Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 118/2026

ZO
('l-Ilmentatriċi')

vs

Bank of Valletta p.l.c.
(C 2833)
('BOV', 'il-Bank' jew 'il-Fornitur tas-Servizz')

Seduta tal-20 ta' Novembru 2026

L-Arbitru,

Ra l-Ilment[1] datat 17 t'April 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi t-telf sħiħ li sofriet meta saru żewġ pagamenti frawdolenti ta' €4,600 u €200 mill-kont tagħha mal-BOV.

Il-pagamenti saru fl-14 t'Ottubru 2025 filgħaxija, fil-ħin ta' bejn 21:32 u 21:34[2] favur **Fofana Dahba** f'kont b'IBAN jibda DE (Germanja) u b'narrazzjoni ta' ***'Family/Friend'*** u ***'Loan Repayment'***[3]. Fl-i*statement* dawn jidhru bid-data tal-15 t'Ottubru 2025[4] u l-SMS tal-Bank bin-notifika tal-pagamenti irċevietu fil-ħin ta' 07:03 tal-15 t'Ottubru 2025[5].

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

[1] Paġni (P.) 1 - 7 b'dokumentazzjoni addizzjonali minn P. 8 - 52.
[2] P. 66
[3] P. 20; 22
[4] P. 156
[5] P. 135

- 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[6] 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:

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

- Fl-14 t'Ottubru 2025, fil-ħin ta' 19:57, irċeviet messaġġ biex javżawha li numru ġdid kien ġie miżjud.[7] Dan daħal fuq il-kanal ta' SMS fejn normalment tirċievi notifiki mill-Bank.
- Wara li rat il-messaġġ frawdolenti li kien jistedinha tagħfas *link* jew iċċempel numru, hija għafset il-*link*[8] u daħlet ġo *website* li ħasbitha ġenwina ta' BOV.
- Ġiet indotta ddaħħal in-numru tal-*mobile* u wara ftit ċemplitilha persuna, mara, fuq numru jixbaħ dak li fuqu kienet tirċievi SMS mill-BOV. In-numru kellu żero żejjed iżda hi xorta emmnet li kienet telefonata ġenwina mill-Bank. Ammettiet li hi daħħlet ukoll il-*User ID* u l-*password*.[9]
- Waqt it-telefonata irċeviet ukoll SMS mill-BOV fil-ħin ta' 20:40 fejn ġiet informata b'*activation code* valida għal siegħa.[10] Ammettiet li din daħħlitha fil-*website* li ħasbet li kienet ta' BOV.
- Permezz tal-kxif tal-*password* u l-*activation code* skatta proċess biex il-frodist jaqleb il-*BOV App* fuq *device* tal-frodist u minn hemm 'il quddiem seta' jagħmel pagamenti daqslikieku (f'għajnejn BOV) kienet qed tagħmilhom l-Ilmentatriċi.
- L-għada, meta kmieni irċeviet l-SMS li jinnotifikaw il-pagamenti, għamlet rapport kemm lil BOV kif ukoll lill-Għassa tal-pulizija[11].
- Għal xi raġuni mhux ċara, r-*recall* min-naħa tal-Bank skatta biss fis-7 ta' Jannar 2026 u dan ma rnexxiex.
- Fid-9 t'April 2026, BOV informawha li, skont il-mudell tal-Arbitru, offrewlha rifużjoni parzjali ta' 40% (€1,920)[12], iżda hi rrifjutat u fetħet dan l-ilment għax trid rimborż sħiħ ta' €4,800[13].

[7] P. 41
[8] P. 12; 130
[9] P. 131
[10] P. 134
[11] P. 12 - 14
[12] P. 10
[13] P. 3

L-Ilment

L-Ilmentatriċi qed titlob kumpens sħiħ għax skont hija:

> *"1. There was no assistance to help cancel the transactions in the evening. the payments could have been cancelled.*
>
> *2. the instant/immediate payment system was implemented a week before this scam, which made it easier for scammers.*
>
> *3. after I reported immediately, police report and at the Bov branch, they did not apply for recall of funds until after 3 months had passed.*
>
> *4. I asked that the immediate payment system should be optional as I do not want it to be Eur5000, this was rejected. this system accomodates the scammers but not the clients.*
>
> *5. As per similar experiences of scam victims, to intentional fraud, that we are seeing on local news, my family and I have sufferred not only financial exploitation but we experienced severe distress in these past months.*
>
> *6. Bank of Valletta offered a refund of 40 percent but I believe I am entitled to more than this amount."*[14]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[15] tagħhom datata 7 ta' Mejju 2026, BOV qalu:

> *"4. Whereas according to the Bank's records*[16] *the transactions effected on the 14th October 2025 in the amount of €4,600 and €200 were duly authorised at 21:32:18 and 21:34:35 respectively through the Complainant's banking channels following successful authentication. As part of the Bank's security framework, which is fully aligned with the requirements of the Payment Services Directive 2 (PSD2),*

[14] *Ibid*.
[15] P. 56 - 64 u dokumenti annessi p. 65 - 129
[16] Doc. A

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 it was fraudulent at the time of processing;

5. *Whereas at the outset, the Bank submits that the payments in question were processed as SEPA Instant Payments, which are designed to be irrevocable and settled within seconds of authentication. While recall requests were submitted and multiple follow-up reminders were issued to the beneficiary bank, recovery of funds is not guaranteed under the SEPA Instant framework, as the recipient may withdraw the funds immediately upon receipt. In this case, despite the Bank's efforts to initiate recalls and pursue recovery, no funds were returned, and the process was ultimately closed due to the absence of a substantive response from the beneficiary bank. The Complainant has stated that she does not agree with the compulsory nature of instant payments and the applicable transfer limits, arguing that these features facilitated the fraud and should have been optional. However, it is significant to note that the Bank's implementation of SEPA Instant Payments was not discretionary, but a direct result of binding European Union legislation. The Instant Payments Regulation[17] requires all payment service providers in euro area Member States, including the Bank, to offer instant euro payment services. The Bank is therefore legally obliged to enable instant payments;*

6. *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"*

[17] Regulation (EU) 2024/886

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*[18]*"*

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 moreover the abovementioned Commission Regulation provides that the Bank can decide not to 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 SCA;*

10. *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*

[18] Article 4(30) of PSD2.

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 was duly authorised following successful validation of the Complainant's credentials, and there was no indication of fraud at the time of processing;

11. *Whereas the Bank's terms and conditions state that:*

> *"All payments, Instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your security credentials [...] are deemed as binding on you. You authorise us to act on any Instruction that we receive through the Channels [...] You will be liable for any transactions that we carry out on your behalf.*[19]*"*
>
> *"You will however be unlimitedly responsible for all transactions carried out via the Channels prior to notification to us [...] if you have: [...] not notified us immediately of having suspicions or noticing irregular or unauthorised transactions or on becoming aware that your BOV Channel Credentials have become compromised, lost or stolen; [...] acted in any other way with gross negligence or fraudulently."*[20]
>
> *"[...] once the payment is authorised following the verification of payee check, the Bank does not bear liability if the payment is credited and sent to the wrong beneficiary."*[21]
>
> *"We will not be responsible nor liable for losses or costs which you may suffer [...] if we fail to comply*

[19] Doc. B, Page 24.
[20] Doc. B, Page 25.
[21] Doc. B, Page 18.

with any of our obligations due to [...] unforeseeable circumstances outside our reasonable control [...] or due to our obligations to comply with any applicable law or regulations [...] unless any such losses, costs, damages, actions or expenses arise due to the gross negligence of the Bank."[22]

12. *Whereas the Bank further submits that the disputed transaction fell within the daily and per-transaction limits*[23]*, wherein the maximum permitted for third party payments via personal internet banking is €5,000 per transaction and up to a maximum of €5,000 per day. The payments in question, being €5,000, was therefore within such parameters;*

13. *Whereas without prejudice to the above, if the Complainant is alleging that this transaction was not authorised by her, then the Bank is still not obliged to refund her, since even if she 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

[22] Doc. B, Pages 23 to 24.
[23] Doc. C (https://www.bov.com/bov-digital-banking-limits)

receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe."

14. *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"

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 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;*

16. *Whereas it is significant to state that prior to the incident, the Complainant's registered number received twelve anti-fraud SMS warnings from the Bank between November 2023 and September 2025 consistently instructing her 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. DO NOT 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 weblinks that ask you to provide card details, PIN, verification codes or on-line banking passwords."

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

(iv) *23rd July 2024 – "SPOT THE SCAM. BOV will NEVER ask you to unblock accounts, ask for Card Details, PIN, Verification codes or Passwords via telephone or sms/email with links."*

(v) *23rd October 2024 – "SPOT THE SCAM. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests."*

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

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

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

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

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

17. *Whereas in addition to the above SMS warnings, the the Bank's anti-fraud communications have consistently cautioned customers never to disclose sensitive information, such as passwords, PINs, verification codes, or online banking credentials, over the phone. Customers are regularly reminded that the Bank will never request such information via telephone, and that any such request should be treated as suspicious and reported immediately;*

18. *Whereas moreover 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. 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 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. D**'.*

19. *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.

20. *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 and this against the above-mentioned article 45(1) of the Directive;*

21. *Whereas besides this, she also acted against article 45(2) of the Directive because she did not take all the reasonable steps to keep his bank transfer number 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;*

22. *Whereas therefore, any alleged fraud occurred due to the participation of the Complainant who provided confidential information to a fraudster and followed the instructions given to him. All this contributed to her gross negligence."*[24]

Seduti

Fl-ewwel seduta tal-10 ta' Ġunju 2026, l-Ilmentatriċi spjegat il-każ tagħha kif ġa riprodott hawn fuq. Dwar id-dewmien fir-*recall* qalet:

"Ngħid li l-għada filgħodu, x'ħin mort il-bank, min kellmitni tal-bank, u għamlitli l-affarijiet, qaltli, 'Issa ħa nipprova napplika

[24] P. 57 - 64

għar-recall of funds.' U jien ħallejt f'idejha. Wara xi xahar jew xahrejn, ċempilt u qaluli, 'Għax dak jieħu ż-żmien, jieħu ż-żmien.'

Imbagħad, f'Jannar ċempluli u qaluli li kien hemm xi misunderstanding jew l-email marret għand ħaddieħor, u qaltli, 'Ser napplikawlek illum.'

Ngħid li dan kien Jannar. Bi żball, dakinhar m'għamluhx.

Imbagħad, qaluli, li ma kienx hemm funds."[25]

Fil-kontroeżami qalet:

"Mistoqsija x'dettalji daħħalt meta dħalt fil-fraudulent website, naħseb li t-telephone number biss.

Ngħid li biex inħassar dawk l-affarijiet li hemm, qaltli li ser tibgħatli code, daħħalt il-code.

Mistoqsija qabel daħħaltx il-User ID, ngħid li iva, daħħalt il-User ID u l-password.

Mistoqsija jekk dan l-activation code ikkomunikajtux lilha, ngħid le, daħħaltu fis-sistema.

Mistoqsija ppruvajtx inċempel lill-bank qabel ma daħħalt u tajt ċertu informazzjoni personali tiegħi – meta rċevejt il-link u bdew jistaqsu għal ċertu affarijiet personali – ngħid li le, ma ċempiltx il-bank.

Qed niġi referuta għar-risposta tal-bank (paġni 61 – 62) fejn hemm lista ta' SMSs li l-bank bagħat fuq il-mobile tiegħi mill-11 ta' Novembru 2023 sa l-aħħar wieħed qabel sar dan l-inċident, fl-4 ta' Settembru 2025.

Mistoqsija niftakarx irċevejtx dawn l-SMSs, ngħid li iva, niftakar li rċevejthom. Imma jien ma kontx naf li meta jkun hemm fraud, tista' ċċempillek persuna bil-Malti u tkun taf dawk id-dettalji kollha.

[25] P. 131

Nikkonferma li għidt li ċempilt lill-Customer Care u infurmawni li ma setgħux jgħiduli xi transactions saru bil-lejl.

Mistoqsija nikkonferma li ħadu azzjoni biex jipprevenu li jsiru aktar tranżazzjonijiet, ngħid, iva.

Mistoqsija qattx għamilt pagamenti online, ngħid, iva."[26]

Wara s-seduta, l-Ilmentatriċi bagħtet kopji tal-SMS kif mitluba mill-Arbitru[27]. BOV bagħtu kopja ta' *statement* tal-kont għall-perjodu minn Jannar 2025 sa Ġunju 2026.[28] Dawn juru li l-Ilmentatriċi kienet familjari ma' kif tagħmel pagamenti *online* mis-sistema ta' BOV[29].

Fit-tieni seduta li nżammet fil-25 ta' Settembru 2026, il-Bank ressaq ix-xhieda ta' Michael Gatt, espert fis-sistema tal-pagamenti elettroniċi tal-BOV. Spjega kif f'għajnejn il-Bank, il-pagament ilmentat deher awtorizzat mill-Ilmentatriċi u dan skont ir-regoli Ewropej dwar pagamenti. Spjega li f'dan il-każ jidher li l-Ilmentatriċi kkoperat mal-frodista billi daħħlet il-kodiċi mitlub, li hija biss kellha, biex seta' jsir pagament *Instant Payment*. Dan sar permezz ta' bidla fid-*device* nhar l-14 t'Ottubru 2025 permezz ta' *activation code* li l-Ilmentatriċi talbet mis-sistema Signature 1 tal-*BOV App*[30].

Fil-kontroeżami, x-xhud ikkonferma li x-xhieda tiegħu hija bbażata fuq *logs* li ġew mgħoddija mill-kollegi tiegħu.

Xehed ukoll Luke Cutajar li kien inkarigat mir-*recall* tal-pagamenti u qal li r-*recall* sar fis-7 ta' Jannar 2026 minkejja li l-pagament kien sar f'Ottubru 2025. Iżda d-dipartiment tiegħu kien biss infurmat meta sar ir-*recall* fejn dan ma kellux suċċess u, fi Frar 2026, il-każ ingħalaq għax ma rċevewx risposta minkejja diversi *reminders*. Qal ukoll:

"Ngħid li l-pagament sar fl-14 t'Ottubru, għandi email li min-naħa tal-branch ikkuntattjat l-AFC imma aħna ġejna kkuntattjati fis-7 ta' Jannar 2026. Ngħid li xorta waħda kienet diffiċli ħafna sempliċiment għax kien

[26] P. 131 - 132
[27] P. 133 - 135
[28] P. 153 - 156; p. 137 - 142
[29] P. 154; 155; 160
[30] P. 163

Instant Payment. Anke kieku kienet dak il-ħin jew l-għada, xorta waħda kienet tkun diffiċli ħafna."[31]

Xehed ukoll Keith Vella, *Deputy MLRO* u *Head Transaction Monitoring Proactive Analysis* tal-BOV, li spjega l-*monitoring payments system* li jopera l-Bank biex jipprevjeni l-frodi.

"Ngħid li dan il-każ jinvolvi żewġ tranżazzjonijiet allegatament frawdolenti li seħħew minn kont tal-klijenta fejn mill-kont li jispiċċa ...1162, fil-15 t'Ottubru ħarġu żewġ tranżazzjonijiet: waħda ta' €4,600 u l-oħra ta' €200 lejn bank fil-Ġermanja. L-IBAN hu Ġermaniż.

Ngħid li dawn l-ewwel żewġ tranżazzjonijiet marru ġol-Berliner Sparkasse Landesbank Berlin. L-instructions kienu ħarġu fl-14 t'Ottubru u l-Value Date huwa l-14 t'Ottubru imma fl-istatement huma mniżżlin fil-15 t'Ottubru.

Ngħid li fis-sistemi tagħna ma kien hemm l-ebda impediment biex dawn iż-żewġ tranżazzjonijiet joħorġu minn ġol-kontijiet tal-klijenta. Ma kien hemm l-ebda impediment fuq il-klijenta tagħna u lanqas fuq min kien ser jirċevihom.

Ngħid li l-Ġermanja hija kkunsidrata bħala pajjiż low risk.

Ngħid li l-mod kif ġew keyed dawn it-tranżazzjonijiet mill-klijenta biex finalment jiġu executed mill-bank huwa l-istess mod kif il-klijenta, fit-30 ta' Ġunju 2025, mill-kont tagħha li jispiċċa ...9686 kienet għamlet tranżazzjoni ta' €10,000 lejn kont ġewwa l-APS ġewwa Malta.

Dan jista' jiġi kkonfermat mill-istatement mibgħut lill-Arbitru.

Ngħid li fil-25 ta' Ġunju 2025, il-klijenta, mill-kont tagħha li jispiċċa ...1162, għamel ukoll tranżazzjoni lejn il-Kanada li għalkemm l-ammont tagħha kien ta' €525, xorta kien ukoll within

[31] P. 166

> ***the profile li l-klijenta qiegħda tibgħat jew tagħmel tranżazzjonijiet ma' persuni jew klijenti oħra barra minn Malta.***
>
> ***Ngħid li dejjem irridu nżommu ġo moħħna li s-sistema taħdem on a risk-based approach, li l-bank isegwi l-istruzzjonijiet u l-gwidi li joħorġu regolaturi kemm lokali kif ukoll internazzjoniali. U dawk iż-żewġ tranżazzjonijiet li qed nitkellmu fuqhom, is-sistema ma ħassitx li kellha twaqqafhom jew inkella ttella' xi alerts fuqhom wara li jkunu mgħoddija."***[32]

Waqt il-kontroeżami qal:

> ***"Mistoqsi hux korrett jingħad li dawn kienu l-uniċi żewġ transactions li kien hemm għal barra minn Malta minn dan il-kont partikolari li semmejt, ngħid li minn dak il-kont li ħarġu dawn iż-żewġ tranżazzjonijiet allegatament frawdolenti, kienu l-uniċi tnejn, at least fl-aħħar ħames snin, li kienu transacted lejn pajjiżi barra minn Malta.***
>
> ***Imma s-sistema ma tarax biss accounts individwali per se imma wkoll ir-relazzjoni li l-bank għandu mal-klijent, jiġifieri, at a customer level, is-sistema tara l-kontijiet kollha tal-klijent ukoll barra dawk individwali."***[33]

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

[32] P. 164
[33] P. 164 - 165

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 użat biex jasal għal deċiżjoni dwar kif ser isir *'apportionment'* tal-konsegwenzi tal-frodi. Il-mudell fih ukoll diversi rakkomandazzjonijiet biex il-banek ikomplu jsaħħu l-protezzjoni tal-konsumatur kontra frodisti li kulma jmur dejjem isiru aktar kapaċi u kreattivi.

Iżda l-Arbitru jħoss il-bżonn jemfasizza li filwaqt li huwa minnu li l-banek ma għandhomx mezz kif jipprojbixxu li jsir *spoofing/smishing* fil-mezzi ta' komunikazzjoni li jużaw mal-klijenti, iridu jagħmlu iżjed biex iwissu b'mod effettiv lill-klijenti biex joqgħodu attenti; biex ma jagħfsux *links* li jkunu f'dawn il-messaġġi avolja jkun jidher li ġejjin mill-bank konċernat fuq il-mezz li normalment juża l-bank biex jibgħat messaġġi lill-klijenti.

Mhux biżżejjed li jagħmlu avviżi kontinwi fuq il-*website* tagħhom. Mhux biżżejjed li joħorġu twissijiet fuq il-*mass media* jew *social media.* Il-konsumatur huwa impenjat bil-problemi tal-ħajja ta' kuljum u ma għandux jiġi pretiż li billi jsir avviż fuq il-*website*, fil-ġurnali/TV jew fuq il-paġna ta' *Facebook* tal-bank, b'daqshekk il-konsumatur jinsab informat.

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

Fuq kollox, il-PSD 2 tagħmilha ċara[35] 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, jagħmel awtorizzazzjoni speċifika tal-pagament *a favur* tal-frodist.

Dan il-fatt huwa wkoll inkluż fil-mudell.

Il-mudell jagħti wkoll konsiderazzjoni għal xi ċirkostanzi partikolari tal-każ. Jista' jkun hemm ċirkostanzi partikolari fejn il-messaġġ tal-frodist ikun anqas suspettuż.

Il-mudell għandu wkoll għarfien dwar jekk l-Ilmentatriċi tkunx midħla tas-sistemi ta' pagamenti *online* mal-Bank billi tkun għamlet 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.[36] [37]

Deċiżjoni

L-Arbitru jiddeċiedi skont kif provdut f'Artikolu 19(3)(b) tal-Kap. 555 tal-Liġijiet ta' Malta b'referenza għal dak li, fil-fehma tiegħu, ikun ġust, ekwu u raġonevoli fiċ-ċirkostanzi u merti sostantivi tal-każ.

[34] Deċiżjoni 13 ta' Settembru 2018 C-54/17
[35] Article 64 of PSD 2
[36] (EU) 2018/389 tas-27 ta' Novembru 2017 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[37] PSD 2 UE 2015/2366 Artikolu 68(2).

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 il-messaġġ fuq *channel* normalment użat mill-Bank	(50%)	50%
Żieda għax l-Ilmentatriċi kkoperat b'mod sħiħ biex sar il-pagament ilmentat	30%	(30%)
Żieda għax tkun irċeviet 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 jġorrhom il-BOV.

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

F'dan il-każ partikolari, il-pagamenti ilmentati saru billi b'xi mod il-frodist(a) saret taf il-*User ID*, il-*One Time Password* u saħansitra l-kodiċi biex ġew approvati l-pagamenti ilmentati.

In vista ta' din ix-xhieda u tal-fatt li din l-informazzjoni kienet biss fil-pussess tal-Ilmentatriċi u setgħet tiġi a konoxxenza tal-frodist(a) biss jekk l-Ilmentatriċi

żvelathomlha, l-Arbitru jikkonkludi li l-Ilmentatriċi kkoperat mal-frodist(a) billi għaddiet kull informazzjoni li kienet meħtieġa biex jiġu approvati l-pagamenti ilmentati.

Fix-xhieda tagħha l-Ilmentatriċi ammettiet dan billi qalet:

> ***"Allura, jiena ħsibtha xi ħaġa ġenwina. Ngħid li f'dan l-SMS kien hemm li xi ħadd ġie added fuq il-kont tiegħi u biex tagħfas xi ħaġa biex tikkanċella din il-ħaġa, trid tagħfas din il-link. U jien għafast din il-link.***
>
> ***Wara li għafast din il-link ċemplitli waħda li kienet tinstema' ġenwina ħafna. Bdiet tistaqsini ħafna affarijiet.***
>
> ***Ngħid li l-messaġġ kien 'If NOT authorised, visit https://loginat-bov.com (paġna 41 tal-proċess), u għafast il-link u ġejt diverted għal sit oħra li kien qisu tal-Bank of Valletta, bil-kulur u x'naf jien.***
>
> ***Imbagħad, qaluli biex indaħħal il-mobile number u ċemplitli din is-sinjorina minn fuq numru li dak il-ħin kien jixbaħ l-istess numru fejn nirċievi l-messaġġi. Kien jixbħu ħafna, kien hemm żero żejjed imma jien ħsibt li qed iċempluli mill-bank. U din il-mara bagħtitli SMS b'code. Jien poġġejt dak l-activation code imma jien ma kontx naf x'kien qed jiġri."***[38]

L-Ilmentatriċi ammettiet ukoll li kienet irċeviet SMS ta' twissija minn BOV biex ma tagħfasx fuq *links* inklużi f'SMS anke jekk dawn jidhru li ġejjin mill-Bank.

Qalet:

> ***"Mistoqsija niftakarx irċevejtx dawn l-SMSs, ngħid li iva, niftakar li rċevejthom. Imma jien ma kontx naf li meta jkun hemm fraud, tista' ċċempillek persuna bil-Malti u tkun taf dawk id-dettalji kollha."***[39]

Qalet ukoll:

"Mistoqsija qattx għamilt pagamenti online, ngħid, iva."[40]

[38] P. 130
[39] P. 132
[40] *Ibid*.

Għalhekk l-Arbitru ma jagħtix solliev lill-Ilmentatriċi fuq dawn il-kriterji inklużi fil-mudell.

Iżda l-Arbitru jħoss li f'dan il-każ hemm ċirkostanzi speċjali li jimmeritaw li l-Ilmentatriċi jitnaqqsilha l-piż ta' negliġenza grossolana b'doża ta' 40%, jiġifieri 20% aktar mill-20% normalment spjegati fil-mudell.

Din iż-żieda hija ġustifikata minn dawn il-fatturi:

1. Dan huwa każ fejn il-frodist mhux biss bagħat SMS qarrieq iżda sostna l-kredibbiltà 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 jippersonifika b'mod espert lill-Bank permezz ta' telefonata *'live'*, allura, l-SMS bil-*link* frawdolenti tidher anqas suspettuża, minkejja t-twissijiet li l-Bank kien ħareġ. 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.

2. F'dan l-aġġustament, minħabba ċirkostanzi speċjali, l-Arbitru qed jieħu wkoll konsiderazzjoni 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* 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 *unenrolment* minn fuq id-*device* ta' qabel għax il-*mobile app* tista' tkun reġistrata fuq *device* wieħed biss) għandu wkoll ikun hemm eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

   L-argument li l-pagamenti setgħu jsiru biss jekk il-klijent jikkomunika l-*activation code* lill-frodisti huwa validu. Iżda l-frodisti qed isiru dejjem aktar kreattivi u għalhekk hemm bżonn ta' konsiderazzjoni profonda biex

> filwaqt li jinżammu pagamenti b'xamma ta' frodi, ma niġux restrittivi b'mod li jiġu mblukkati pagamenti ġenwini li ovvjament huma f'maġġoranza kbira.
>
> Hemm eżempji ta' istituzzjonijiet finanzjarji u banek li għandhom sistemi ta' pagamenti b'teknoloġija avvanzata, fejn f'każ serju ta' dubju jintbagħat SMS fuq il-*mobile* reġistrat, 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.[41]

L-Arbitru ma jsib ebda nuqqas da parti tal-BOV dwar *transaction monitoring* peress li l-pagamenti kienu fil-limitu ta' pagamenti akkordat ta' €5,000. Apparti minn hekk, l-Ilmentatriċi għamlet pagament *online* ta' €10,000 fit-30 ta' Ġunju 2025[42], ieħor ta' €221.78 fl-20 ta' Jannar 2025[43] u pagament estern ta' dollari Kanadiżi CAD 816.45 fil-25 ta' Ġunju 2025[44]. Għalhekk lanqas jista' jingħad li dawn kienu l-ewwel pagamenti esterni li qatt għamlet.

L-Arbitru mhux jagħmel aġġustament minħabba li l-*recall* sar diversi xhur wara li l-każ kien ġie rrapportat. Filwaqt li BOV għandhom tort li l-proċess tar-*recall* beda daqstant tard, ma jirriżultax li dan seta' kien xi detriment għall-Ilmentatriċi għax ir-rapport tagħha sar diversi sigħat wara li l-pagamenti kienu saru u, bis-sistema tal-*Instant Payments* li tibgħat il-flus f'affari ta' sekondi, anke kieku r-*recall* sar immedjatament wara r-rapport, huwa ferm improbabbli li kien ikollu eżitu aħjar.

Għalhekk il-mudell qed jiġi rivedut hekk:

[41] Dan it-tip ta' sistema diġà qed topera permezz ta' *3D Secure* f'każ ta' pagamenti bil-*card* lill-*merchants* għal xiri *online*.
[42] P. 160
[43] P. 154
[44] P. 155

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

B'kollox, għalhekk, l-Ilmentatriċi hija intitolata għal kumpens ta' 40% tat-telf li sofriet mill-pagamenti frawdolenti li ġew iddebitati fil-kont tagħha mal-Bank.[45]

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 s-somma ta' elf, disa' mija u għoxrin ewro (€1,920).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.65% fis-sena[46] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[47]

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

[45] 40% ta' €4,800

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

[47] 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.

Fl-aħħarnett, l-Arbitru jirreferi għal rapporti mhux konfermati li l-pulizija rnexxielhom 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 possibbiltà 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 40% għall-BOV u 60% għall-Ilmentatriċi.

_____

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

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 anonimizzati skont l-artikolu 11(1)(f) tal-Att.