given consent in the form agreed with the payment service provider. Any transaction executed without such specific consent constitutes an unauthorised payment transaction.*
- *Pursuant to Article 72, where the payer denies having authorised a transaction, the burden of proof lies with the payment service provider to demonstrate not only authentication, but also that the transaction was not affected by a technical breakdown or other deficiency of the service provided. The mere use of authentication credentials does not discharge this burden where system vulnerabilities permit a fraudster to generate or manipulate authorisations without the payer's further involvement. Yet, despite that BoV informed me that the User ID was inputted the bank official present in our meeting of the 12th November was unable to provide evidence through which IP address my User ID was inputted.*
- *In accordance with Article 73, in the case of an unauthorised payment transaction, the payer's payment service provider is required to refund the amount immediately.*
- *Article 74 limits any potential payer liability strictly to cases involving the payer's fraud or gross negligence. Where the transaction results from weaknesses, deficiencies, or design flaws in the PSP's systems enabling a fraudster to effect a specific authorisation without the payer's active consent, the payer bears no financial liability.*
- *Consequently, under Article 73, a payment service provider cannot evade responsibility by relying on the appearance of authorisation if such authorisation was made possible solely due to shortcomings in its own systems or processes. The transaction must therefore be treated as unauthorised, with a full refund."*[9]

[9] P. 5 - 7

Risposta tal-Fornitur tas-Servizz

Fir-risposta[10] tagħhom, il-BOV qalu:

> ***"The Bank's Point of View***
>
> 1. *Whereas according to the Bank's records[11] the transactions of €1,500.19 and €950.71 were duly authorised on the 5th September 2025 at 12:20 and 12:43 respectively. As part of the Bank's security framework, which is fully aligned with the requirements of the Payment Services Directive 2 (PSD2), multiple layers of authentication were applied to ensure that the transactions originated from credentials and systems in the Complainant's name. In fact, the transactions had no indication that they were fraudulent;*
>
> 2. *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"*
>
> 3. *Whereas the Bank implemented the necessary measures to ensure that its systems are secure and in line with the PSD2 which provides the following on Strong Customer Authentication (SCA):*
>
> > *"'**strong customer authentication**'[12] means an authentication based on the use of two or more elements categorised as **knowledge (something only the user knows)**, **possession (something only the user possesses)**[13] and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability*

[10] P. 65 - 73 u dokumenti annessi p. 74 - 120
[11] Doc. A
[12] Emphasis added
[13] *Ibid*.

> *of the others, and is designed in such a way as to protect the confidentiality of the authentication data"*[14]

4. *Whereas apart from SCA, the Bank also implements a system of dynamic linking as outlined in Commission Delegated Regulation (EU) 2018/389, which supplements PSD2;*

5. *Whereas these payments were approved using the confidential details of the Complainant. The Bank had no control over the transfers because they were initiated without the Bank's intervention. Once the Bank receives legitimate instructions for a third-party payment through its secure and authenticated channels, the Bank is obliged to implement them, as it is reasonably expected that the only person with access to such confidential details and systems is the account holder. In this case, the transactions were duly authorised following successful validation of the Complainant's credentials, and there was no indication of fraud at the time of processing. In fact, this is outlined in the Bank's terms and conditions which provide the following:*

> *"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***[15] *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*

[14] Article 4(30) of PSD2.
[15] Emphasis added.

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

6. *Whereas moreover the abovementioned Commission Regulation provides that the Bank can decide to not apply SCA for transactions which are considered to have a low level of risk*[18]*. Therefore, one can conclude that when a transaction is considered to be of a higher risk, the Bank should implement the use of SCA. In fact, the Bank always implements the use of SCA to ensure that it implements the highest level of security possible (even if a transaction is considered to be low risk). In fact, in this case, both transactions were approved through SCA;*

7. *Whereas 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:*

> *"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*

[16] Doc. B, 2.22 'Any Instruction to Us', Page 24.
[17] Doc. B, 2.18(q)(ii), Page 14.
[18] Article 18 of Regulation (EU) 2018/389.

> *reasonable steps to keep its personalised security credentials safe."*

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

> *"The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence"*

9. *Whereas the fact that the Complainant provided the necessary details which enabled the approval of the payment, goes against the Bank's terms and conditions which provide the following:*

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

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

11. *Whereas upon receiving the Complainant's report on the 5th September 2025, the Bank immediately (i) blocked and cancelled the Complainant's cards, (ii) restricted access by setting the Complainant's internet banking package as pending, (iii) escalated the case to the relevant internal units, (iv) cancelled the GBP 1,000.14 payment as it was still in time to be stopped, and (v) initiated recall requests*[20] *for the remaining payments, requesting a copy of the police report in English to support the recall process;*

12. *Whereas, prior to the incident, the Complainant's registered number received nine anti-fraud SMS warnings from the Bank between November 2023 and September 2025, consistently instructing 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."*

[20] Doc. C and Doc. D

(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) *16th 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) *3rd September 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." / "Il-Bank of Valletta qatt ma jibgħatlek SMS b'links biex tagħfas fuqhom. Tagħfashomx għax tista' tiġi misruq! Jekk tiġi f'dubju, ċempel lill-Bank fuq 21312020."*

13. *Whereas the abovementioned 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.''[21] It also explains what personal details such scam may ask for which indicates that the communication is not genuine;*

14. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams. In fact, in the past years, the Bank has published*

[21] Doc. E

multiple newspaper articles and coordinated TV and radio appearances where Bank employees explain what spoofing is and how to identify it. A comprehensive list of the available resources till September 2025 is being attached as 'Doc.F'.

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

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

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

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

18. *Whereas therefore, any alleged fraud occurred due to the participation of the Complainant who provided confidential details to a fraudster and followed the instructions he gave him. All this contributed to his gross negligence."*[22]

Seduti

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

Fil-kontroeżami kompla jgħid:

"Mistoqsi naqbilx li fil-5 ta' Settembru jien irċevejt telefonata minn persuna li stqarret u li jien emmint li kienet rappreżentanta tal-bank, ngħid li, iva.

Mistoqsi naqbilx li din il-persuna jien ma kontx nafha personalment, ngħid li ma nafhiex.

Mistoqsi waqt dik it-telefonata x'informazzjoni tajtha eżatt relatata ma' affarijiet personali, ngħid li jien xejn, xejn ma tajtha just kif għidt. Hi qaltli li xi t-3.00 a.m. inġibduli xi flus u huma ndunaw li hija fraud u waqaf kollox. Kont għidtilha li kont xogħol u kont ninsab konfuż. Qaltli li hi kienet hemm biex tgħinni u qaltli li kulma rrid nagħmel hu li nidħol fl-application, nidħol fis-Signatures, nagħfas Signature 1. Wara li għafast Signature 1 ...

Qed jingħad li fil-complaint tiegħi, (paġna 3), jien tajtha l-One-Time Password.

L-Arbitru jispjega li jien irċevejt l-activation code. Mistoqsi inix nirreferi għal dan meta ngħid li tajt il-One-Time Password, ngħid li iva, għal dak.

Ngħid li meta għafast fuq il-One-Time Password telgħuli six numbers fuq. U qaltli biex ngħidhomlha.

[22] P. 66 - 72

Qed jingħad li skont is-sekwenza t'avvenimenti jiena tajtha l-One-Time Password imbagħad irċevejt SMS u fl-SMS qaltli 'Here is your activation code ... activate your BOV mobile app.'

Naqbel li jien għaddejt dik l-activation code lil dik il-persuna li kelli fuq it-telefon.

Naqbel li jien tajt lil terza persuna l-One-Time Password u l-activation code.

Mistoqsi issuspettajtx u ppruvajtx inċempel il-bank biex nivverifika jekk din kinitx telefonata leġittima, ngħid li jien dak il-ħin kont xogħol u kif qaltli hekk li ġejt frodat, dak il-ħin, l-ewwel ħaġa li tiġik ġo moħħok hu li tagħlaq il-kontijiet. U hi qaltli hekk biex inkun safe, però, meta rajt li kienet ħaġa stramba, mort il-branch ma ċempilt imkien. Kif sirt naf hekk, mort malajr il-branch tan-Naxxar.

Mistoqsi naqbilx li l-bank bagħatli diversi SMS warnings rigward dawn l-attivitajiet kontra links mibgħuta b'SMS, ngħid imma dawk kienu fuq links.

Qed jingħad li anke fuq telefonati bagħat warnings il-bank fuq il-verification codes u passwords.

Ngħid li fuq verification codes, meta ddaħħal mobile ġdid, il-bank jgħidlek biex tagħfas l-activation code li jkun intbagħat, biex tgħidulu. Naf għax kemm-il darba bdilt il-password tal-mobile.

Dr Raquel Hannah Theuma ser tikkonferma fuq dawn il-warnings rigward telefonati.

Mistoqsi naqbilx li mingħajr l-activation code u l-One-Time Password, din il-frodi ma kinitx isseħħ, ngħid li din ċemplitli għax kien fadlilha dawn l-affarijiet li jiena nibqa' ngħid li kellha xi informazzjoni fuqi, kien jonqosha żewġ affarijiet jew oħra, u ċemplitli. Ngħid li rigward il-User ID, kif għidt fil-laqgħa, din il-mara ġabitu minn x'imkien. Jien tajt il-One-Time Password u l-activation code imma qatt ma tajt il-User ID."[23]

L-Ilmentatur talab li jingħata *log* li turi l-ħin preċiż li fihom saru l-pagamenti.

L-Arbitru indika Dok A[24] anness mar-risposta tal-BOV li turi l-ħinjiet tal-pagamenti ilmentati.

---

[23] P. 130 - 131
[24] P. 74

Fit-tieni seduta li nżammet fil-21 t'April 2026, xehed Keith Vella - *Deputy MLRO* u *Head* ta' *AFC Transaction Monitoring & Proactive Analysis* tal-BOV.

Huwa spjega kif taħdem il-*payments monitoring system* tal-Bank u wara qal:

"Ngħid li fl-ebda ħin dawn il-pagamenti ma waqfu u kemm il-Pre u l-Post-Transaction Monitoring System ħadmu tajjeb u ma kellhomx għalfejn jieqfu għal diversi raġunijiet. Red flags fuq dawn iż-żewġ pagamenti ma kienx hemm; l-ammonti kienu modesti; il-pagamenti kienu sejrin lejn a low-risk jurisdiction; ma kien l-ebda impediment biex dawn iż-żewġ tranżazzjonijiet jiġu transacted u plus hekk, kienu wkoll within the profile tal-klijent.

Meta ngħid within the profile, ma jfissirx li għax klijent qatt ma bagħat transactions barra minn Malta, bħalma ġara f'dan il-każ, allura, kull transaction jew l-ewwel transaction li jagħmel il-klijent trid tieqaf bilfors fl-Pre- u Post-Transaction Monitoring System.

Ngħid li jaqgħu fil-profile tal-klijent għax kemm f'Settembru 2025, f'Ġunju 2025, f'Diċembru 2024, il-klijent bl-istess mod kif jista' jibgħat pagament barra minn Malta irid isegwi l-istess proċedura biex jibgħat pagament f'Malta stess. L-istess modus operandi li tintuża biex aħna nibagħtu pagament barra minn Malta, (bħal dawn li ġew transacted mill-kont tal-klijent), l-istess nagħmlu biex nibagħtu pagament lil xi ħadd hawn Malta.

Ngħid li l-ammonti kienu within the profile għax il-pagamenti li l-klijent bagħat f'Malta stess lil entitajiet jew persuni oħra kienu madwar €5,000 u €3,000 u, għaldaqstant, jaqgħu within the profile. U dawn l-ammonti kienu akbar mill-ammonti li qed jiġu disputed hawnhekk."[25]

Fil-kontroeżami qal:

"Nikkonferma li t-transactions li jsiru kemm għal barra u kemm għal Malta tintuża l-istess proċedura. Kulma jkun hemm differenti hu l-IBAN.

Qed jingħad li skont ir-records tal-bank, l-Ilmentatur huwa baker, però, l-pagament hu relatat ma' farm.

Mistoqsi wara dawk il-proċessi ta' Pre- u Post-Transaction Monitoring, possibbli li ma telgħet l-ebda alert, ngħid li, le, ma kellhiex għalfejn ittella' alert.

[25] P. 153 - 154

Mistoqsi x'kienu l-ħinijiet meta ż-żewġ transactions telqu mill-bank, ngħid li t-tranżazzjoni ta' €950.71 telqet f'12:43:14 (SWIFT – p. 147).[26]

BOV ressaq ukoll ix-xhieda[27] ta' Michael Gatt, espert fis-sistema tal-pagamenti elettroniċi tal-BOV. Spjega kif, f'għajnejn il-Bank, il-pagamenti ilmentati dehru awtorizzati mill-Ilmentatur u dan skont ir-regolamenti Ewropej dwar pagamenti.

Spjega li f'dan il-każ jidher li l-Ilmentatur ikkopera mal-frodist billi kixef il-kodiċi, *activation code,* mitluba li huwa biss kellu permezz ta' SMS mibgħut lilu mill-BOV wara li ntalab permezz ta' *Signature 1 panel* tas-sistema, u dan ippermetta lill-frodista tieħu f'idejha iċ-ċavetta li jawtorizza pagamenti daqslikieku kien l-Ilmentatur li qed jawtorizzahom.

Fil-kontroeżami qal:

"Mistoqsi naqbilx li mir-records tal-bank l-Ilmentatur ma għafas l-ebda link; mistoqsi jekk il-bank għandux log li l-Ilmentatur għafas xi link, ngħid li jekk l-Ilmentatur għafas xi link, il-link ma bagħathiex il-BOV, jiġifieri jekk il-link ma bagħathiex il-BOV, kif irid ikollna record tagħha?

Mistoqsi jekk wieħed jagħfas il-link il-bank ikollux li l-proċess sar għax ingħafset il-link, ngħid li l-link mhijiex tal-BOV. Li nista' ngħid, skond ir-records tal-bank, li ġie mitlub an Activation Code u dan l-Activation Code ingħata.

L-Activation Code jista' jiġi mitlub w billi tmur il-branch (li f'dan il-każ ma sarx), jew tidħol fl-Internet Banking u terġa' tagħmel request għal Activation Code jew inkella ċċempel il-Customer Service Centre.

F'dan il-każ ġie ġġenerat Activation Code through l-Internet Banking. Għandna wkoll on record li l-Activation Code intbagħat fuq il-mobile number tal-Ilmentatur li dan, b'xi mod jew ieħor, ġie għall-konoxxenza tal-frodista.

Jien qed nitkellem fuq x'qed juruni l-logs."[28]

Qam argument jekk il-User ID li l-Ilmentatur iddikjara li ma kixfux lill-frodista jifformax parti mill-i*Strong Customer Authentication* (SCA) taħt ir-regolamenti bankarji jew le.

[26] P. 154
[27] P. 155 – 156
[28] p. 156

L-Ilmentatur qal li dan il-User ID ma jinbidel qatt u probabbli li l-frodista kellha informazzjoni minn ġewwa l-Bank dwaru.

Ġie kkonfermat ukoll li permezz tal-fatt li l-*Activation Code* ġie kkomunikat lill-frodista, il-pagamenti ilmentati saru minn *token* ġdid li ġie rreġistrat skont fejn ġie ttrasferit il-*Mobile App*, għax *token serial* 706081 inbidel għal *token serial* 9690055 avolja l-*mobile number* irreġistrat baqa' bla mittiefes.

Fuq talba tal-Ilmentatur, saret seduta oħra fid-29 ta' Mejju 2026, biex jixhed Luke Cutajar, inkarigat mis-sistema tar-*recalls* tal-Bank. Huwa qal:

"Ngħid li [l-Ilmentatur] kellu erba' pagamenti. Kien hemm tnejn minnhom li kienu għadhom ma ġewx ipproċessati mill-bank u, allura, irnexxielna jiġu reversed. F'dak il-każ konna lħaqnihom. U wieħed minnhom ta' €1,500.19 u l-ieħor ta' €950.71 laħqu telqu mill-BOV u hemmhekk nidħlu aħna biex nagħmlu r-recall of funds. Però, ultimately, irċevejna risposta lura li ma kienx għad baqa' flus għand il-benefiċjarju. U, għaldaqstant, kellna nagħlqu l-każ.

Ngħid li fil-każ tal-€1,500.19, irċevejna request biex nagħmlu recall of funds fuq id-database tagħna fis-6.30 p.m. Aħna, min-naħa tal-BOV, ma naħdmux dak il-ħin. Aħna naħdmu sal-4.00 p.m.

Ngħid li rajniha first thing after the weekend, it-Tnejn filgħodu fejn proprjament rajniha qabel il-ħin tax-xogħol. Rajniha f'7:48 a.m. Bgħatna email u Swift message u bgħatna wkoll camt.056 lill-benefiċjarju.

Ngħid li nibagħtu wkoll reminders jekk naraw li ma rċevejna xejn min-naħa tal-benefiċjarju. Però, f'dan il-każ irċevejna acknowledgement li l-investigazzjoni għadha ongoing fil-11. Bgħatna aktar reminders fit-12 u anke fis-17. Irċevejna aktar acknowledgements mill-beneficiary bank li l-investigazzjoni kienet għadha ongoing. Imbagħad, irċevejna camt.029 (li tfisser recall declined) min-naħa tal-benefiċjarju fejn qalulna AM04 li tfisser li ma fadalx flus.

Ultimately, kellna nagħlqu l-każ għax ma stajna nagħmlu xejn aktar.

Fil-każ l-ieħor, ġrat l-istess ħaġa. Irċevejniha fis-6.30 p.m. u rajniha t-Tnejn filgħodu f'7.48 a.m. ukoll. Bgħatna email u Swift message u bgħatna wkoll camt.056 (li tfisser recall of funds) lill-benefiċjarju.

Irċevejna l-istess tip ta' acknowledgements fejn l-investigazzjoni kienet għadha ongoing. Imma, mbagħad, erġajna irċevejna camt.029, li ġiet declined with reason AM04 li tfisser No funds remaining in beneficiary's account.

U għalaqna l-każ b'dak il-proċess ukoll.

Ngħid li dawn kienu l-istess bank imma l-benefiċjarji kienu differenti. Il-creditor kien Jamie Ken Smith u għandi l-IBAN number u tad-€950 kien James Meklovsky Malone.

***Nikkonferma li recalls kien hemm tnejn u t-tnejn fallew*."[29]

Fil-kontroeżami qal li huwa inkarigat mir-*recalls* dwar trasferimenti li jkunu telqu wara li jirċievi notifika dwarhom u, għalhekk, ma setax jirrispondi għalfejn żewġ pagamenti telqu u tnejn inżammu u lanqas għalfejn ma ġiex infurmat qabel biex ir-*recall* isir dakinhar stess (il-Ġimgħa) u mhux kellu jistenna sat-Tnejn.[30]

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 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-

[29] P. 160
[30] In-notifika biex isir *recall* waslet għand id-Dipartiment fis-6.30 p.m. tal-Ġimgħa meta l-Ilmentatur mar il-fergħa tan-Naxxar jirrapporta l-każ fil-ħin tas-1 p.m. (p. 3) u għamel rapport l-Għassa fil-ħin tas-2:44 p.m. (p. 35).

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 każi fejn l-ilmentaturi faċilment jaqgħu f'din il-kategorija.

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

[31] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[32] Article 64 of PSD 2

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.[33] [34]

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 għac-cirkostanzi partikolari ta' dan il-każ, l-Arbitru irid jispjega li l-User ID mhuwiex parti mill-obbligi SCA taħt il-PSD2[35]. Dan huwa kodiċi li qatt ma jinbidel, ekwivalenti għan-numru tal-kont li jintuża għall-IBAN. Jista' jkun magħruf minn diversi uffiċjali tal-bank u, għalhekk, mhux ikkonsidrat bħala kodiċi sigriet. Tant li dan ma jinbidilx anke jekk jiġi rrapportat frodi.

Is-suspett li l-frodista kellha informazzjoni interna dwar il-User ID hu suspett raġonevoli, iżda jibqa' suspett li ma jaffetwax ġudizzju jekk il-pagamenti kinux awtorizzati permezz ta' SCA u *2-Factor Authentication* skont PSD 2.

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

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

	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	0%	(0%)
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	20%	(20%)
Sub-total	(30%)	(70%)
Tnaqqis għal ċirkostanzi speċjali	(20%)	20%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(50%)**	**(50%)**

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 50% tal-piż u l-50% 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 ma jistax jigi akkużat li kkopera mal-frodist għax, fil-fatt, ma kien għafas fuq l-ebda *link* f'messaġġ frawdolenti. Il-fatt li kixef OTP u l-*activation code* mhix meqjusa fi grad ta' ko-operazzjoni meta ssir telefonikament ma' persuna konvinċenti li kienet tirrappreżenta lill-Bank.

L-Arbitru jagħmel distinzjoni bejn min jirċievi SMS frawdolenti u jkollu ċans jaħsibha, jċempel il-bank biex jiċċekja u anke jħares lejn notifiki ta' twissija li jkun irċieva qabel, u każ bħal dan fejn iċemplulu fuq numru jixbaħ lil dak tal-bank, u tkellmu persuna li b'mod konvinċenti tippersonifika lill-bank u tilgħabha li qed tgħinu jikkanċella pagamenti mhux awtorizzati.

L-Ilmentatur dwar dan qed jiġi ppenalizzat 20% għall-fatt li ma mexiex man-notifiki li kien jibgħat il-Bank kif deskritt hawn taħt.

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.

L-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat minn xi ħadd li tippersonifika b'mod espert lill-Bank permezz ta' telefonata '*live*', allura, minkejja t-twissijiet li l-Bank ikun ħareġ, il-prekawzjonijiet normali jitwarrbu speċjalment meta jkun mhedded li hemm pagamenti frawdolenti li ser isiru u l-midinba tilgħabha tal-verġni b'mod espert.

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, 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 niġux 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'tekonoloġija 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 dewmin biex isir kuntatt permezz tat-telefon mal-klijent.[36]

B. Filwaqt li s-sistema ta' moniteraġġ ta' pagamenti tal-Bank kienet effettiva biex waqqfet tnejn mill-erba' pagamenti frawdolenti, mhux l-istess jista' jingħad għas-sistema tar-*recalls* tal-Bank.

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

> L-Ilmentatur irrapporta l-każ fil-ħin tas-13:00, u mix-xhieda ħareġ li notifika biex isir *recall* waslet fid-dipartiment konċernat fil-ħin tas-18:30 meta d-dipartiment jagħlaq fil-ħin tal-16:00 u, għalhekk, ir-*recall* setgħet biss issir wara l-*weekend*.

Meta jsir rapport ta' frodi iridu jsiru żewġ affarijiet b'mod tempestiv:

1. Jiġi mblokkat l-*Internet Banking* u jinkanċellaw il-*cards*.

   Dan sar.

2. Isir *recall* urġenti dwar it-trasferimenti li jkunu laħqu telqu biex isir attentat li l-fondi jiġu mblokkati qabel ma jsiru disponibbli lill-frodisti. Dan ma sarx. Ħames sigħat u nofs huwa żmien twil wisq u seta' ppreġudika l-possibilità ta' rkupru effettiv.

B'kollox, għalhekk, qed jiġi intitolat għal kumpens ta' 80% tat-telf li sofra minn pagamenti frawdolenti li ġie ddebitat lill-kont tiegħu.

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, disa' mija u sittin ewro punt sebgħa tnejn (€1,960.72).[37].

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[38] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv. [39]

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

---

[37] 80% ta' €2,450.90

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

[39] [39] 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 80% għall-BOV u 20% 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 wara li jiskadi l-perjodu tal-appell. Dettalji personali tal-ilmentatur/i jkunu anonimizzati skont l-artikolu 11(1)(f) tal-Att.