Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 104/2026

CO

('l-Ilmentatriċi')

vs

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

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

Seduta ta' 9 Settembru 2026

L-Arbitru,

Ra l-Ilment[1] datat 07 April 2026 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi t-telf li sofriet meta sar pagament frawdolenti ta' €5,000 mill-kont tagħha mal-BOV.

Il-pagament sar fid-19 ta' Jannar 2026 fil-ħin ta' 14:42 favur X.X.X. Formosa f'kont ma' ditta lokali liċenzjata (*Moneybase*).

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 l-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 - 79.

– 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-19 ta' Jannar 2026, fil-ħin ta' 13:43 irċeviet messaġġ biex javżawha li n-numru 79020447 kien ġie miżjud.[3] Dan daħal fuq il-kanal ta' SMS fejn normalment tirċievi notifiki mill-Bank.

– Wara li rat il-messaġġ frawdolenti fil-ħin ta' 14:20, ċemplet lill-*call centre* tal-BOV u peress li ma kienx hemm risposta ħalliet messaġġ irrekordjat biex iċemplulha lura.

[2] L-Uffiċċju tal-Arbitru wkoll ħareġ twissijiet – ara: https://www.youtube.com/watch?v=3podDv2R_Jc&t=3s
[3] P. 10

- Irrispondiet l-SMS fuq l-istess kanal fejn infurmat *NOT AUTHORISED* iżda dan il-messaġġ ma wasalx fid-destinazzjoni li xtaqet.

- Allura f'paniku għafset il-*link* fl-SMS https://bovportals.com/ u daħħlet il-kodiċi sigrieti ġo *website* li dehret bħal ta' BOV u b'hekk tat aċċess għall-kont tagħha lill-frodist(a).

- Il-*website* falza infurmatha li kienu se jċemplulha fuq in-numru 99180001 li kien numru fejn kienet tirċievi SMS mill-Bank.

- Fil-ħin ta' 14:35 irċeviet it-telefonata fejn il-frodista infurmatha li kien laħaq sar pagament mhux awtorizzat ta' €5,000 iżda l-Bank kien żammu minħabba li kien hemm suspett ta' frodi. Qaltilha li jekk tirċievi xi SMS mill-Bank dwar dan il-pagament ma tatix kasu għax l-għada kienet ser tara rifużjoni tal-pagament. Qaltilha wkoll li jekk iċemplulha mill-Bank tgħidilhom li l-problema kienet riżolta. Din it-telefonata damet madwar 13-il minuta.[4]

- Wara ndunat li n-numru li fuqu kienet tkellmet mal-frodista kien b'disa' numri fejn kien hemm 0 żejjed u għalhekk issuspettat li seta' kien każ ta' frodi u ċemplet lill-BOV fil-ħin ta' 15:28 (il-pagament kien sar fil-ħin 14:42). BOV pprovdew reġistrazzjoni ta' din it-telefonata lill-Arbitru li turi li l-Bank mal-ewwel imblokka l-*internet banking* u l-*cards* u talab lill-Ilmentatriċi tagħmel rapport malajr l-għassa. Ġiet infurmata li se jsir *recall* malajr għalkemm ġie kkonfermat li l-pagament kien diġà telaq bis-sistema ta' *Instant Payments.*

- Sar rapport l-għassa fil-ħin ta' 16:40.[5] Kopja ngħatat lill-BOV l-għada filgħodu.

- Fit-5 ta' Marzu, BOV infurmawha li skont il-mudell tal-Arbitru ma kienet intitolata għall-ebda rifużjoni.[6]

- Fit-30 ta' Jannar, BOV ġew infurmati li ma kienx hemm flus fil-kont fejn ġew trasferiti l-flus u għalhekk ir-*recall* ingħalaq bla suċċess.

[4] P. 11; 17
[5] P. 46 - 48
[6] P. 19 - 21

L-Ilment

L-Ilmentatriċi qed titlob kumpens ta' €5,000 għax skont hija:

> *"**4. Summary of Complaint***
>
> *This complaint concerns a fraudulent transaction which was induced through a sophisticated impersonation scam that exploited what appeared to be BOV's own official communication channel.*
>
> *I submit that BOV's decision to refuse compensation entirely is contrary to the facts of the case, inconsistent with the consumer protection framework governing payment services in Malta and the European Union, and fails to properly assess:*
>
> - *the **reasonable appearance of authenticity** created by the spoofed communication;*
> - *the **promptness with which I acted** to notify and stop the fraud;*
> - *the **bank's own communication and response vulnerabilities**; and*
> - *the legal standard required to establish **fraud, negligence, or gross negligence** on the part of a payment service user.*
>
> *I respectfully request the Arbiter to determine that BOV bears at least partial, and potentially substantial, responsibility for the loss and to direct appropriate reimbursement and/or compensation."*[7]

….

> *"**6. Legal and Regulatory Framework***
>
> ***6.1 Maltese and EU payment services framework***
>
> *This dispute falls within the legal framework governing **payment services and unauthorised payment transactions** under **Directive (EU) 2015/2366 (PSD2)**, as transposed into Maltese law and reflected in the Central Bank of Malta's payment services framework. The Maltese regulatory framework recognises the PSD2 principles that:*

---

[7] P. 52

- *a payer is entitled to protection against unauthorised payment transactions;*
- *the payment service provider bears the burden of proving that a transaction was authenticated, accurately recorded, and not affected by technical or procedural failure; and*
- *a customer should not bear losses unless the provider can establish fraud or* ***gross negligence*** *on the part of the user.*

The consumer-facing guidance issued in Malta also reflects the same legal position, namely that:

- *banks must generally refund unauthorised transactions without undue delay; and*
- *they cannot refuse reimbursement merely because the correct credentials or authentication tools were used, unless they can prove fraud or gross negligence.*

6.2 Burden of proof and the meaning of "gross negligence"

A central issue in this case is whether my conduct can properly be characterised as ***gross negligence****.*

Under PSD2 principles and the approach reflected by the Office of the Arbiter for Financial Services, ***gross negligence requires more than mere carelessness, mistake, or ordinary error of judgment****. It requires conduct showing a* ***serious and significant departure from the standard of care*** *expected of a payment service user. The Arbiter's own published model on allocation of responsibility expressly highlights that the assessment must take account of* ***all of the circumstances*** *and that gross negligence must mean more than ordinary negligence.*

That principle is especially important in fraud cases involving:

- *spoofed communications,*
- *impersonation of the bank,*

- *customer confusion induced by the bank's apparent communication environment, and*
- *urgent attempts by the customer to notify the provider and stop the transaction.*

The mere fact that a customer interacted with a fraudulent communication or was deceived by a sophisticated impersonation does ***not automatically amount to gross negligence****. The relevant legal question is whether the bank can show conduct so seriously careless as to justify shifting the entire loss to the customer.*

I submit that the facts of this case do ***not*** *reach that threshold.*

6.3 EU case-law and evolving judicial interpretation

The issue of unauthorised transactions, burden of proof, and customer liability is also being increasingly examined at EU level.

In ***Case C-665/23, IL v Veracash SAS****, the Court of Justice of the European Union considered the operation of the refund and notification framework in the context of unauthorised transactions and highlighted the significance of the legal obligations imposed on payment service providers and users under the payment services regime. While that case concerned the timing of notification under the earlier PSD framework, it reinforces the principle that the legal regime is designed to protect users against unauthorised transactions subject only to carefully defined exceptions.*

More recently, a further EU-level development has emphasised the same consumer-protection logic: namely, that the bank's duty to refund unauthorised transactions is primary, and that allegations of customer fault require proper legal proof rather than assumption. That developing jurisprudential direction is fully consistent with the protective purpose of PSD2 and with the allocation of evidential burden onto the payment service provider.

I respectfully submit that the correct legal approach is therefore not whether the customer made ***any mistake at all****, but whether the provider has discharged the heavy burden of proving* ***fraud or gross negligence*** *in* *circumstances where the scam was materially enabled by the appearance of authenticity associated with the bank's own communication ecosystem.*

6.4 Relevance of Maltese adjudicative approach

*The Office of the Arbiter for Financial Services has itself recognised, in its published materials and decisions, that the assessment of fraud-scam disputes requires a **fact-sensitive allocation of responsibility** between bank and customer, rather than an automatic shifting of loss to the consumer.*

Indeed, publicly referenced decisions of the Arbiter show that these disputes are assessed by reference to:

- *the sophistication of the fraud;*
- *the nature of the authentication process;*
- *the information known to the customer;*
- *whether the customer was induced by a convincing impersonation; and*
- *whether the bank can truly establish conduct amounting to gross negligence.*

I therefore submit that the correct approach in my case is not a simplistic conclusion that "the customer clicked a link," but rather a full assessment of whether the surrounding facts demonstrate a failure of care so serious as to justify total denial of redress. They do not.

7. Grounds of Complaint

7.1 The fraudulent message was made to appear as a BOV communication

*The most important feature of this case is that the fraudulent SMS appeared **within BOV's existing SMS thread**.*

This created a powerful and entirely understandable impression that the message formed part of BOV's legitimate communication channel.

A bank customer is entitled to place substantial reliance on the authenticity of communications appearing in an established thread previously used by the bank.

If a fraudster is able to exploit that channel in such a way that a message appears indistinguishable from genuine bank correspondence, then that is not simply a matter of customer carelessness. It is a serious factor relevant to the allocation of responsibility.

7.2 The scam was sophisticated and convincingly impersonated the bank

This was not an obvious or primitive phishing attempt.

The fraud involved:

- *a spoofed SMS appearing in the official BOV thread;*
- *a webpage indicating that the fraud section had been notified;*
- *display of a genuine BOV number;*
- *a near-identical spoofed callback number;*
- *a caller presenting herself as part of the bank's fraud process; and*
- *a plausible explanation as to why the €5,000 transaction appeared on the account.*

The level of deception was such that it would likely mislead a reasonable consumer acting under urgency and stress.

7.3 I acted promptly, responsibly, and consistently to stop the fraud

At every stage, I acted with urgency and in good faith:

- *I called BOV immediately;*
- *I left my number when the lines were busy;*
- *I sent **"NOT AUTHORISED"** in the same thread;*
- *I contacted BOV again within minutes after identifying the suspicious number;*

- *I cooperated fully with BOV's fraud team; and*
- *I filed a police report the same day.*

These are not the actions of someone acting recklessly or indifferently.

On the contrary, they are the actions of a customer trying repeatedly and urgently to stop a suspected fraud.

7.4 The transaction was processed despite prompt notification and intervention attempts

A particularly troubling aspect of this case is that the transaction was still processed even though:

- *I had already attempted to contact the bank;*
- *I had already replied **"NOT AUTHORISED"**;*
- *I had already spoken with the Card Fraud Department;*
- *my cards and account access had been blocked; and*
- *the bank had been informed of the fraud well before the final confirmation of processing at **18:18**.*

This strongly suggests that the issue is not solely attributable to customer conduct.

It raises legitimate concerns regarding:

- *the timeliness of fraud response;*
- *the adequacy of intervention mechanisms;*
- *the operation of fraud monitoring; and*
- *whether sufficient preventive controls existed once the bank had been put on notice.*

7.5 BOV cannot fairly shift the entire loss onto me

Even if it were argued that I made an error in clicking the link or engaging with the fraudulent caller, that would not automatically entitle BOV to shift the entire loss onto me.

*Under the governing legal framework, the issue is not whether the customer was deceived, but whether the customer acted with **fraud or gross negligence**.*

In my respectful submission:

- *I was induced by a highly sophisticated and convincing fraud;*
- *the fraud materially relied on the appearance of BOV's own communication thread and fraud process;*
- *I attempted to stop the fraud immediately; and*
- *I reported the matter without delay.*

*Those facts are fundamentally inconsistent with a finding that I should bear **100% of the loss**."*[8]

Risposta tal-Fornitur tas-Servizz

Fir-risposta[9] tagħhom datata 27 t'April 2026, BOV qalu:

"4. Whereas according to the Bank's records[10] the transaction effected on the 19th January 2026 in the amount of €5,000, was duly authorised at 14:42:16 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), multiple layers of authentication were applied to ensure that the transaction originated from credentials and systems in the Complainant's name. In fact, the transaction had no indication that it was fraudulent at the time of processing;

[8] P. 55 - 59

[9] P. 84 - 93 u dokumenti annessi p. 94 - 162

[10] Doc. A p. 95

5. *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"

6. *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[11]"*

7. *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;*

8. *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;*

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*

[11] Article 4(30) of PSD2.

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

10. *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.[12]*"*

"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."[13]

"[…] 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."[14]

"We will not be responsible nor liable for losses or costs which you may suffer […] if we fail to comply 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

[12]Doc. B, Page 24. p. 119
[13]Doc. B, Page 25. P. 120
[14]Doc. B, Page 18. p. 113

regulations […] unless any such losses, costs, damages, actions or expenses arise due to the gross negligence of the Bank."[15]

11. *Whereas the Bank further submits that the disputed transaction fell within the daily and per-transaction limits*[16]*, 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 payment in question, being €5,000, was therefore within such parameters;*

12. *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 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 that:*

    "The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting

[15] Doc. B, Pages 23 to 24; p. 118 - 119.
[16] Doc. C (https://www.bov.com/bov-digital-banking-limits)

fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence"

14. *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;*

15. *Whereas it is significant to state that prior to the incident, the Complainant's registered number received eleven anti-fraud SMS warnings from the Bank between November 2023 and January 2026 consistently instructing her not to click links and not to disclose passwords, PINs, verification codes or online-banking credentials via SMS/email/phone:*

    (i) *10th November 2023 – "SPOT THE SCAM. Please be vigilant. BOV never sends links by SMS. DO NOT click on any links and do not provide peersonal information, passwords or card details."*

    (ii) *6th 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) *26th 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) *16th April 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links."*

(viii) *16th July 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide your Card, Account details, PIN, Codes, or Passwords via phone or sms/email links."*

(ix) *29th August 2025 – "BOV will never send you SMS messages asking you to press on links. Do not click on them as you risk being defrauded! In case of doubt call BOV on 21312020."*

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

(xi) *22nd October 2025 – "SPOT THE SCAM. BOV will NEVER ask you to transfer money or provide any details via message links or inform you to click on any links via a mobile message."*

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 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'**.*

17. *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.

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

19. *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;*

20. *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;

III. Timeline of Events

(i) 19th January 2026 –

a) At 14:42:16 the transaction in dispute of €5,000 was processed from the Complainant's account;

b) At 15:28 the Complainant called the Bank's Card Fraud Department, and she speaks to a Bank representative who immediately suspended the Complainant's user ID, blocked her cards and internet banking access, and instructed her to file a police report and take it to the branch. The Bank representative then informed the Bank's Payment Investigations Unit ("PIU") requesting that a recall of funds be initiated;

c) At 15:43, the Bank's PIU sent a recall of funds request[17] *via email and SWIFT message to the beneficiary bank, flagging the payment as "VERY URGENT FRAUDULENT PAYMENT" and requesting immediate cancellation and return of funds;*

d) At 15:47, a camt recall message was sent through SEPA channels to the beneficiary bank;

(ii) ***19th – 30th January 2026*** *– The Bank sent three email reminders and three SWIFT reminders to the beneficiary bank, actively following up on the recall request culminating in the beneficiary bank's reply stating "no funds remain" in the recipient's account, and thus, the recall was declined. The case was subsequently closed and the Complainant was advised accordingly;*

21. Whereas in view of the above, the Bank submits that it acted without delay, initiating the recall process immediately, and

[17] Doc. E, p. 160

> *followed up persistently with multiple reminders and escalations until the final response was received from the beneficiary bank;"*[18]

Seduti

Fl-ewwel seduta tas-26 ta' Mejju 2026, l-Ilmentatriċi spjegat il-każ tagħha kif diġà riprodott hawn fuq. Iżda ċaħdet li wara li għafset il-*link,* permezz tagħha tat xi informazzjoni ta' kodiċi sigrieti lill-frodista.

> ***"Ngħid li meta dħalt fil-link, jiena ma tajt l-ebda informazzjoni. Ma daħħalt l-ebda Username; ma daħħalt l-ebda PIN u ma daħħalt l-ebda IBAN, xejn.***
>
> ***Jien kemm għafast il-link u daqshekk.***
>
> ***Ngħid li b'dik il-link, irnexxielha din il-persuna tieħu over il-kontijiet tal-bank tiegħi. U kienet tinstema' ġenwina u kienet tinstema' taf x'inhi tagħmel.***
>
> ***Ngħid li jien ma tajtha l-ebda informazzjoni, lanqas fuq it-telefon, għax dak il-ħin jien bil-panic lanqas kont naf il-User ID u xejn minn tiegħi, jiġifieri jiena żgur m'għaddejtilhiex din l-informazzjoni.***
>
> ***Ngħid li irnexxielha taċċessa l-kont tiegħi u għamlet transaction ta' €5,000. Qaltli li din it-transaction avolja kienet ser tidher li naqset mill-kont tiegħi, l-għada ser tiġi refunded, li ser terġa' tidħol fil-kont tiegħi.***
>
> ***Imbagħad, it-telefonata waqfet hemm. Għidtilha li kont qed nistenna t-telefonata mill-bank u qaltli li at that point, it was resolved, u ma kienx hemm bżonn aktar komunikazzjoni mal-bank, u qaltli li min-naħa tagħhom, kont ser nirċievi r-refund sa l-għada.***
>
> ***Lili aċċertatni b'mod vera kunfidenti li jiena lanqas assumejt li ma kinitx mill-bank."***[19]
>
> ***….***

[18] P. 86 - 93

[19] P. 164 - 165

"Qed niġi referuta mill-Arbitru għar-rapport tal-Pulizija fejn hemm miktub,

'She confrmed my address and my User ID.'

Ngħid li l-User ID qalituli hi. Hi tatni l-informazzjoni flok tajthielha jiena. Ngħid li l-User ID huwa numru. Ngħid il-verità, lanqas nużah dak in-number għax jiena għandi l-Face Recognition u nidħol bil-Face Recognition fi-BOV Mobile, jiġifieri jiena personalment ma nafux offhand dak in-numru, jiġifieri żgur ma tajtulhiex jiena verbalment.

Ngħid li jiena qed nassumi li x'ħin għafast il-link, tajt l-aċċess. Ngħid li jien ma għafasthiex b'intenzjoni ħażina; jien ma ridtx li ssir dik it-tranżazzjoni.

Ngħid li jiena ma nistax nifhem għalfejn il-bank qalli li t-tort kollu tiegħi minħabba gross negligence."[20]

Fil-kontroeżami qalet:

"Nikkonferma li fid-19 ta' Jannar 2026 irċevejt SMS li kien fih link.

Qed jingħad li wara li rċevejt dak il-link, jien stqarrejt li ppruvajt inċempel il-bank immedjatament.

Mistoqsija għalfejn ċempilt il-bank, jekk hux għax ġieni xi suspett fuq il-link tal-messaġġ, ngħid li jien ippruvajt inċempel biex nieħu azzjoni kemm jista' jkun immedjata biex jekk daħal xi numru, xi involviment ta' persuna oħra, dak jitwaqqaf minnufih u ma ssir l-ebda transaction.

Ngħid li jien ma ċempiltx għax kien hemm il-link. Jien ċempilt għax kien hemm dak in-numru li kien qed jindika li ser jieħu aċċess għall-kont tiegħi. Għalija kien allarmanti u ridt nieħu azzjoni. Ovvjament, dħalt fil-link wara li ċempilt il-BOV u ma qbadtx. At that point, bgħatt dak il-messaġġ 'NOT AUTHORISED' u ma wasalx apparentement. U wara dħalt fil-link.

Mistoqsija niftakarx liema numru tal-bank kont qed nipprova nċempel minn meta rċevejt il-link u t-telefonata, ngħid li għandi miktub f'wieħed

[20]P. 165

mill-appendices għax bl-amment ma nafx ngħid. Għandi l-call log tat-telefonati kollha li għamilt.

Qed niġi referuta għal dak li għidt li meta dħalt fil-link, telgħet window li qaltli li kont ser nirċievi telefonata minn BOV number; u li din il-window ma talbitni xejn aktar.

Mistoqsija nikkonferma li din il-window qalitx hekk biss, ngħid li milli niftakar ma talbitni xejn aktar, però, kieku talbitni l-User ID, jien ma kontx kapaċi nagħtihulha għax lanqas nafu.

Mistoqsija xi wriet il-window, ngħid li l-window uriet in-numru minn fejn kellha tiġi t-telefonata li huwa dak in-numru bit-tliet zeros u one at the end u jien, eventwalment, irċevejt it-telefonata bl-4 zeros. U ndunajt wara li qtajt mill-call. Dak li nista' niftakar.

Qed jingħad li niftakar kollox imma dan id-dettall importanti ma niftakrux.

Ngħid li le, ma niftakrux. Ngħid li kont under a state of shock and panic u ma niftakarx jekk talbitni xi ħaġa oħra u tajthielha, però, hands on heart, jiena ma naf li tajtha l-ebda numru ieħor.

Nikkonferma li mbagħad irċevejt telefonata.

Qed jingħad li biex nidħol fl-Internet Banking u biex nagħmel tranżazzjoni hemm bżonn li nagħti l-kredenzjali tiegħi u hemm bżonn li jittieħdu ċerti passi.

Mistoqsija naqbilx fuq dan, ngħid iva, u l-persuna li kienet fuq il-linja miegħi li jiena ħsibt li hija mill-BOV, iggwidatni.

Mistoqsija kif iggwidatni, x'kienu l-passi li qaltli biex nagħmel, fejn hi kienet taf il-User ID, ngħid li jiena mbagħad dħalt fil-BOV Mobile mill-app tiegħi bil-Face Recognition. Ngħid li ma daħħalt l-ebda User IDs, eċċ. U kien at that point li saret it-transaction.

Ngħid li hi ggwidatni fuq it-telefonata fuq il-passi li għandi nagħmel. Id-dettalji ta' dawk il-passi, ma niftakarhomx ċari x'kienu għax kont under pressure dak il-ħin fejn kont fil-ħin tax-xogħol u qed iċċempilli din tagħmilli pressure.

Qed jingħad li din it-tranżazzjoni ma setgħetx issir bil-User ID tiegħi biss u jrid jiġi stabbilit x'wassal biex isiru dawn it-tranżazzjonijiet.

Ngħid li hemmhekk jiena komplejt nikkonferma li din kienet ġenwina, li din hija mill-bank la kienet taf il-User ID.

Mistoqsija neskludix li waqt li kont qed nitkellem ma' din l-iscammer (li ħsibtha rappreżentanta tal-bank), jiena tajtix ukoll xi kodiċi oħra illi mingħajrhom il-bank qed jgħid li żgur ma kienx isir il-pagament, ngħid li jien ma niftakarx eżatt din x'talbitni u x'tajtha. Ma neskludix għax it-tranżazzjoni saret u għax taħt dak il-mument ta' paniku, jien ridt li nwaqqaf din it-tranżazzjoni.

Mistoqsija kontx irċevejt xi messaġġi fuq il-BOV Mobile li forsi ma nkludejtx fl-ilment tiegħi, jekk irċevejtx xi messaġġ dakinhar bl-activation code, ngħid li dakinhar tad-19 ta' Jannar 2026, jien ma rċevejtx messaġġ b'activation code.

Qed niġi referuta għall-paġni 89 u 90 tal-proċess, fir-risposta tal-bank, fejn hemm lista ta' SMSes mibgħuta lili mill-bank direttament li jwissu lill-klijenti biex ma jagħfsux fuq links u biex ma jaqsmux dettalji bankarji permezz tat-telefon. Li dawn il-11-il messaġġ intbagħtu lili f'perjodu bejn Novembru 2023 u t-22 t'Ottubru 2025 biex javżawni biex ma nagħfasx links anke jekk dawn ikunu jidhru li ġejjin mill-Bank of Valletta.

Mistoqsija naqbilx li rċevejt dawn l-SMSes, ngħid li ma niftakarx imma mhux se ngħid li ma rċevejthomx. Sfortunatament, il-mobile ma jeħodnix daqshekk lura, allura, ma nistax nikkonferma jekk waslulix jew le għax qed jagħtini minn 31 October 2025 'il quddiem. Ngħid li l-mobile hu tas-sena li għaddiet, 2025.

Ngħid li mhux ser ngħid li ma rċevejthomx għax inkun qed nigdeb jekk ngħidlek li ma rċevejthomx u nkun irċevejthom. Ngħid li ma nafx irċevejthomx, imma xorta nemmen li jekk intbagħtu sa mid-October

2025, xorta nikkonferma li wara mid-October ma daħlu xejn aktar bħala alerts b'dawn il-messaġġi.

Nerġa' ngħid li kieku dan il-messaġġ ma daħalx fl-SMS thread tal-BOV, awtomatikament kont ser ninjorah.

Qed jingħad li fl-ilment tiegħi elenkajt messaġġi minn Novembru u Diċembru 2025.

Mistoqsija allura kif qed ngħid li ma nistax nara messaġġ li rċevejt qabel, ngħid li ċ-chat ma tħallinix immur aktar lura. Ngħid li bħalissa t-thread l-aktar li tmur lura hija Friday, 31 October 2025. Jekk xahar ieħor immur niċċekkja tmurli sa November għax ma jżommlix it-thread tal-messaġġi l-aktar antiki.

Dak li qed nipprova ngħid hu li jista' jkun irċevejthom imma just m'għadnix qed narahom.

Mistoqsija nafx fuq id-diversi kampanji li qed isiru fuq dawn it-tipi ta' scams, ngħid li le, ma nafx. Jekk isiru fuq social media, ma tantx insegwi."[21]

Fit-tieni seduta li nżammet fit-2 ta' Lulju 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 mitluba, li hija biss kellha, biex seta' jsir pagament *Instant Payment* permezz ta' *Signature 2* fil-*Mobile App.* Il-pagament sar bl-istess *token* li dejjem saru pagamenti simili permezz tal-*mobile app.* Ma kien hemm l-ebda bdil tal-App minn device għal ieħor permezz ta' xi *Activation Code* kif rajna f'każi oħra ta' lmenti dwar frodi.

Fil-kontroeżami x-xhud qal:

"Naqbel li tajt run through ta' kif suppost taħdem is-sistema.

[21] P. 165 - 168

Mistoqsi ġaladarba jkun hemm dan is-Signature 2 fejn aħna nibagħtu permezz ta' numru ta' telefon, ngħid li le, is-Signature 2 tiġi ġġenerata mill-Mobile App tal-klijent.

Mistoqsi dwar il-komunikazzjoni fejn nibagħtu numru, ngħid li dak hu każ separat ta' Activation Code. F'dan il-każ, ma kienx hemm Activation Code.

Mistoqsi meta l-Bank jibgħat alert permezz ta' SMS, x'numru juża, ngħid li hemm numru wieħed li huwa 9918 0001. Ngħid li b'dan in-numru nikkomunikaw mal-klijenti tagħna imma mhux biex jagħfsu links. Dan il-messaġġ kien riċevut fuq il-kanal ta' SMSes li l-bank ġieli juża biex jikkomunika mal-klijenti tiegħu.

Mistoqsi jekk il-Bank kellux każijiet simili bħal dan il-każ, ngħid li iva.

Mistoqsi hijiex xi ħaġa li qed issir frekwenti, ngħid li jekk wieħed jidħol fuq is-sit tal-Arbitru jkun jaf eżatt.

Qed jingħad li dawn qed ikunu frekwenti ħafna.

Mistoqsi jekk naqblux li s-sistema tal-bank qed tiġi hacked, ngħid li le.

Dr Theuma tintervjeni biex tgħid li dawn il-mistoqsijiet mhumiex relevanti għax-xhieda tas-Sur Gatt li hija dwar il-passi tekniċi tal-pagamenti.

L-Arbitru jgħid li jekk wieħed jaqra d-deċizjonijiet tiegħu, hemm spjega tal-ispoofing li jsir (u anke kien ħareġ Technical Note fuqu) mill-frodisti biex jispoofjaw in-numru tal-bank.”[22]

Xehed ukoll Luke Cutajar li kien inkarigat mir-recall tal-pagamenti u qal li r-recall sar fil-pront iżda ma rnexxiex għax il-flus jidher li nġibdu mill-frodisti qabel ma wasal ir-recall.

Xehed ukoll Ryan Caruana*, MLRO u Group Chief Anti-Financial Crime Officer* tal-BOV, li spjega l-monitoring payments system li jopera l-Bank biex jipprevjeni l-frodi.

[22] P. 195 - 196

"M'hemm xejn ħażin li persuna tibgħat ammont daqshekk baxx minn account li jopera normali - fejn dak l-ammont kien fil-profil tal-Ilmentatriċi - lil persuna li hija low risk, lejn ġurisdizzjoni li hija Maltija, bl-ammont ta' €5,000, ġo ġurisdizzjoni li hija lliċenzjata f'Malta stess, lejn kumpanija komuni, well-known man-nies li tagħmel dawn it-tip ta' investimenti. Ngħid li bħala bank ma kelli qatt inkun naf il-klijent ta' Moneybase min hu.

Jiġifieri jekk kien hemm nuqqas li xi ħadd irċieva flus li mhumiex tiegħu, flus li missu qatt ma rċevihom, hija l-Moneybase, kumpanija oħra, u mhux il-bank għaliex il-flus tal-Ilmentatriċi huma flus li ġew minn sorsi tajbin, flus li l-Ilmentatriċi qaltilna li ser iġġib, il-profil tagħha ġie updated reċentement. Taqla' ammont li hu raġonevoli għax-xogħol li tagħmel.

Jekk dawk il-flus waqqafthomlha kont immur kontra Point B ta' paġna 19, tal-obbligu li għandu l-Bank. U aktar minn dan, ir-risk base hija tant expected li nagħmel hekk, illi sejjer pagament, kumpanija Maltija, ġurisdizzjoni Maltija, Moneybase li hija very well-known għall-investimenti, fejn ukoll il-klijenta anke għamlet tranżazzjonijiet barra 'l pajjiż.

F'Settembru 2024, il-klijenta għamlet pagamenti barra 'l pajjiż. Qed ngħid hekk, jiġifieri m'hemm xejn xi ngħid jekk din għamlet tranżazzjonijiet barra 'l pajjiż. Il-flus huma tagħha u tużahom bl-aħjar mod kif għandha tużahom, però, hemmhekk meta l-persuna għamlet diversi tranżazzjonijiet Malta, allura, wieħed jistaqsi, għax għamlet l-ewwel darba ma' Moneybase, għandna nwaqqfu t-tranżazzjoni? Kieku nagħmlu hekk noħolqu chaos ġol-pajjiż, kieku kellna nwaqqfu tranżazzjonijiet li qatt ma saru qabel ġo istituzzjonijiet Maltin fejn wieħed jinvesti b'ammonti li huma verament żgħar.

Ngħid li l-Bank mexa mal-obbligazzjonijiet tiegħu. Ma nifhem qatt għalfejn it-tranżazzjoni kellha tieqaf meta kienet tranżazzjoni minn Malta għal Malta, lejn kumpanija well known, illiċenzjata Malta b'IBAN Malti. Ngħid li aħna mxejna mal-obbligi tagħna eżatt, anzi aktar, għax

> ***il-BOV huwa l-leader peress li jagħmel Pre-Transaction Monitoring fejn għaldaqstant aħna mxejna ma' dawk l-obbligi li kellna."***[23]

Fuq talba tal-Arbitru BOV bagħtu kopja ta' statement għal perjodu ta' sena qabel il-każ tal-ilment li kien juri pagamenti online fis-6 ta' Jannar 2025, fit-18 ta' Frar 2025, u fis-26 ta' Ġunju 2025.[24]

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.

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.

---

[23]P. 198 - 199

[24]P. 170; 172; 181

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*[25] 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[26] 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

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

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.[27] [28]

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.

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

[27](EU) 2018/389 tas-27 ta' Novembru 2017 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[28]PSD 2 UE 2015/2366 Artikolu 68(2).

	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-pagament ilmentat sar billi b'xi mod il-frodist(a) saret taf il-*USER ID*, il-*One-Time Password* u saħansitra l-kodiċi biex ġie approvat il-pagament ilmentat.

Filwaqt li waqt is-seduta l-Ilmentatriċi ċaħdet li tat din l-informazzjoni, waqt il-kontroeżami ammettiet li:

> ***"Jien ma niftakarx eżatt din x'talbitni u x'tajtha. Ma neskludix għax it-tranżazzjoni saret u għax taħt dak il-mument ta' paniku, jien ridt li nwaqqaf din it-tranżazzjoni."***[29]

Anke fit-telefonata li saret immedjatament wara li biha rrapportat il-każ lill-BOV, l-Ilmentatriċi ġiet mistoqsija jekk tatx xi dettalji lill-frodist(a) u rrispondiet 'iva'[30].

Qalet ukoll:

> ***"erġajt dħalt mill-bovportal u rnexxieli nidħol bl-authenticator u bil-generator mill-BOV mobile".***[31]

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 jiġi approvat il-pagament ilmentat.

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' 30%[32], jiġifieri 10% aktar mill-20% normalment spjegati fil-mudell.

[29] P. 167

[30] Mir-*recording* tat-telefonata

[31] *Ibid*.

[32] F'każijiet oħra fejn il-frodi saret permezz ta' *activation code* li bidel it-*token*, l-Arbitru żied id-doża ta' responsabbiltà fuq il-Bank b'20%, iżda f'dan il-każ ma kienx hemm bdil fit-*token*.

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 ma jsib ebda nuqqas min-naħa tal-BOV dwar *transaction monitoring* peress li din kienet tranzazzjoni unika fil-limitu ta' pagamenti akkordat ta' €5,000.

Għalhekk il-mudell qed jiġi rivedut hekk:

	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	(30%)	30%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(0%)	0%
TOTAL FINALI	**(30%)**	**(70%)**

B'kollox, għalhekk, l-Ilmentatriċi hija intitolata għal kumpens ta' 30% tat-telf li sofriet mill-pagament frawdolenti li ġie ddebitat fil-kont tagħha mal-Bank.[33]

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 u ħames mitt ewro (€1,500).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.40% fis-sena[34] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[35]

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 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 30% għall-BOV u 70% għall-Ilmentatriċi.

____

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[33] 30% ta' €5,000

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

[35] 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.