Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 280/2025

TV

('l-Ilmentatriċi')

vs

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

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

Seduta tat-30 ta' Ġunju 2026

L-Arbitru,

Ra l-Ilment[1] datat 12 Novembru 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi tal-anqas 70% tat-telf li sofriet meta saru ħames pagamenti frawdolenti mill-kont tagħha mal-BOV li b'kollox jammontaw għal €4,892.

Fil-fatt dawn il-pagamenti kollha saru nhar id-9 ta' Mejju 2025 kif spjegat fit-tabella:

Ħin	Ammont €	Referenza
12:08:58	978	p. 59; 164
12:09:28	969	p. 59; 164
12:22:01	959	p. 59; 164
12:22:34	995	p. 59; 164
12:31:51	991	p. 59; 165
TOTAL	**4,892**	

[1]Paġni (P.) 1-11 b'dokumentazzjoni addizzjonali minn P. 11 - 45.

Il-pagamenti kollha saru favur ċertu Greggory Isaac Jamie Philips. B'mod stramb dan Philips waqt il-proċess tal-pagamenti kien bagħat pagamenti favur l-Ilmentatriċi ta' €6 u €50. Irriżulta wkoll li l-BOV kien irkupra permezz ta' recall ammount żgħir ta' €13.26 li ġie ikkreditat fil-kont tal-Ilmentatriċi fis-27 ta' Mejju 2025. B'hekk it-telf jonqos b'€69.26 għal €4,822.74. In vista ta' spejjeż oħra inkorsi waqt il-każ, l-Arbitru qed jaċċetta li t-telf huwa dak dikjarat ta' €4,892.[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'.*

- 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-

[2] L-Ilmentatriċi, però, inkorriet spejjeż ghat-transferiment €8 x 5 = €40; spejjeż tar-recall €20 x 5 = €100; u spejjeż tal-bdil tal-card €5.

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

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:

- Fid-9 ta' Mejju 2025, fil-ħin ta' 11:47, irċeviet messaġġ biex javżawha li se jċemplulha u messaġġ ieħor biex tagħfas link.[4] Dan daħal fuq il-kanal ta' SMS fejn normalment tirċievi notifiki mill-Bank. Fil-ħin ta' 11:48 kellha telefonata fuq numru 99180001 fejn persuna kellmitha bil-Malti u qalet li kienet Cynthia mil BOV u xtaqet tistaqsi dwar żewġ pagamenti ta' €900-ilwieħed li kienu skedati li jsiru fl-4 p.m. u kienu saru minn device I-phone 15.[5]

- Fuq it-telefonata kellha avviż 'Suspected Scam' imma Cynthia assiguratha li dak kien għax fuq dan in-numru iċempel biss il-Bank u ma tistax iċċempel lura.[6]

- L-Ilmentatriċi ċaħdet li kienet għamlet dawn il-pagamenti u Cynthia qaltilha li ser tibgħatilha code biex tneħħi dawn il- pagamenti.

- Cynthia baqgħet tkellimha biex tgħidilha li kien hemm bżonn jagħmlu *reset* tal-*USER* ID u ġġwidata x'għandha tagħfas.

- Fuq iċ-*channel BOV Mobile* irċeviet SMS fil-ħin ta' 12:01 li kien jgħid

[4] P. 13; p. 122
[5] P. 40
[6] P. 12

'Here is your activation code. Please use it within 1 hour to activate your BOV Mobile APP: WqGOZVt3.'[7]

- Wara irċeviet messaġġi biex jinfurmawha li żewġ pagamenti suspettużi ġew blokkati. U ftit wara notifiki li saru żewġ pagamenti ta'€969 u €978. Kif kienet għadha fuq it-telefon ma' Cynthia qaltilha bin-notifiki iżda dik assigurata li l-pagamenti ġew blokkati.

- Wara t-telefonata għamlet kuntatt mal-Bank għax bdiet tissuspetta u meta qabdet mal-*fraud section* ikkonfermawlha li dik kienet scam u sa dak il-ħin stess kienu ġa għaddew tliet pagamenti oħra b'żieda mat-tnejn li rrapportat.

- Probabbli ma sarux pagamenti oħra għax kien intlaħaq il-limitu ta' €5,000 li jistgħu isiru f'ġurnata waħda.

- Sar rapport lill-pulizija dakinhar stess fil-ħin ta' 16:50 u tat kopja tar-rapport lill-Bank biex isir il-proċess ta' recalls f'attentat biex jiġu imblokkati l-fondi qabel ma jinġibdu mill-frodisti.

L-Ilment

L-Ilmentatriċi qed titlob kumpens ta' €3,415 kif ġie spjegat qabel li jammontaw għal madwar 70% tat-telf sostnut ta' €4,892.

L-argument prinċipali tal-Ilmentatriċi huwa li hi kienet vittma ta' frodi sofistikata li mhux biss intuża SMS fuq il-kanal normali tal-Bank iżda saħansitra kien hemm telefonata konvinċenti bil-Malti minn persuna li dehret midħla sew tal-proċeduri tal-Bank. Sostniet li qatt ma kienet irċeviet twissijiet dwar telefonati bħal dawn.

BOV offrewlha kumpens ta' 50% iżda hija ma aċċettatx u qed tfittex irkupru ta' 70% skont il-mudell tal-Arbitru.

"Although I acknowledge my mistake in not recognizing the deception sooner, this incident demonstrates that fraudsters are capable of replicating official bank channels perfectly, misleading even vigilant customers."[8]

[7] P. 126
[8] P. 6

"Furthermore, after reviewing the criteria used in my case, I am concerned about the 20% increase in my responsibility applied on the basis that I had been "warned." I do not believe the general warnings I received adequately addressed the nature of the scam or equipped me with the information necessary to identify it.

In light of this, I feel the Bank did not provide the level of protection or clarity expected, and I respectfully ask that this be reconsidered. I remain willing to resolve this matter amicably and directly.

The Bank informed me that it applied the Arbiter's model to determine a refund, stating this was its own interpretation and not an Arbiter decision. The model starts with 100% user responsibility and adjusts based on circumstances. Since my case involved spoofing (fraud appearing to come from BOV), the Bank deducted 50%. As I did not authorize the transactions, no extra responsibility was added. However, 20% was added because a general fraud awareness SMS was sent in January 2025, and another 20% was reduced since the amounts were not typical for my account. The Bank therefore concluded I was 50% responsible and offered a 50% refund. I respectfully believe my responsibility should be limited to 30%, given the sophistication of this spoofing fraud, and I therefore request a 70% refund in line with the Arbiter's fairness principles which equates to €3,415."[9]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[10] tagħhom, datata 02 ta' Diċembru 2025, il-BOV qalu:

5. *"Whereas according to the Bank's records, the five transactions referenced above were duly authorised on the 9th May at 12:08, 12:09, 12:22, and 12:31. 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;*

[9] P. 7 - 8
[10] P. 50 – 57 u dokumenti annessi p. 58 - 114

6. *Whereas Article 40(1) of the Directive No. 1 of the Central Bank of Malta, provides that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. The Bank received legitimate instructions from credentials associated with the Complainant and therefore has no obligation to refund her:*

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

7. *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' 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) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data"

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

9. *Whereas 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 terms and conditions of the Internet Banking system which provide the following:*

   "You authorise us to act on any instruction that we receive through the Channels which has been, or reasonably appears to have been, sent by you

and which, where applicable, has been sent using your Security Number/s or BOV Mobile PIN or biometric data."

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

10. *Whereas besides the fact that the payments were duly authorised, there is also the fact that the transaction amount was within the limit imposed for these kinds of transactions. With respect to the transactions in question in this arbitration, which are 'third-party transactions', the limit is €5,000. Therefore, there were no suspicious signs for the Bank with respect to this transaction. One should also note that the PSD 2 does not oblige the Bank to impose any limit on transactions. It only stipulates that if there is the possibility to put in place spending limits, the customers should be informed of this;*

11. *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. 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 strong customer authentication.*

12. *Whereas without prejudice to the above, if the Complainant is alleging that these transactions were not authorised by her, then the Bank is still not obliged to refund her, since even if he did not have the intention to approve a payment, she 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:*

"45. (1) The payment service user entitled to use a payment instrument shall:

use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;

(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe."

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

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

14. *Whereas the fact that the Complainant provided the necessary details which enabled the approval of the payment, goes against the terms and conditions of the internet banking service which provides the following:*

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

15. *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 Bank's website or from the BOV Mobile App. Whereas the Bank never before requested the Complainant (or any other customer for that matter) to access their internet Banking from a link in a SMS, because it has the adequate systems for this service to be accessed.*

Moreover, the Bank never calls customers requesting the details which were asked from the Complainant. In fact, the Bank warns customers to be careful what information they disclose, particularly on links;

16. *Whereas besides communication on social media, in November 2023 the Bank also launched a scheme of sending SMS's directly to its' customers in order to inform them of ongoing scams which may be directed at them. In fact, prior to this incident, the Bank had sent the Complainant two SMSs on the 20th January 2025 and on the 15th April 2025 stating the following:*

    '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.'

17. *Whereas as can be seen, the Bank warns customers to be careful what information they disclose and that the Bank does not request certain details through SMS or calls. This is done in order to avoid incidents of fraud and prevent customers from falling victim to spoofing/smishing where fraudsters may impersonate Banks. As will be explained throughout the proceedings, the Bank cannot control such incidents of spoofing/smishing;*

18. *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 SMS's, 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." It also explains what personal details such scam may ask for which indicates that the communication is not genuine;*

19. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about*

these scams. 'DOC. E1' 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 and 27th 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. E2';

20. *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.'

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

22 *Whereas besides this, she also acted against article 45(2) of the Directive because she did not take all the reasonable steps to keep her 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;*

23. *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 her. All this contributed to her gross negligence;*

24. *Whereas the five payments of €969, €978, €995, €959, and €991 were approved on the 9th May 2025 at 12:08:59, 12:09:29, 12:22:02, 12:22:35, and 12:31:52 respectively. These payments were processed immediately in accordance with the Bank's Terms and Conditions, which state that if a customer requests an immediate payment, the Bank cannot cancel or amend the instruction once received. This clause is in conformity with Article 80 of PSD2, entitled "Irrevocability of a payment order".*

25. *Whereas the Complainant contacted the Bank to report the incident, and the Bank immediately blocked her internet banking access to prevent further unauthorised transactions. The Bank then initiated recall requests for all five payments, which requests are made through a secure digital system between banks. It is important to note that the outcome of the recall process depends entirely on the receiving bank's internal procedures and availability of funds. BOV has no control over other banks and therefore cannot dictate the timeframe for their response or guarantee the success of the recall;*

26. *Whereas the Bank respectfully submits that it acted promptly and diligently to recover the funds. Once the Bank received a reply, it informed the Complainant accordingly. On the 12th May 2025, the Bank was informed that the recalls for four payments were declined by the foreign bank since no funds were available for return, while the recall for €959 remained ongoing. This demonstrates that the Bank exhausted all possible recovery channels within its control;*

27. *Whereas the Bank continued to pursue the recall for €959 and kept the Complainant informed of all developments. On the 27th May 2025, the Complainant's account was credited with €13.26, which had been returned by the beneficiary bank. The Bank explained that this is a common tactic used by fraudsters to make transactions appear less*

suspicious. Despite the minimal amount recovered, this shows the Bank's commitment to mitigating the loss;

28. *Whereas the Bank submits that it implements robust measures to ensure that its internet banking systems are secure and fully compliant with EU law, including PSD2 requirements for strong customer authentication. The Bank also continuously issues warnings and educational material on scams and fraudulent schemes. However, these measures are rendered ineffective if customers disregard the Bank's terms and conditions and ignore repeated warnings. In this case, the Complainant voluntarily disclosed sensitive banking credentials to a third party, which constitutes gross negligence. Therefore, the customer cannot reasonably expect the Bank to assume responsibility for losses resulting from her own actions;"*

Seduti

Fl-ewwel seduta tat-2 ta' Marzu 2026, l-Ilmentatriċi spjegat il-każ tagħha kif ġa riprodott hawn fuq. Ammettiet li kienet daħhlet fil-website, li wara rriżulta li kienet frawdolenti, il-User ID, il-One-Time Password u l-code li rċeviet fuq il-mobile.

Sostniet li filwaqt li kienet tirċievi SMS b'notifiki ta' twissija mill-BOV biex ma tagħfasx *links* anke jekk l-SMS ikun jidher li ġej mil-Bank, hi qalet:

"Ngħid li jien qatt ma rċevejt xi taħriġ jew spjegazzjoni min-naħa tal-Bank of Valletta rigward l-ispoofing jew l-iscamming. Ngħid li messages le. U lanqas irċevejt personalment xi tip ta' taħriġ ieħor.

Ngħid li fil-perjodu bejn id-9 ta' Mejju 2024 u d-9 ta' Mejju 2025, qatt ma għamilt pagamenti mill-kont tiegħi li huma simili ta' dawk li tteħduli dakinhar tal-iscam. Jiġifieri qatt ma għamilt pagamenti ta' €4,500 f'ġurnata waħda.

Ngħid li ġieli għamilt online payments imma mhux mill-app imma bil-key, mit-token.

Ngħid li kont naf kif nuża t-token biex nagħti s-signatures u biex nawtorizza pagamenti, però, dejjem BOV Mobile użajt.

Mistoqsija mill-Arbitru meta kien l-aħħar pagament li għamilt bit-token qabel dan, ngħid li żmien. Ma nafx ngħid f'dik is-sena, bejn id-9 ta' Mejju 2024 u d-9 ta' Mejju 2025, għamiltx payment, però, żmien twil."[11]

Fil-kontroeżami qalet:

"*Nikkonferma li f'Mejju 2025 jiena irċevejt telefonata minn numru li jien assumejt li kien tal-bank u nikkonferma wkoll li waqt din il-call, jien irċevejt dan l-SMS li fih kien hemm il-link.*

Mistoqsija jekk f'dawk it-tletin minuta li damet il-call, ġinix f'moħħi li naqta' mill-call u nikkuntattja n-numru uffiċjali tal-bank, ngħid li, le.

Mistoqsija jekk qattx il-bank ikkuntattjani fuq dan in-numru minħabba l-Home Loan, ngħid li nkun ikkuntattjata mill-branch. Ma jkunx hemm komunikazzjoni minn dan in-numru.

B'referenza għall-paġna 12 tal-ilment tiegħi, qed jiġi kkwotat x'għidt f'din l-email lill-bank, "She then asked me to log in to my BOV account via the app or website to check for any unauthorised transactions. While doing this, I noticed that her number was flagged as 'Suspected Scam.'"

Mistoqsija fid-dawl ta' dan għalfejn ma kkuntattjajtx il-bank, ngħid li jien għidtilha u qaltli li ġara hekk għax qatt ma ċempluli minnu u huma biss jistgħu iċemplu minn fuq dan in-numru u jiena ma nistax inċempel lura. Ngħid li jiena ma qtajtilhiex meta rajtha. Ngħid li ma ġietnix f'rasi.

Mistoqsija fejn rajtha din, ngħid fuq il-mobile.

Nikkonferma li f'dan l-SMS kien hemm link, għafastha u dħalt f'website li assumejt li kienet tal-bank.

Nikkonferma li daħħalt il-User ID, il-One-Time Password u l-code li bagħtitli hi mill-BOV Mobile.

Nikkonferma li f'dan il-ħin, l-mobile kien fil-pussess tiegħi biss u ma kien hemm ħadd ħdejja jew li xi ħadd kien qed jikkontrollali l-mobile.

[11] P. 118

Nikkonferma li l-authentication app hija marbuta mal-mobile tiegħi biss u nużaha jiena biss.

Nikkonferma li l-aċċess u l-passi ta' awtentikazzjoni setgħu saru biss bl-involviment tiegħi peress li kelli l-mobile u tajt ċertu informazzjoni li hija personalizzata għalija biss.

Mistoqsija kontx naf qabel dan l-inċident li l-bank ma jitlobx kredenzjali jew kodiċijiet permezz ta' links jew SMS, ngħid li ma jitolbux fuq telefon, kont naf. Fil-fatt, hi bdiet tgħidli biex ma ngħidilha xejn u jien għidtilha, 'Ovvja li le.' U tal-links, dak il-ħin, ma nafx.'"[12]

Fuq talba tal-Arbitru, l-Ilmentatriċi wara s-seduta bagħtet kopja tal-SMSs kollha konċernati f'dan il-każ.[13]

Fit-tieni seduta li nżammet fil-21 t'April 2026, il-Bank ressaq ix-xhieda ta' Michael Gatt, espert fis-sistema tal-pagmenti elettroniċi tal-BOV. Spjega kif f'għajnejn il-Bank, il-pagamenti ilmentati dehru awtorizzati mill-Ilmentatriċi u dan skont ir-regoli Ewropej dwar pagamenti.

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

Spjega li:

"Ngħid li biex jintalab Activation Code, trid tmur fl-Internet Banking, tmur fil-functionality tal-mobile settings u hemmhekk tkun tista' tagħmel rikjesta għal Activation Code. Trid tiffirma din ir-rikjesta u kif tiffirmaha, titlaq SMS bl-Activation Code fuq il-mobile number irreġistrat fir-records tal-bank.

Meta jkollok l-Activation Code u l-Login ID, hemmhekk tista' tirreġistra device ġdid bħal meta, eżempju, tibdel il-mobile set tiegħek.

[12] P. 118 - 119
[13] P. 122 - 127

Nikkonferma li dawn il-pagamenti ilmentati saru kollha minn device ġdid li l-frodist irnexxielu jirreġistra permezz tal-Activation Code. Infatti, s-serial number tat-token inbidel.”[14]

Fil-kontroeżami ix-xhud qal:

“Naqbel li l-Ilmentatriċi kienet irċeviet SMSes li kienu jidhru li ġejjin mill-bank għax mibgħuta fuq l-istess thread li s-soltu l-bank jibgħat il-messaġġi fuq in-numru 99180001.

Mistoqsi allura naqbilx li dan seta’ jikkonvinċi lill-klijenta li kienet qed titkellem ma’ rappreżentant ġenwin tal-bank, ngħid li l-bank jikkomunika mal-klijenti, però, fl-SMSes tal-bank li jibgħat is-soltu qatt ma jgħidlek biex tikklikkja fuq link u tagħti l-Login ID u l-kredenzjali tiegħek.

Mistoqsi meta ġie rreġistrat dan id-device ġdid, il-klijenta ġietx ikkuntattjata min-naħa tal-bank biex tikkonferma jew tawtorizza dan id-device il-ġdid, ngħid li meta inti tuża l-Login ID li taf inti biss u tuża l-Activation Code li intbagħat lilek biss, il-bank ma għandux għalfejn jistaqsik jekk irreġistrajtx mobile ġdid.

Hemm a set of security steps li ġew segwiti kollha f’dan il-każ u għall-bank dan hu kollu leġittimu.

Ngħid li aħna ma nċemplux kull meta jiġi rreġistrat device ġdid għax hemm set ta’ proċeduri u steps – mhux waħda, tnejn jew tlieta – li jekk jiġu segwiti ma jkunx hemm għalfejn inċemplu lill-klijent għax huma credentials li jafhom biss il-klijent u ħadd aktar.

Mistoqsi rigward l-SMS warnings li jibgħat il-bank humiex standard, li jintbagħtu lil kulħadd l-istess u japplikaw għal kull klijent, ngħid li l-messaġġ jinbidel kull tliet xhur, però, l-messaġġ jintbagħat l-istess għal kull klijent.

Mistoqsi meta kien l-aħħar messaġġ li ntbagħat lill-Ilmentatriċi qabel ma sar il-frodi, ngħid li bl-amment ma nafx imma nista’ niċċekkja.

Dr Raquel Hannah Theuma tirrispondi għal din il-mistoqsija:

[14] P. 129

Nikkonferma li qiegħda mniżżla fir-risposta.

Intbagħtetilha waħda fl-20 ta' Jannar 2025 u waħda fil-15 t'April 2025.

Nikkonferma li l-messaġġi ta' Jannar u t'April kellhom l-istess wording."[15]

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head* ta' *Transaction Monitoring u Pro-active Analysis* tal-BOV, li spjega l-*monitoring payments* system li jopera l-Bank biex jippreveni l-frodi. Qal ukoll li l-Ilmentatriċi kienet għamlet pagamenti *online* f'Jannar u Frar 2025 għal ammonti aktar minn elf ewro.[16]

Fil-kontroeżami qal:

"Mistoqsi nikkonferma li dawn it-tranżazzjonijiet li għadni kif semmejt issa li għamlet l-Ilmentatriċi kienu kollha lejn entitajiet lokali, ngħid li semmejt l-aħħar u li qabbilthom mat-tranżazzjonijiet li huma allegati frawdolenti, iva.

Qed jingħad li l-ebda waħda minnhom ma qabżet l-€4,000 f'ġurnata waħda. Ngħid li ma nistax nirrispondi eżattament issa għax hawnhekk għandi t-tranżazzjonijiet li huma pressa poco viċin l-ammont li allegatament ġew iffrodati lis-Sinjura; m'għandix l-istatement kollu quddiemi.

Ngħid li t-tranżazzjoni ta' €25,000 saret fis-27 t'April 2021.

Mistoqsi nikkonferma li dawn l-ammonti ta' tranżazzjonijiet saru fi żmien qasir, fi ftit mumenti minn xulxin, ngħid li saru bejn 12:09 u 12:32.

Qed niġi mistoqsi, allura, la nġibdu dawn l-ammonti ta' flus fi ftit minuti għalfejn ma ġewx flagged mis-sistemi tal-bank.

Ngħid li on a risk-based approach u x-scenarios li għandna fis-sistemi, kollha kemm huma bbażati fuq guidance li nirċievu mingħand ir-regolaturi, mil-liġijiet li għandna fil-pajjiż rigward AML, u anke mit-topologies li nkunu qed naraw f'dak il-perjodu. Din hi sistema ħajja, jiġifieri mhix xi ħaġa li tħalliha hemmhekk u taħdem għal dejjem u, ovvjament, dejjem isiru updates, kemm il-Pre- u kemm il-Post-Transaction Monitoring Systems ma ħassewx li għandhom

[15] P. 129 - 130
[16] P. 130 - 133

jitwaqqfu dawn il-payments. Ma kien hemm l-ebda red flags għalfejn kellhom jitwaqqfu dawn il-payments.

U kif semmejt ukoll, jekk il-klijenta kienet qed tibgħat lil dak il-benefiċjarju, kienet qed tirċievi wkoll mingħand dak il-benefiċjarju.

Mistoqsi l-fatt li l-Ilmentatriċi qatt ma għamlet pagament lejn il-Lithuania għaliex mhuwiex meqjus riskjuż, ngħid ma jfissirx li klijent, hu min hu, li qatt ma għamel transaction barra minn Malta jew qatt ma għamel transaction partikolarment differenti għandek twaqqaf it-transaction mal-ewwel darba.

Hemm diversi riskji li jittiħdu in konsiderazzjoni u ma jfissirx li għax klijent qatt ma għamel cross-border transaction, dik it-transaction għandha tieqaf.

Qed jingħad li meta l-Ilmentatriċi indunat li qed jitteħdulha l-flus, ikkuntattjat il-bank; użat il-Helpline u kienet qed titkellem ma' xi ħadd fuq il-linja meta tteħdulha aktar flus.

Mistoqsi minkejja l-bank ikun infurmat, ma jkunx hemm proċess ta' twaqqif dak il-ħin meta hi tkun qiegħda fuq il-linja, ngħid li fuq din ma nistax nirrispondi għax dak jieħdu ħsieb dipartiment ieħor."[17]

Fuq talba tal-Arbitru, l-BOV bagħtu kopja ta' *statement* għal perjodu ta' sena qabel il-każ tal-ilment li kien juri pagament *online* fil-21 ta' jannar 2025[18] u oħrajn fit-30 ta' Jannar 2025 u 05 ta' Frar 2025.[19]

Sottomissjonijiet finali

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

Konsultazzjoni mal-*Malta Communications Authority*

Biex l-Arbitru jifhem l-intriċċi teknoloġiċi dwar kif frodist jista' jippersonifika ruħu qisu l-Bank biex jiffroda lill-klijenti, stieden għal konsultazzjoni lill-espert tas-*security* kemm tal-BOV kif ukoll tal-*Malta Communications Authority* (MCA).

[17] p. 133 - 134
[18] P. 156
[19] P. 157

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-banek ikomplu jsaħħu l-protezzjoni tal-konsumatur kontra frodisti li kulma jmur dejjem isiru aktar kapaċi u kreattivi.

Iżda l-Arbitru jħoss il-bżonn jenfasizza 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*[20] 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-Ilmentatriċi faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[21] 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/Ilmentatriċi. 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/Ilmentatriċi, 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-Ilmentatriċi 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.[22] [23]

[20] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[21] Article 64 of PSD 2
[22] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[23] PSD 2 Eu 2015/2366 Artiklu 68(2).

Deċiżjoni

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

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

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatriċi**
Ilmentatriċi li tkun uriet traskuraġni grossolana	0%	(100%)
Tnaqqis għax irċeviet l-messaġġ fuq *channel* normalment użat mill-Bank	(50%)	50%
Żieda għax l-Ilmentatriċi ikkoperat b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax tkun irċieviet twissija diretta mill-Bank fl-aħħar 3 xhur	20%	(20%)
Sub-total	0%	(100%)
Tnaqqis għal ċirkostanzi speċjali	(20%)	20%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(20%)**	**(80%)**

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 80% tal-piż u l-20% l-oħra iġorrhom il-BOV.

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

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

L-Arbitru jifhem li waqt it-telefonata konvinċenti mas-suppost rappreżentanta tal-Bank, l-Ilmentatriċi setgħet naqqset jew warrbet is-salvagwardji soliti għax mill-informazzjoni li bdiet tagħtiha dehret telefonata ġenwina.

Għalhekk l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatriċi jitnaqqsilha 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-Ilmentatriċi ġiet iffaċċjata minn xi ħadd li tippersonifika 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 ġa 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 eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

L-argument li l-pagamenti setgħu jsiru biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi u għalhekk hemm bżonn ta' konsiderazzjoni profonda biex filwaqt li jinżammu pagamenti b'xamma ta' frodi, ma niġux restrittivi b'mod li jiġu 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. [24]

B. Dawn il-pagamenti kellhom karatteristiċi strambi biżżejjed biex il-Bank seta' issuspetta li ma kienx kollox normali speċjalment rigward il-temp ta' madwar 23 minuti li matulhom saru ħames pagamenti lill-istess benefiċjarju barrani.

C. Fil-futur qarib (2027/2028) tidħol fis-seħħ leġislazzjoni ġdida permezz tal-PSR u PSD3[25] li fost provvedimenti ġodda jobbligaw lill-banek biex f'każ ta' pagamenti frawdolenti fejn ikun hemm persunifikazzjoni tal-Bank mill-frodist, il-Bank ikun obbligat li jagħmel rifużjoni sħiħa lill-vittma. L-Arbitru jqis li l-banek għandhom jippreparaw 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'

[24] Din it-tip to sistema ġa qed topera permezz ta' 3D secure f'każ ta' pagamenti bil-*card* lill-*merchants* għal xiri *online*.
[25] https://financialregulations.eu/blog/psd3-psr-eu-payment-services-guide

persunifikazzjoni, speċjalment jekk issir b'aktar minn kanal wieħed bħal dan il-każ (SMS u telefonata).

B'kollox, għalhekk, l-Ilmentatriċi hi intitolata għal kumpens ta' 50% tat-telf li sofriet minn pagamenti frawdolenti li ġew iddebitati fil-kont tagħha mal-Bank.[26]

Għaldaqstant, *ai termini* tal-Artikolu 26(3)(c)(iv) tal-Kap. 555 tal-Liġijiet ta' Malta, l-Arbitru qed jordna lil *Bank of Valletta p.l.c.* iħallas lill-Ilmentatriċi is-somma ta' elfejn, erba' mija u sitta u erbgħin ewro (€2,446).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[27] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[28]

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.

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 50% għall-BOV u 50% għall-Ilmentatriċi.

_____

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[26] 50% ta €4892

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

[28] [28] 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.

Nota ta’ Informazzjoni relatata mad-Deċiżjoni tal-Arbitru

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-Ilmentatriċi/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.