Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 148/2025

BO

('l-Ilmentatur')

vs

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

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

Seduta tat-12 ta' Frar 2026

L-Arbitru,

Ra l-Ilment[1] datat 10 Lulju 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €3,819.12 rigward pagamenti (inkluż spejjeż) li saru mill-kont li Ilmentatur għandu mal-BOV favur terzi li wara rriżulta li kien frawdolenti.

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.*

[1]Paġni (P.) 1-7 b'dokumentazzjoni addizzjonali minn P. 8 - 31.

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

- Minkejja diversi twissijiet[2] maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-bank ma jibgħatx *links* fil-messaġġi tiegħu, u li l-klijent għandu jikkomunika mal-bank biss tramite l-App u/jew il-*website* uffiċjali u dan permezz tal-kredenzjali li l-bank ikun ta lill-klijent, il-klijent b’nuqqas ta’ attenzjoni jagħfas il-*link*.

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

- B’riżultat, jinħoloq nuqqas ta’ ftehim bejn il-bank u l-klijent dwar min hu responsabbli jġorr il-piż tal-pagament frawdolenti. Il-klijent isostni li l-bank ma pproteġihx meta ħalla kanal ta’ komunikazzjoni li normalment użat bejn il-bank u l-klijent jiġi ppenetrat mill-frodist, u li l-bank messu nduna li kien pagament frawdolenti għax, ġeneralment, il-klijent ma jkollux storja ta’ pagamenti bħal dawn. Il-bank isostni li l-ħtija hija kollha tal-klijent għaliex permezz ta’ traskuraġni grossolana (*gross negligence*), 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-09 ta’ Mejju 2025, fil-ħin ta’ 10:24, l-Ilmentatur irċieva l-messaġġ frawdolenti fuq il-*mobile* permezz ta’ SMS fejn is-soltu jirċievi notifiki mill-BOV, li infurmah li li ġiet innotata xi attività frawdolenti fuq il-kont tiegħu.[3]

- Iċċekkja l-kont tiegħu u ma ra xejn ħażin jew suspettuż.

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

[3] P. 13

- Daqs 10 minuti wara, ċemplitlu persuna li qalet li kien jisimha Cynthia u li kienet qed iċċempillu mill-BOV fuq numru normali tal-Bank.

- Kellimitu bil-Malti u dehret midħla tal-proċeduri tal-Bank. Kellmitu fuq it-tliet kontijiet li kellu u qaltlu li qed tkellmu fuq kont speċifiku u tatu il-bilanċ li kellu f'dan il-kont. B'hekk dehret li kienet telefonata ġenwina.

- Qaltlu li hi qed tara pagamenti skedati għal xi ġurnata viċina (Wednesday) u qaltlu li la ma kienx talab dawn il-pagamenti, aħjar tikkanċellahom.

- Fil-ħin ta' 10:37, irċieva SMS li talbu jagħfas fuq link li kienet https://BOVHelpSupport.com u talbitu idaħħal il-USER ID u jagħmel proċess ta' awtentikazzjoni ġdida. Sadanittant żammitu 'on hold' għal madwar 5 minuti meta taparsi kienet qed tikkanċella l-pagament frawdolenti. Tatu wkoll referenza '**bov/3245671/paj'** bħala n-numru tal-inċident biex tikkonvinċih dwar l-awtentiċità tagħha.[4] Għafas fuq il-link għall-ħabta ta' 10:52.

- Wara diskussjonijiet tekniċi dwar kif l-aħjar wieħed jista' jnaqqas ir-riskju ta' pagmenti frawdolenti, it-telefonata intemmet fil-ħin ta' 11.03.

- Mir-risposta tal-BOV jirriżulta li waqt jew ftit wara li kienet għaddejja t-telefonata, saru dawn il-pagamenti:

    - €986 fil-ħin ta' 10:54:25

    - €975 fil-ħin ta' 10:57:54

    - €903 fil-ħin ta' 10:58:23

    - €909 fil-ħin ta' 11.09.48

  Sar pagament ieħor fil-ħin ta' 11:10.40 iżda peress li l-Ilmentatur ċempel lill-Bank fil-ħin ta' 11:11, dan il-pagament laħaq inżamm u ma jiffurmax parti mill-ilment.

- L-erba' pagamenti hawn fuq elenkati jammontaw għal €3,773, iżda inġabru lura €53.88 mir-recalls li għamel il-Bank. Kien hemm spejjeż tar-

[4] P. 14

recall ta' €100 u, għalhekk, it-telf totali li għalih qed jintalab rimborż jammonta għal €3,819.12.

- Skont il-BOV, kien fil-ħin ta' 10:43 li saret approvazzjoni permezz ta' *activation code* sigriet mibgħut fuq il-mobile tal-Ilmentatur biex jinbidel it-token li kien awtorizzat japprova pagamenti. Fil-fatt, il-pagamenti ġew approvati minn token b'numru ġdid li jidher li kien ikkontrollat mill-frodisti wara li l-Ilmentatur b'negliġenza kkopera magħhom biex tahom l-*activation code* sigriet.[5] Dan jikkontrasta ma' dak li qal l-Ilmentatur li kien għafas il-link malizzjuż fil-ħin ta' 10:52.

- L-Ilmentatur isostni li l-SMS bl-activation code il-ġdid li l-Bank jgħid li bagħatlu fil-ħin ta' 10:43, huwa qatt ma rċevih u, għalhekk, ma setax jagħti din l-informazzjoni lill-frodist kif qed isostni l-BOV. Għalhekk isostni li dawn il-pagamenti ma kinux awtorizzati minnu skont ir-regolamenti tal-pagamenti u, għalhekk, intitolat għal rifużjoni sħiħa.

- Min-naħa tiegħu, il-Bank isostnu li l-logs tiegħu juri li dan l-SMS intbagħat fuq in-numru tal-*mobile* tal-Ilmenatur reġistrat mal-Bank u l-pagamenti ilmentati setgħu isiru biss jekk min kellu fil-pussess tiegħu il-*mobile device* (l-Ilmentatur) għadda din l-informazzjoni lill-frodist.[6]

  Mitlub jibgħat kopja ta' dan l-SMS, il-BOV qal li huma jkollhom biss il-*logs* li ntbagħat iżda kopja tal-SMS tista' tinkiseb jew mill-Ilmentatur (li jgħid li ma rċevihx), jew mis-service provider tal-*mobile*.[7]

- Sar rapport fl-għassa tal-Pulizija tas-Siġġiewi.[8]

- Ir-recalls li għamel il-BOV biex jipprova jwaqqaf u jirkupra l-pagamenti li laħqu telqu kellhom eżitu żgħir ħafna li lanqas biss kopra l-ispejjeż tar-*recalls*.[9]

[5] P. 150; 154
[6] P. 148 - 149
[7] P. 166
[8] P. 144 - 145
[9] P. 98 -134

L-Ilment

L-Ilmentatur qal li l-BOV offrewlu biss kumpens parzjali ta' 30% skont il-mudell li ppubblika l-Arbitru, iżda huwa jinsisti għal rimborż sħiħ minħabba li jħoss li:

- *"**Lack of Explicit Consent PSD2 Article 64):***

  No valid consent was given for these payments. Consent under PSD2 must be explicit and pre-transaction, not generic or session-based.

- ***Failure to Apply Strong Customer Authentication (PSD2 Article 97, RTS Article 10):***

  Strong Customer Authentication must be applied and dynamically linked to each specific payment (amount and payee). No such dynamic SCA step was performed for these unauthorized transactions.

- ***Inadequate Transaction Risk Analysis (RTS Article 18):***

  The bank is required to conduct real-time risk-based analysis, especially for high-risk or unusual transactions such as new device logins, first-time payees, or large-value SEPA transfers. The fraud involved precisely these high-risk factors, which should have triggered enhanced verification and protective measures.

- ***Data Confidentiality Concerns (PSD2 Article 94, GDPR):***

  The fraudster's detailed insider knowledge of my accounts and security protocols strongly suggests a possible breach of confidential data or a lapse in information security, which is a separate but related failure of the bank's obligations.

Burden of Proof and Gross Negligence

PSD2 places the burden of proof on the bank to demonstrate that the transactions were properly authorised by me, and that no technical or security failure occurred. As per PSD2 Article 72 and established guidance, 'gross negligence' requires clear, intentional disregard for security, not merely being *the victim of sophisticated social engineering. I have at all times acted in good faith and with reasonable care."*[10]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[11] tagħhom, il-BOV qalu:

1. *"Whereas BO ("the complainant") explains that on the 9th of May 2025 at 10:24 he received an SMS appearing to be from BOV regarding suspicious activity on his account. He eventually received a call and was guided to input his internet banking details.*[12] *He states that "two unauthorized payments were processed after the call ended."*[13]

2. *Whereas according to the Bank's records, the abovementioned transactions were duly authorised on the 9th of May 2025 at 10:54, 10:57, 10:58, 11:09 and 11:10.*[14] *As part of the Bank's security system which is in line with the Payment Services Directive 2 (PSD 2), there are various levels of authentication to ensure that the transactions were carried out from credentials and systems in the complainants' name. In fact, the transactions had no indication that they were fraudulent.*

3. *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. As explained, the Bank received legitimate instructions from credentials associated with the complainant and therefore has no obligation to refund the complainant.*

4. *Whereas the Bank implemented the necessary measures to ensure that its' systems are secure and in line with the PSD 2 which provides the following on 'strong customer authentication':*

   '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

[10] P. 16
[11] P. 39 - 46 u dokumenti annessi p. 47 - 137
[12] P. 13 - 14 of the complaint.
[13] P. 14 of the complaint.
[14] DOC.A – Internet Banking Log of the complainant.

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;*[15]

5. *Whereas apart from strong customer authentication, the Bank implements also a system of 'dynamic linking' as outlined in the Commission Delegated Regulation (EU) 2018/389, which supplements the PSD 2. Article 5 provides the following:*

   "Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

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

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

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

   d) any change to the amount or the payee results in the invalidation of the authentication code generated.''

6. *Whereas these payments were approved by the confidential details of the complainant. The Bank had no control over these transfers because they were done without the Bank's intervention. Once the Bank receives legitimate instructions for a 'third party payment' from the adequate channels, the Bank implemented them, as it is reasonably expected that the only person who has access to such confidential details and systems*

[15] Article 4(30) of PSD2.

*is the person with whom they are associated. In fact, this is outlined in the terms and conditions of the Internet Banking system (attached and marked as **'DOC.B'**) 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.''*[16]

> *"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.''*[17]

7. *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 five thousand euro, as can be seen in the highlighted section in the document attached and marked as **'DOC.C'** (this document is accessible from the Bank's website.) 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.*[18]

8. *Moreover, the above-mentioned Commission Regulation provides that the Bank can decide to not apply strong customer authentication for transactions which are considered to have a low level of risk.*[19] *Therefore, one can conclude that when a transaction is considered to be of a higher risk, the Bank should implement the use of strong customer authentication. In*

[16] DOC.B: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 5.
[17] Ibid., page 4.
[18] Article 28(2) of Directive 1 of the Central Bank of Malta which reflects article 52(2) of the PSD 2.
[19] Article 18 of Regulation (EU) 2018/389.

fact, the Bank always implements the use of strong customer authentication 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.

9. *Therefore, it is completely unfounded for the complainant to say that the Bank has "inadequate fraud prevention and security measures,"*[20] *since the Bank adheres to the highest level of security as established by the PSD2.*

10. *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, 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:*

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

*a) **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.***

11. *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**."*

[20] P. 4 of the complaint.

12. *The fact that he 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.''*[21]

13. *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 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.*

14. *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 BO the following SMS's during the year 2024 and beginning of 2025:*

[21] DOC.B: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 7.

25th of 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.*

22nd of July 2024 - *SPOT THE SCAM. BOV will NEVER ask you to unblock accounts, ask for Card details, PIN, Verification codes or Passwords vis telephone or sms/email with links.*

22nd of 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.*

20th of 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.*

15th of 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.*

15. *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.*

16. *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 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.''[22] *It also explains what personal details such scam may ask for which indicates that the communication is not genuine.*

17. *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 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.E2'.***

18. *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 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'*[23] *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.*

---

[22] DOC.D: 'Spot the Scam: Bank impersonation Scams'
[23] https://www.mfsa.mt/publication/the-mfsas-guide-to-secure-online-banking/

19. *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 of the internet banking service and this against the above-mentioned article 45(1) of the Directive.*

20. *Besides this, he 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.*

21. *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 his gross negligence.*

<u>Timeline of Events</u>

22. *Whereas the payments were approved on the 9th of May 2025 10:54, 10:57, 10:58, 11:09 and 11:10 respectively. These kind of payments are processed immediately as can be clearly seen in the terms and conditions marked as* ***'DOC.B'****, particularly in the section entitled 'Cancelling or changing a payment instruction' which provides 'If you ask us to make a payment immediately, we cannot change it or cancel the payment instruction because we start processing it when we receive it.'' The Bank submits that this clause is in conformity with article 80 of the Payment Services Directive 2, entitled 'Irrevocability of a payment order'.*

23. *Whereas when BO called the Bank to report the incident on the same day at 11:29, the representative blocked the internet banking of the complainant and also initiated a recall of the funds. The Bank also managed to cancel one of the payments before the funds left the Bank.*

24. *Whereas on the same day, the Bank also made a recall request to the beneficiary and correspondent banks, which request is made through a digital, internal system between Banks.[24] The outcome of the recall process depends completely on the bank where the funds were received since they would have their internal procedures and rules and BOV has no control*

[24] **DOC.F** – Recall request sent by BOV.

over other banks and therefore cannot dictate how long they take to answer the recall request or what kind of answer they give.

25. *Therefore, the Bank respectfully submits that it did its' utmost to recover the funds and give them to the complainant. Once the Bank had a reply, it informed the complainant accordingly, as can be seen from the attached email marked as* ***'DOC.G'****.*[25]

26. *Finally, the Bank submits that it implements measures to ensure that its' internet banking systems are secure (in line with EU law). The Bank also makes on a continuous basis, various warnings on scams which may be directed towards its' customers. However, this is all futile if customers choose to ignore the terms and conditions of service and any warnings made by the Bank. Thus, the customer cannot expect the Bank to take responsibility for his actions which show gross negligence.*

<u>Conclusion</u>

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

Seduti

Fl-ewwel seduta tad-19 ta' Novembru 2025, l-Ilmentatur qal illi l-aħħar żewġ pagamenti minn dawk ilmentati tħallew jgħaddu wara li kien diġà ċempel lill-Bank biex jirrapporta l-frodi.

Qal ukoll li kien jiftakar li taha *'signatures one or two'* imma mhux erbgħa daqs kemm saru pagamenti frawdolenti.

Qal illi l-messaġġ bil-link frawdolenti daħlet fil-ħin 10:37 waqt it-telefonata, iżda billi 'Cynthia' kienet qed tagħtih informazzjoni kunfidenzjali dwar il-kont tiegħu, allura, huwa ġie konvint li kienet telefonata awtentika u, għalhekk, għafas fuq il-*link*. Qal li minn hemm 'il quddiem, huwa forsi approva pagament wieħed jew tnejn; mill-bqija ma approvax pagamenti aktar u jidher ċar li l-frodisti rreġistraw id-*device* tagħhom fuq is-sistema u, għalhekk, il-pagamenti li saru mhux kollha ġew approvati minnu.

[25] **DOC.G**: Email dated 3rd of June 2025.

Ikkonferma li kien irċieva l-SMSes tal-BOV (elenkati f'paġna 43) li l-Bank ma jibgħatx *links* fuq SMS iżda insista li dan kien japplika meta tirċievi SMS waħdu u mhux meta jkun hemm ukoll telefonata li tagħtik informazzjoni kunfidenzjali li għandu biss il-Bank.

Fit-tieni seduta li nżammet nhar is-06 ta' Jannar 2026, xehed GM, espert mill-BOV fis-sezzjoni ta' pagamenti li qal:

"Ngħid li ili mpjegat mal-Bank of Valletta għal aktar minn 30 sena u ili fis-section tal-Payments madwar ħmistax-il sena.

Ngħid li f'dan il-każ, il-pagamenti saru mill-Internet Banking u ġew awtorizzati through the software token.

Ngħid li ġara f'dan il-każ li ġie ġġenerat activation code u dan l-activation code ġie kkomunikat lill-frodista. Ġaladarba l-frodista jkollu f'idejh il-Login ID u l-generated code jista' jirreġistra l-app fuq il-mobile tiegħu u hekk ikollu kontroll fuq l-Internet Banking ta' dak li jkun.

Ngħid li hemm proċedura sħiħa ta' kif jiġi ġġenerat l-activation code, jiġifieri jekk ma tiġix followed din il-proċedura step-by-step, l-activation code ma jiġix ġenerat. Ġaladarba l-activation code jiġi ġġenerat, xorta jintbagħat fuq il-mobile number li l-bank ikollu rrekordjat miegħu. Infatti, mil-logs jidher li l-activation code intbagħat fuq il-mobile tal-Ilmentatur.

B'xi mod jew ieħor, ġie kkomunikat lill-frodist u minn hemm, il-frodist kellu l-Login ID u l-activation code u ħa over l-Internet Banking tas-Sinjur.

Ngħid li ġaladarba inti ħadt over l-Internet Banking, tista' tilloggja normali, tipprepara t-tranżazzjonijiet, imbagħad inti timxi mal-proċedura normali tas-Signatures biex inti tawtorizzahom.

Ġaladarba inti tiżvela l-activation code, hemmhekk tlift il-kontroll tal-Internet Banking tiegħek.

Ngħid li f'dan il-każ, il-pagamenti kkontestati kollha ġew awtentikati b'dan il-mod. Infatti, anke l-ħinijiet. Jekk wieħed jara t-time sequence minn meta ġie ġġenerat l-activation code at 10.43 u, sussegwentement, it-tranżazzjonijiet l-oħrajn kollha, it-timeline juri dejjem software token generated biex ġew awtorizzati dawn it-tranżazzjonijiet.

Ngħid li SMS alerts jintbagħtu għalkemm il-Bank mhux obbligat li jibgħat SMS alerts u ngħid li SMS alerts intbagħtu għal kull pagament.

Is-Sinjur, as such, m'għamilhomx hu t-tranżazzjonijiet, imma kien il-frodista li awtorizzahom minħabba l-proċedura tal-activation code.

Biex inkun aktar ċar, l-activation code jista' jiġi ġġenerat biss minn tliet metodi: jew tmur fiżikament il-branch, jew mill-Internet Banking jew inkella ċċempel il-Customer Service Centre u hemm proċedura oħra ta' verifiki, eċċ. Però, dejjem jintbagħat fuq il-mobile number tal-klijent.

Ngħid li l-Bank qatt ma jibgħat links jew jitlob credentials permezz ta' SMS jew bit-telefon. Infatti, jekk wieħed jara l-wording tal-warnings li nibagħtu, dejjem ikun hemm highlighted li l-Bank qatt ma jitlob informazzjoni, aħseb u ara kemm jitlob biex jingħata l-activation code.

Mistoqsi jekk fid-9 ta' Mejju 2025 kienx ġie rreġistrat xi device ġdid jew kienx hemm xi device change, ngħid li ġaladarba ġie ġġenerat l-activation code, biex nagħti eżempju, qisek inti bdilt il-mobile u jekk int bdilt il-mobile, l-App tal-BOV ma taħdimx. Allura, trid tgħaddi minn dan il-proċess kollu biex tiġġenera dan l-activation code. Din l-istess ħaġa ġara, ġiet disabled l-App l-antika u ġiet enabled l-App il-ġdida, ovvjament following the safety features u l-proċeduri kollha. Din ma ssirx waħeda.

Ngħid li f'dan il-każ, biex ġie attivat l-activation code, inti għandek l-App fuq il-mobile, u l-ewwelnett, trid taċċessa l-mobile, tidħol fuq l-App biex tiġġenera l-One-Time Password, imbagħad, trid tilloggja fuq l-Internet Banking, tuża l-Login ID u l-One-Time Password, tmur fil-mobile settings u minn hemmhekk tiġġenera l-activation code billi tiffirma t-tranżazzjoni biex jiġi ġġenerat l-activation code. L-activation code jintbagħat fuq il-mobile number li l-Bank ikollu reġistrat fuq is-sistema tiegħu, jiġifieri dejjem fuq il-mobile number li kien hemm qabel. Imbagħad, inti tmur fuq l-App il-ġdida, tuża l-Login ID u l-activation code li jkun bagħatlek il-Bank u minn hemm lil hemm, int ikollok kontroll fuq l-App fuq id-device il-ġdid. Però, jridu jiġu segwiti dawn il-proċeduri kollha.

Ngħid li ladarba jiġi rreġistrat id-device il-ġdid, awtomatikament jiġi deactivated id-device l-antik għax din ma tistax tkun fuq żewġ mobiles.

Ngħid li trid terġa' tilloggja fuq l-Internet Banking. Mingħajr mobile App ma tistax tiġġenera l-activation code, trid terġa' tmur step oħra.

***Il-Bank ma jitlobx aktar mezzi ta' identifikazzjoni u lanqas jagħmel xi pause on payments."*[26]**

Fil-kontroeżami, l-Ilmentatur ċaħad li huwa rċieva SMS bl-*activation code* fuq il-*mobile* tiegħu waqt li GM insista li l-Bank għandu *log* li dan kien intbagħatlu u huwa biss seta' jgħaddi dan l-*activation code* lill-frodist li mingħajru ma kienx jista' jwettaq il-frodi.

L-Arbitru talab lill-Ilmentatur jerġa' jiċċekkja jekk fil-fatt kienx irċieva l-SMS bl-*activation code* kif qed isostni l-Bank u talab lill-BOV jibgħat il-*logs* bil-ħinijiet dwar in-notifika tal-*activation code*.[27]

L-Ilmenatatur baqa' jsostni li dan l-SMS bl-*activation code* qatt ma rċevih[28] filwaqt li l-BOV baqa' jsostni li dan l-*activation code* intbagħat fuq il-mobile tiegħu u l-Ilmentatur biss seta' għadda din l-informazzjoni lill-frodist li mingħajrha ma setax iwettaq il-pagamenti frawdolenti.

Sottomissjonijiet finali

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

Konsultazzjoni mal-*Malta Communications Authority*

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

Mill-konsultazzjoni joħroġ illi dan it-tip ta' frodi magħruf teknikament bħala *Spoofing* u *Smishing* jew kollettivament bħala *Social Engineering Scams,* ma jippermettix lill-Bank li jieħu xi prekawzjoni (għajr ovvjament twissijiet effettivi biex il-klijenti joqgħodu attenti) biex il-frodist ma jkunx jista' juża dan il-kanal ta' komunikazzjoni biex jippersonifika l-Bank u jiffroda lill-klijenti.

---

[26] P. 146 - 148
[27] P. 152 - 154
[28] P. 160

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

[29] 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[30] 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 responsabbiltà 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.[31] [32]

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:

[30] Article 64 of PSD 2

[31] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)

[32] PSD 2 Eu 2015/2366 Artiklu 68(2).

	Perċentwal ta' ħtija tal-Fornitur tas-Servizz	**Perċentwal ta' ħtija tal-Ilmentatur**
Ilmentatur li jkun wera traskuraġni grossolana	0%	100%
Tnaqqis għax irċieva l-messaġġ fuq *channel* normalment użat mill-Bank	50%	(50%)
Żieda għax l-Ilmentatur ikkopera b'mod sħiħ biex sar il-pagament ilmentat	(30%)	30%
Żieda għax ikun irċieva twissija diretta mill-Bank fl-aħħar 3 xhur	(20%)	20%
Sub-total	0%	100%
Tnaqqis għal ċirkostanzi speċjali	20%	(20%)
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	20%	(20%)
TOTAL FINALI	**40%**	**60%**

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 60% tal-piż u l-40% l-oħra 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 jigu approvati l-pagamenti inkluż b'mod partikolari l-*activation code* biex jinbidel it-token li japprova pagamenti.

L-Arbitru jinnota iċ-ċaħdiet kategoriċi ta' l-Ilmentatur f'dan ir-rigward iżda l-bilanċ tal-probabbilità jikkonsidrah favur l-argument tal-Bank li dan l-SMS kien irċevih u bilfors kien ikkomunikah lill-frodist għax huwa biss kellu dan l-*activation code* fil-pussess tiegħu u mingħajru l-frodist ma kienx jista' jwettaq għemilu qarrieqi.

Dan huwa sostnut ukoll mix-xhieda tal-Ilmenatur fejn qal:

***"Ngħid li kulma għamilt dħalt darba u Signatures għamilt one, maybe two. M'inix ċert."'*[33]**

L-Arbitru jifhem li waqt it-telefonata konvinċenti ta' Cynthia, l-Ilmentatur kien konvint li din kienet telefonata ġenwina mill-BOV u, għalhekk, is-salvagwardji soliti ġew imwarrba.

Peress li l-BOV bagħat SMSes regolari biex iwissi kontra li klijenti jagħfsu links fuq SMS li jkun jidher ġej mill-BOV ma jistax inaqqas il-piż tal-ħtija ta' negliġenza grossolana peress li kien avżat sew b'mod dirett.[34]

Iżda 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' 40%, jiġifieri 20% aktar mill-20% normalment spjegati fil-mudell.

---

[33] P. 139

[34] P. 43 juri li l-aħħar SMS ta' twissija kien intbagħat fil-15 t'April 2025 anqas minn xahar qabel ma seħħ dan il-każ.

Dan huwa l-ewwel 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.

Kif din il-persuna 'Cynthia' kellha aċċess għal informazzjoni interna u kunfidenzjali tal-Bank dwar klijenti żgur mhux ħtija tal-Ilmentatur u sta għall-Bank biex jagħmel l-investigazzjonijiet dwar dan, għax l-Arbitru għandu ilmenti oħra li juru li dan ma kienx xi każ uniku.

F'dan l-aġġustament, minħabba ċirkostanzi speċjali, l-Arbitru qed jieħu wkoll kunsiderazzjoni li huwa kien diġà esprima opinjoni 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* li, allura, l-istess numru tal-SMS baqa' rreġistrat mal-Bank, iżda fil-proċess kien hemm bidla fis-*software token* li jawtorizza l-pagamenti.[35]

L-Arbitru jirrakkomanda li meta jkun hemm reġistrazzjoni ta' *software token* ġdid, għandu wkoll ikun hemm eżercizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu.

L-argument li dan seta' jsir biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi, kif jixhed dan il-każ fejn jidher li kellhom aċċess għal informazzjoni interna u kunfidenzjali dwar klijenti tal-Bank.

Għalhekk jeħtieġ li l-Bank iżid il-kontrolli kif indikat billi meta jiġi rreġistrat *token* ġdid jiġu mwaqqfa pagamenti għal ftit ħin sa ma jsir kuntatt mal-klijent permezz ta' telefonata diretta.

L-Arbitru ma għandux kompetenza li jinvestiga kif informazzjoni kunfidenzjali ħarġet mill-Bank.[36] Dan huwa xogħol il-Bank u xogħol il-Pulizija biex jinvestigaw kif dan seta' jiġri.

---

[35] P. 149; 150; 154; 166 (5 ii – iii)

[36] L-Arbitru ħa inizjattiva biex l-Assoċjazzjoni tal-Banek toħroġ twissija urġenti dwar telefonati frawdolenti bħal f'dan il-każ.

Iżda l-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat 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.

L-Arbitru qed ukoll jiskuża l-Ilmentatur b'20% għax ma giet ipprovduta l-ebda evidenza li kien midħla ta' kif isiru pagamenti *online bl-internet banking*, jew li kien għamel xi pagament simili fit-12-il xahar qabel seħħ dan il-każ.

B'kollox, għalhekk, qed jiġi intitolat għal kumpens ta' 60% tal-pagamenti frawdolenti li ġie debitat lill-kont tiegħu.

L-Arbitru ma jsibx li -Bank naqas b'xi mod li pagamenti ma ġewx imwaqqfa mill-*payment monitoring systems* li jopera. Meta pagamenti jsiru fi żmien ftit minuti diffiċli li l-*monitoring system* tiskatta biex jitwaqqfu il-pagamenti għax ma hemmx aspettativa (s'issa) li dawn il-mekkaniżmi jaħdmu *'real time'* b'mod istantanju. U, f'dan il-każ, il-pagamenti kienu għal ammonti relattivament żgħar li ma jqajmux suspett istantanju.

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' elfejn mitejn u wiehed u disghin ewro punt erbgha sebgha (€2291.47).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.15% fis-sena[37] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv. [38]

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

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

[38] [38] Fil-każ li din id-deċiżjoni tiġi appellata, u tali deċiżjoni tkun ikkonfermata fl-appell, l-imgħax pagabbli jiġi kkalkolat mid-data tad-deċiżjoni tal-Arbitru.

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 60% għall-BOV u 40% 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.