Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 275/2025

ZI

('l-Ilmentatur')

vs

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

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

Seduta tas-17 t'April 2026

L-Arbitru,

Ra l-Ilment[1] datat 10 ta' Novembru 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €2,313 rigward pagament (inkluż spejjeż) li sar mill-kont li Ilmentatur għandu mal-BOV favur terzi li wara rriżulta li kien frawdolenti.

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

- Il-pagament ikun għal ammont ġeneralment taħt il-€5,000 biex ma jinżammx minħabba li jeċċedi d-*'daily limit'* ta' pagamenti li jkun maqbul bejn il-Bank u klijent tat-tip *'retail'.*
- Il-frodist jirnexxielu jippenetra b'mod frawdolenti il-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew *e-mail.*

[1]Paġni (P.) 1 - 6 b'dokumentazzjoni addizzjonali minn P. 7 - 18.

- 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:

- Fil-25 ta' Mejju 2025, l-Ilmentatur irċieva SMS[3] jistiednu jagħfas *link* biex jaġġorna *3D Secure App* tal -BOV. Dan kien fuq numru li fuqu ġieli rċieva messaġġi mill-BOV, għalkemm mhux b'*link* fihom.

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

[3] P. 100

- Wara li għafas il-link bilfors ta xi informazzjoni biex seta' jiskatta proċess biex l-APP tiġi rreġistrata fuq *device* ieħor. Fil-fatt, irċieva kodiċi 7196 li filwaqt li wissih biex ma jgħidu lil ħadd u ma jdaħħlu fl-ebda *website*, iżda jużah biss fl-APP, jidher li dan il-kodiċi intuża mill-frodist biex l-APP ġiet reġistrata fuq *device* ieħor.[4]

- Jumejn wara jirċievi SMS ġenwin mill-BOV jinfurmah li sar pagament ta' US$2576.32 (ekwivalenti għal €2,315).[5] BOV irrapportaw li dan sar fil-ħin ta' 15:12:30.

- Il-frodi ġiet irrapportata lill-BOV kif l-Ilmentatur induna biha u l-Bank immedjatament waqqaf l-*internet banking* u bblokkja l-*mobile app*. BOV talab lill-Ilmentatur biex jagħmel rapport l-għassa.

- Sar rapport lill-pulizija fil-jum tal-għada, 28 ta' Mejju 2025 fil-ħin ta' 09:50.[6]

- Mir-risposta tal-BOV jirriżulta li l-*card* konċernata li tispiċċa b'numru …. 5852 kienet *unenrolled* minn fuq il-*mobile* reġistrat u *enrolled* fuq *device* ieħor nhar il-25 ta' Mejju 2025 fil-ħin ta' 21:12:57.[7] Il-frodi seħħ jumejn wara u l-*card* u l-*app* ġew ibblokkjati u baqgħu ibblokkjati sa ma ġew *enrolled* fuq id-*device* oriġinali fil-5 ta' Lulju 2025. Il-Bank spjega li l-APP tista' tkun *enrolled* fuq *device* wieħed biss.

- Ma jidhirx li sar proċess ta' *chargeback*. Anke kieku sar, mhux probabbli li ma kienx jirnexxi peress li l-pagament ġie awtorizzat bi *3D Secure.*

- BOV offrew kumpens ta' 30% tal-ammont u qalu li dan kien skont il-mudell li fassal l-Arbitru.

  L-Ilmentatur ma aċċettax u qed jitlob kumpens sħiħ għax iħoss li hu ma awtorizzax il-pagament.

[4] P. 99
[5] P. 32
[6] P. 17
[7] P. 25

Risposta tal-Fornitur tas-Servizz

Fir-risposta[8] tagħhom, il-BOV qalu:

‘‘*Respectfully submits:*

Whereas the Complainant asserts that he never attempted such payments and immediately reported the matter to the Bank, which cancelled his cards and directed him to file a police report;

Whereas the Bank offered the Complainant an ex-gratia compensation of €694.00 (30% of the loss), citing precedents established by the Office of the Arbiter for Financial Services (OAFS). The Complainant considers this offer dismissive and inadequate, insisting on full reimbursement of €2,285.38 (converted at BOV's exchange rate of 1.1273 on 30th October 2025);

Whereas the Bank shall preface by noting the Complainant's inconsistent statements. While in his initial correspondence with the Bank , he claims that a prompt which appeared legitimate appeared and which purportedly emanated from within the Bank's own application environment, therefore, suggesting an in-app pop-up, he is now stating, in his complaint, that he was asked to change his 3D Secure password via SMS believed to be from the Bank. In this regard, the Bank respectfully submits that these are two very distinct mechanisms. The Bank denies that its mobile application generates pop-ups of the nature described. No screenshots or technical evidence were submitted to substantiate the claim that the prompt originated from the Bank's application.

The Bank asserts that a spoofed environment is not a vulnerability in the Bank's applications. On the other hand, SMS phishing is external and widely recognised as a scam vector. In view of the Complainant's inconsistency, concerns are raised vis-à-vis his credibility. He insists on never having clicked on any suspicious links, yet the fraud occurred after he acted on an unverified prompt, and furthermore, such doubts are heightened considering the lack of evidence to corroborate his alternating statements;

Whereas according to the Bank's records, the transaction in question was duly authorised on the 27th May As part of the Bank's security framework, which

[8] P. 23 - 33 u dokumenti annessi p. 34 - 92

complies with the Payment Services Directive 2 (PSD2), the transaction was authenticated through the 3D Secure protocol using push notifications on the device where the card was enrolled. The successful debit of USD 2,576.31 and the two subsequent attempted transactions were processed following Strong Customer Authentication ("SCA"), and there were no indicators within the Bank's systems suggesting that these transactions were fraudulent at the time of authorisation;

Whereas the payment was approved on the 27th May 2025. Such payments are processed immediately, as clearly stipulated in the Bank's general terms and conditions under Section 2.3 – Cancel Payment Instructions/Orders, which states:

> *"We cannot cancel payments that are processed in real-time. You can cancel any payment which you asked us to make on a future date as long as you advise us by 1300 hours (CET) of the Banking Business Day before payment is due to be made."*

Furthermore, Clauses 2(g) and 2(h) of the BOV Skypass Card Terms and Conditions confirm that providing card details, PIN, or 3D Secure passcode signifies consent to execute the transaction, and that transactions cannot be revoked once authorised:

> *"g. Your signature on the sales voucher or other order or authorisation form (such as Direct Debit Mandate or subscription) showing your Card number, the quoting of your Card number and/or other details over the telephone or internet or the inputting of your PIN, or the transmission of your Card/Security Details e.g. by tapping your card at a point of sale, signifies your consent to execute a transaction.*
>
> *h. A transaction cannot be revoked by yourself once you have given your consent as mentioned above. In the case of Card recurring transactions or Card transactions which are initiated by, or through the person for whom payment is intended (the payee), you may not revoke the transaction after transmitting the payment order or giving the payee your consent to execute the transaction."*

This means that once a payment is authorised for immediate execution, it cannot be changed or cancelled because processing begins as soon as the instruction is received. This provision is fully aligned with Article 80 of PSD2, entitled "Irrevocability of a payment order", which establishes that a payment order becomes irrevocable once received by the payment service providers. Therefore, the Bank acted in compliance with both its contractual and regulatory obligations when processing the transaction;

Whereas internal, audited logs confirm that all three attempts were 3D Secure authenticated via push notifications on the 25th May 2025, thereby satisfying the technical requirements for SCA under PSD2. The Bank's logs establish the following 3DS enrolment history:

i. 30th September 2021 – Card ending 5852 was initially enrolled on device OnePlus IN2013;

ii. 25th May 2025 at 21:12:57 – Card ending 5852 was re-enrolled on a Google Android emulator (sdk_gphone64_x86_64), with this enrolment remaining active until 5th July 2025 at 10:20:12;

iii. 25th May 2025 – 3D Secure authentication for all three disputed transactions occurred via push notifications, satisfying PSD2 requirements for two-factor authentication;

iv. 27th May 2025 at 15:12:30 – Transaction of €2,313.54 was processed and authenticated through the active enrolment on the emulator device;

v. *5th July 2025 at 10:30:46 – Subsequent re-enrolment on device OnePlus IN2013;*

Whereas in order for the card to be enrolled on another device, the Complainant first needed to unenroll it from the previous device he was using it on. Subsequently, in order to enrol his card on another device, he needed to input the following information:

i. The card number,

ii. The card expiration date,

iii. The CVV number, and

iv. A one-time password (verification code) sent by the Bank to the customer's mobile number registered with the Bank.

A passcode then needs to be set up which needs to be used in order to approve each transaction using the BOV 3D Secure app. Otherwise, the biometrics feature may be set up in order to approve future payments;[9]

Whereas once this process is successfully followed, the card is duly registered on the device which should be in the possession of the customer since he should be the only person who has access to the abovementioned information. Therefore, according to the Bank's records, the transactions which are the subject of this claim were duly authorised;

Whereas furthermore, it is pertinent to note that once a cardholder successfully enrols a single card in the BOV 3D Secure application, all other cards linked to that cardholder are automatically enrolled. This eliminates the need for any additional steps or manual intervention. However, for a fraudster to perform a transaction using any of these automatically enrolled cards, they would still require the complete card credentials, namely the PAN, expiry date, and CVV. These details are never displayed within the Bank's application environment. This strongly suggests that if multiple cards were compromised, the cardholder must have provided these details elsewhere, rather than through the Bank's app;

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 deemed authorised only if the payer has given consent to execute the payment transaction. As explained, the Bank received legitimate instructions from credentials associated with the Complainant and therefore is under no obligation to reimburse him;

Whereas the Bank implemented the necessary measures to ensure that its systems are secure and in line with PSD2 which provides the following on 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*

[9] Doc. E

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;"

Whereas the disputed transaction was executed using the Complainant's own confidential authentication credentials, which are personal and non-transferable. The Bank had no control over these transfers because they were initiated without any intervention from the Bank. Once the bank receives legitimate instructions for a third-party payment through its secure channels, it is contractually and legally obliged to process them, as the system presumes that only the authorized account holder has access to such credentials. This principle is expressly set out in the Skypass Card Terms and Conditions;

Whereas besides the fact that the payments were duly authorised, it is also significant to mention that the transaction amount falls within the limit imposed for these kinds of transactions. With respect to the transaction in question in this arbitration, which was affected through a BOV Skypass Visa Credit card to a third-party merchant, the transaction was within the applicable daily limit of €6,000. Therefore, there were no suspicious signs for the Bank with respect to this transaction. One should also note that PSD2 does not oblige the Bank to impose any limit on transactions. It only stipulates that if there is the possibility to put in place spending limits, the customers should be informed of this;

Moreover, under the afore-mentioned Commission Delegated Regulation, supplementing PSD2, the Bank is permitted to apply exemptions from SCA for transactions assessed as low risk. This does not mean that the Bank neglects security, on the contrary, the Bank consistently applies SCA even in cases where an exemption could legally apply. In this case, the disputed transaction was approved through full SCA, meaning, the Complainant's personalised security credentials were used, authentication complied with PSD2 requirement for two independent factors, and the Bank fulfilled its regulatory obligation to ensure secure execution of payment instruction. This demonstrates that the Bank's systems operated correctly and securely, and that the fraud did not result from any failure to implement SCA. Rather, the compromise occurred because the credentials were obtained and used by an unauthorised third party, which falls outside the Bank's control;

Whereas without prejudice to the above, if the Complainant alleges that the transactions were not authorised by him, the Bank is still not obliged to reimburse the amount. This is because, even if the Complainant did not intent to approve the payments, he nevertheless performed the necessary actions that enabled their approval through the Bank's secure channels. This position is support by Article 45 of Directive No. 1 of the Central Bank of Malta, entitled 'Obligations of the payment service user in relation to payment instruments and personalised security credentials' which provides the following:

> *"45. (1) The payment service user entitled to use a payment instrument shall:*
>
> *a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;*
>
> *(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe."*

Whereas article 50(1) of the Directive provides:

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

The fact that the Complainant provided the necessary details which enabled the approval of the payment goes against the BOV Skypass Card Terms and Conditions. Clause 3 expressly requires the Cardholder to keep the PIN, 3D Secure passcode, and any verification codes secret and not disclose them to anyone, including Bank personnel:

> *"In all the above instances, any PIN and/or Card/Security Details communicated to you to be used in conjunction with your Card must be kept secret. This means that you must not disclose such Card/Security Details to anyone else, including Bank personnel, or record them in any way which allows another person to discover them."*

Clause 4 further stipulates that the Cardholder must take all reasonable precautions to prevent the loss, theft, or fraudulent use of the Card and its security details. Under Clause 4(b), the Cardholder is unlimitedly responsible for all transactions carried out prior to notifying the Bank if he fails to comply with these obligations or acts with gross negligence:

> *"a. The Cardholder must take all the reasonable precautions to prevent the loss, theft or fraudulent use of the Card and the PIN being disclosed to any person […]*
>
> *b. You will however be unlimitedly responsible for any, and all, transactions carried out with your Card or your PIN, or Card/Security Details prior to notification in terms of this clause, if you or the Supplementary Cardholder have: i. not used your Card in accordance with these Terms and Conditions, in particular, if you do not take all reasonable steps to keep safe your Card and the PIN, and/or the Card/Security Details; […] acted in any other way with gross negligence or fraudulently."*

Moreover, Clause 2(g) confirms that quoting card details or entering a PIN or 3D Secure passcode signifies consent to execute a transaction, and Clause 2(h) establishes that such transactions cannot be revoked once authorised.

Furthermore, Section 2.23 (Security Notice) reinforces that the customer must take all reasonable precautions to prevent dissemination, loss, theft, or fraudulent use of credentials and is unlimitedly responsible for all transactions carried out prior to notifying the Bank of compromise. This means that once the Complainant entered his credentials and authorised the transaction, the Bank was legally and contractually obliged to execute it, and liability for safeguarding those credentials rests with the Complainant;

Whereas, as a voluntary user of the BOV 3D Secure, the Complainant knows or ought to have known that transaction authentication can only be carried out through the Bank's official BOV 3D Secure app linked to the customer's registered mobile device. The Bank has never requested the Complainant, or any other customer, to approve transactions via links in SMS or through any unofficial channels. Moreover, the Bank does not call customers to request confidential details such as card numbers, CVV, PINs, or authentication codes. On the contrary, the Bank regularly issues warnings and scam alerts advising

customers to exercise caution and avoid disclosing sensitive information, particularly when responding to unsolicited messages or prompts. This reinforces the position that the fraudulent activity originated outside the Bank's systems, that the Complainant disregarded clear security guidance provided by the Bank, and that the Bank fulfilled its duty of care by implementing secure authentication channels and issuing repeated warnings;

Whereas the Bank has consistently taken proactive measures to protect its customers from fraud. In November 2023, it launched an SMS alert scheme to warn customers about ongoing scams. Prior to this incident, the Complainant received multiple SMS warnings including:

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 online banking passwords.*

iii. ***5th April 2024*** *–* ***SPOT THE SCAM.*** *BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests.*

iv. ***22nd July 2024*** *– BOV will NEVER ask you to unblock accounts, ask for Card details, PIN, Verification Codes or Passwords via telephone or sms/email with links.*

v. ***22nd October 2024 – SPOT THE SCAM****. BOV will NEVER ask you for Card details, PIN, Verification codes or Passwords via telephone or sms/email with links. BEWARE of urgent requests.*

Whereas these SMS alerts form part of a broader educational campaign. Since 2023, the Bank has published scam awareness content on its official website and social media channels, including "Spot the Scam: Bank Impersonation Scams" page and "A Spotlight on Smishing" guide. It reinforced these efforts through interactive branch-level quizzes, seasonal alerts, and a public webinar in May 2025 focused on phishing, spoofing, and PSD2 security measures. In addition, the Bank has consistently engaged in public awareness initiatives through TV

appearances, press interviews, and digital campaigns. The Spot the Scam campaign launched in March 2023 was featured on TVM News, followed by interactive quizzes during Cybersecurity Month and video content on official channels. These initiatives demonstrate that the Bank acted reasonably and prudently by educating customers and promoting vigilance against fraudulent schemes.

Whereas in addition to the Bank's own efforts, Maltese authorities have launched extensive educational campaigns to protect consumers of financial services from fraud. The Malta Financial Services Authority (MFSA) publishes resources such as "The MFSA's Guide to Secure Online Banking", which advises:

> *"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."*

National bodies such as MITA's National Cybersecurity Coordination Centre and GEMMA Financial Literacy Programme have complemented these efforts with public campaigns, webinars, and interactive guides on identifying fraud and securing digital banking. These initiatives collectively underscore that consumer vigilance is a shared responsibility and widely promoted across Malta's financial ecosystem;

Whereas despite repeated warnings and educational initiatives, the Complainant carried out all the necessary actions that enabled the disputed payments to be approved. By doing so, he breached the Bank's terms and conditions and acted contrary to Article 45 of the Central Bank of Malta Directive No. 1, which obliges payment service users to follow security guidelines and

contractual terms. The Bank has taken reasonable steps to educate and alert customers, even sending the Complainant SMSs to his personal mobile number, but it cannot physically intervene or compel a customer to stop an action once they voluntarily provide personal and confidential information. The Bank's role is to provide secure systems and clear warnings, not to override a customer's deliberate actions. Furthermore, the Complainant acted against Article 45(2) of the same Directive by failing to take all reasonable steps to keep his personalised security credentials safe. It is reasonably expected that a consumer is aware of and adheres to the terms governing the contractual relationship. In this case, any alleged fraud occurred because the Complainant disclosed confidential details to a fraudster and followed instructions provided by that fraudster. These actions amount to gross negligence, which excludes the Bank from liability under both PSD2 and Maltese law.'[10]

Seduti

Inżammet seduta fis-7 ta' Jannar 2026 fejn l-Ilmentatur ippreżenta l-każ tiegħu li diġà ġie spjegat aktar 'il fuq, fosthom:

'Ngħid li meta għafast dik il-link, jiena ġejt redirected għal dak li ħsibt li huwa t-3D Secure App tal-BOV. U kif intlabt fl-SMS, bdilt il-password.

Ngħid li s-set up, l-iscreen li rajt fuq il-mobile tiegħi, ma ngħidx li kien simili, imma li kien eżatt bħat-3D Secure tal-BOV.

L-Arbitru jirreferi għal paġna 26 tal-proċess (paġna 4 tar-risposta tal-BOV) fejn hemm imniżżla l-isteps li jridu jittieħdu biex isir dan il-pagament fejn il-BOV iddikjara li l-ammont hu ta' 2313.54.

Mistoqsi mill-Arbitru għamiltx dawn l-affarijiet biex seta' jsir dan il-pagament, ngħid li jien it-3D Secure tal-BOV nużah jekk mhux kuljum, nużah frekwenti ħafna, - u kull darba li nagħmel pagament, titla' prompt fit-3D Secure li jgħidulek li trid tawtorizza dan il-pagament tramite t-3D Secure App.

Ngħid li f'dan il-każ, meta sar dan il-pagament, din il-prompt ma telgħetx. Jiena l-unika ħaġa li għamilt meta kklikkkjajt fuq dik il-link, hu li bdilt il-password tat-3D Secure.

[10] P. 23 - 31

Mistoqsi mill-Arbitru jekk meta ngħid li bdilt il-password inkunx qed infisser li bdilt l-activation code, ngħid li le. Ngħid li ġieli t-3D Secure App ġieli staqsietni waqt li nkun fuq l-App tal-BOV biex nibdel il-password tat-3D Secure. U bdilt il-password tat-3D Secure. Dak kollox. It's a password which is embedded in the security of the App, minn dak li nifhem jiena. Però, jiena ma tajt l-ebda awtorizzazzjoni kif inhi l-prassi tas-soltu biex issir dik it-tranżazzjoni.

Ngħid li jiena ma mortx kif is-soltu tmur – dan l-aħħar qed inħallas bil-mobile – tmiss il-mobile mal-payment machine u titlalek l-authorisation biex tawtorizza l-payment through the 3D Secure App.

L-Arbitru jirreferi għall-punt 25 tar-risposta tal-Bank of Valletta fejn jgħid li l-iscammer, bl-għajnuna tiegħi, irnexxielu jirreġistra t-3D Secure App fuq mobile ieħor li huwa tiegħu. U biex għamel dan, jien ridt ngħaddilu xi activation code li jagħtini l-bank.

L-Arbitru jkompli li ġaladarba l-iscammer kellu t-3D Secure App fuq il-mobile tiegħu u, allura, neħħiha minn tiegħi u għamilha fuq tiegħu, dawk in-notifications tal-approval beda jirċevihom hu u mhux jien.

Ngħid eżatt.

Kontroeżami:

Qed jingħad li jiena oriġinarjament stqarrejt li l-prompt ġiet mill-App tal-BOV.

Ngħid li għax hekk ġiegħeluni nifhem; jekk jiena kklikkjajt fuq il-messaġġ, ġie eżatt bħall-App tal-BOV. Ma kellix għalfejn naħseb li ta' fuq l-iscreen ma kienx mill-BOV.

Qed jingħad li imbagħad, kif għidt fl-ilment, irċevejt SMS fejn talabni nagħmel update tat-3D Secure.

Ngħid li jista' jkun li hemm verżjoni u verżjoni, imma ma naħsibx li għandha tagħmel differenza x'verżjoni hi. Jekk jiena qed ngħid li din ġiet mill-App tal-BOV għax jiena I was led to think li dak li qed nagħmel hu through l-App tal-BOV, ma naħsibx li għandha tkun il-bażi ta' għalfejn u kif jiena ġejt scammed.'[11]

...

[11] P. 94 - 95

'Mistoqsi x'passi ħadt wara li għafast il-link biex dan iseħħ, ngħid li wara li għafast il-link, ġie l-iscreen eżatt kif ġieli għamilt qabel tal-BOV App li tgħidlek, jekk m'inix sejjer żball, New Password u Confirm Password, xi ħaġa hekk.

Ngħid li jiena daqshekk għamilt.

Imbagħad, għandek Unenroll, u ttappjajt Unenroll u I unenrolled. Imbagħad, they got reenrolled ovvjament għax imbagħad erġajt għamilt it-3D Secure App mill-bidu, mill-ġdid.

Qed jingħad li meta jsir reenrollment ta' card jeħtieġ ċerta informazzjoni, bħan-numru tal-card, expiry date, CVV number u l-One-Time Password; u l-One-Time Password intbagħat fuq il-mobile tiegħi.

Ngħid li le, ma nistax insib jekk bagħtulix il-One-Time Password bejn il-25 u s-27 ta' Mejju.

Qed jingħad li xi ħadd kellu fil-pussess tiegħu din l-informazzjoni u mistoqsi niftakarx jekk tajtx lil xi ħadd informazzjoni bħal din, ngħid li ma niftakarx u jekk qed tgħidu li l-mobile tiegħi ġie emulated fuq mobile ieħor, jista' jkun li l-One-Time Password ġiet ipprovduta mingħand ħaddieħor.

Ngħid li l-unika One-Time Password li għandi mingħand il-BOV hija tat-28 ta' Mejju meta kienu diġà saru l-pagamenti: 'Your activation code. Please use it within one hour.' U għandi l-activation code. BOV Mobile App.'[12]

Waqt il-kontroeżami, l-Ilmentatur qal li ma jiftakarx jekk kienx jirċievi SMS bi twissija biex ma jagħfasx links li jidhru fuq SMS bħala ġejjin mill-Bank, iżda ma ċaħadx li seta' rċevihom bħalma rċevihom kulħadd.[13] Il-Bank bagħat lista ta' dawn l-SMSes ta' twissija.[14]

Fit-tieni seduta li nżammet fl-24 ta' Frar 2026, xehdet Sandra Stevens li f'isem il-BOV qalet:

'Ngħid li ilni tletin sena fid-dipartiment tal-Cards fil-Bank of Valletta, u illi 19-il sena nimmaniġja s-section tal-Card Fraud.

[12] P. 95 - 96
[13] P. 97
[14] P. 108

Nispjega li t-3D Secure App tista' tiġi downloaded minn kulħadd fuq kwalunkwe device, però, l-cards ġaladarba jittellgħu fl-app jistgħu jiġu enrolled darba biss fuq device wieħed biss.

Dan ifisser li jekk il-card holder diġà jkun niżżel l-app tat-3D Secure u tella' l-cards ġo fiha minn fuq id-device tiegħu, ħadd aktar ma jkun jista' jerġa' jniżżel l-app u jtella' l-cards tal-card holder fid-device tiegħu.

<OMISSIS>

Ngħid li l-bank ma jibgħatx SMSes b'links la waqt registrations, la waqt enrolments u lanqas biex isiru updates, passwords; ma nużawx links. Anzi nirrakkomandaw ħafna lill-klijenti biex ma jużawx links li jirċievu.

Ngħid li f'dan il-każ, mir-records irriżulta li l-card ġiet enrolled fuq it-3D Secure f'Settembru 2021. Imbagħad, f'Mejju 2025 kien hemm l-unenrolment minn fuq id-device li fuqu sar l-enrolment fil-2021. Imbagħad, sar enrolment ġdid fil-25 ta' Mejju 2025. F'Lulju 2025, wara li sar dan il-każ, meta jiġi rrapportat lilna xi ħaġa bħal din, nagħmlu deactivation tal-enrolments kollha li jkun hemm.

Ngħid li meta ġiet enrolled fl-2025, ma kienx hemm l-unenrolment tab fuq id-device tal-card holder, allura l-bank jagħmel deactivation ta' kollox biex il-card holder ikun jista' jerġa' jagħmel l-enrolment tiegħu. Ngħid li dak sar wara f'Lulju.

<OMISSIS>

Ngħid li t-tranżazzjoni tidher li ġiet awtentikata bit-3D Secure.

Rigward jekk ir-re-enrolment u t-tranżazzjonijiet in kwistjoni setgħux isiru mingħajr l-użu ta' kredenzjali validi, ngħid li kien hemm enrolment tajjeb tal-card għax kieku l-authentication process waqt it-tranżazzjoni li qed issir ma kienx jaħdem. Mir-records jirriżulta li l-bank tal-merchant kien qed jitlob authentication bit-3D Secure u aħna ma għamilnihiex bit-3D Secure mentri mhux il-każ. L-entry mode fit-transaction record juri li kienet bit-3D Secure.

L-Arbitru jiġbed l-attenzjoni għall-fatt li kien hemm żewġ attentati oħra wara dan il-każ li fallew.

Mitluba nispjega għalfejn dawn fallew, ngħid li hemm żewġ stadji fi tranżazzjoni li ssir fuq it-3D Secure website:

1. ***l-authentication u, f'dan il-każ, it-tlett attentati ġew awtentikati kollha bit-3D Secure, jiġifieri l-authentication kienet successful, u***

2. ***fejn il-merchant jibgħat authorisation request u din l-authorisation request kemm issir validation tal-card details, jekk ġietx awtentikata diġà, u li hemm fondi biex ikopru dak l-ammont.***

Ngħid li meta ġew biex jgħaddu t-tieni u t-tielet attempt, dawn ġew declined fit-tieni stadju, però, qabel kienu awtentikati bit-3D Secure successfully. Ma nafx bl-amment ir-raġuni għalfejn dawn ġew declined. Jista' jkun li l-card limit ikun intlaħaq.'[15]

L-Arbitru talab lix-xhud tispjega jekk il-kodiċi biex isir *enrolment* li ntbagħat fuq il-*mobile* tal-Ilmentatur setax isir jaf bih il-frodist bla ma l-Ilmentatur ikun ikkomunikah lilu b'xi mod. Qalet li dan hu possibbli biss jekk l-Ilmentatur ikun ta aċċess remot tal-*mobile* tiegħu lil terzi li f'dan il-każ ma jidhirx li sar.

Sostniet li biex isir *enrolment* tal-APP fuq *device* ieħor trid iddaħħal in-numru tal-*card*, l-*expiry date* u *CVV number* u mingħajr din l-informazzjoni ma setax isir *enrolment*.

L-Ilmentatur isostni li huwa ma tax din l-informazzjoni waqt li Sandra Stevens issostni li mingħajr din l-informazzjoni ma setax isir *enrolment* tal-APP fuq *device* ieħor.

Sottomissjonijiet finali

Fis-sottomissjonijiet finali, il-partijiet bażikament sostnew il-pożizzjoni tagħhom kif esibita fl-ilment, fir-risposta u fix-xhieda waqt is-seduti.[16] [17]

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

[15] P. 102 - 105
[16] P. 108 sottomissjonijiet tal-Ilmentatur
[17] P. 110 – 126 sottomissjonijiet ta' BOV

biex il-klijenti joqgħodu attenti) biex il-frodist ma jkunx jista' juża dan il-kanal ta' komunikazzjoni biex jippersonifika l-Bank u jiffroda lill-klijenti.

Analiżi u konsiderazzjoni

L-Arbitru huwa tal-fehma li għall-fini ta' trasparenza u konsistenza, biex jasal għal deċiżjonijiet dwar ilmenti bħal dawn, ippubblika mudell dwar kif jaħseb għandha tinqasam ir-responsabbiltà tal-frodi bejn il-bank konċernat u l-klijent iffrodat u dan billi jieħu konsiderazzjoni ta' fatturi li jistgħu ikunu partikolari għal kull każ.

Għal dan il-għan, l-Arbitru qed jannetti ma' din id-deċiżjoni mudell li ppubblika u li ser jiġi wżat biex jasal għal deċiżjoni dwar kif ser isir '*apportionment'* tal-konsegwenzi tal-frodi. Il-mudell fih ukoll diversi rakkomandazzjonijiet biex il-banek ikomplu jsaħħu l-protezzjoni tal-konsumatur kontra frodisti li kulma jmur dejjem isiru aktar kapaċi u kreattivi.

Iżda l-Arbitru jħoss il-bżonn 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*[18] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara każi fejn l-ilmentaturi faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[19] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

Għalhekk, il-banek jeħtieġ li jkollhom sistema ta' pagamenti robusta biżżejjed biex il-pagament ma jsirx jekk ma jkunx speċifikament awtorizzat mill-klijent/Ilmentatur. Il-banek ma jistgħux ma jerfgħux responsabbilità jekk iħallu toqob fis-sistemi tagħhom li permezz tagħhom il-frodist ikun jista', bla ma jkun hemm aktar involviment tal-klijent/Ilmentatur, jagħmlu awtorizzazzjoni speċifika tal-pagament a favur tal-frodist.

Dan il-fatt huwa wkoll inkluż fil-mudell.

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

Il-mudell għandu wkoll għarfien dwar jekk l-Ilmentatur ikunx midħla tas-sistemi ta' pagamenti *online* mal Bank billi jkun għamel xi pagament simili (ġenwin) fit-12-il xahar ta' qabel. Dan jgħin ukoll biex tiġi ffurmata opinjoni jekk il-*monitoring* tal-pagamenti li l-bank huwa doveruż jagħmel (kif spjegat fil-mudell) huwiex effettiv.[20] [21]

Deċiżjoni

L-Arbitru jiddeċiedi skont kif provdut f'Artiklu 19(3)(b) b'referenza għal dak li, fil-fehma tiegħu, ikun ġust, ekwu u raġonevoli fiċ-ċirkostanzi u merti sostantivi tal-każ. Meta l-Arbitru japplika l-mudell propost għal dan il-każ partikolari jasal għal din id-deċiżjoni:

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

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

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr il-piż kollu tat-telf għaliex:

1. Injora għal kollox twissijiet li l-BOV bagħat biex ma jagħfasx fuq *links* f'SMS anke jekk jidhru ġejjin mill-Bank li l-aħħar wieħed kien datat 15 t'April 2025, jiġifieri anqas minn 3 xhur qabel ma ġara l-każ ilmentat.[22]

2. Il-probabbilità li l-Ilmentatur għadda l-informazzjoni lill-frodist biex isir l-*unenrollment* tal-APP minn fuq il-*mobile* tiegħu għal fuq id-*device* tal-frodist tidher aktar kredibbli minn kwalunkwe ipoteżi oħra. Din iżżid id-doża ta' traskuraġni grossolana mill-Ilmentatur. Din l-aktar evidenti meta l-twissija fuq messaġġ tal-Bank bil-kodiċi, biex ma jgħidu lil ħadd[23] u ma jdaħħlu bl-ebda *website*, spiċċa uzat mill-frodist biex irreġistra t-3DSecure APP fuq *device* kontrollat mill-frodist li seta' japprova l-pagament ilmentat kif ukoll żewġ pagamenti oħra li nżammu.

   L-Arbitru jsib negliġenza grossolana min-naħa tal-Ilmentatur skont il-preamboli 71 u 72 ta' PSD 2 (Directive EU 2016/2366) peress li l-Ilmentatur żvela kodiċi sigrieti speċifikament kontra it-twissijiet li ngħata fil-messaġġ li l-Bank bagħatlu bil-kodiċi.

   Preamboli ta' Direttiva EU 2105/2366 (PSD2)

   (71) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the L 337/46 Official Journal of the European Union 23.12.2015 EN payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user

[22] P. 110
[23] P. 99

should be liable only for a very limited amount, unless the payment service user has acted fraudulently or with gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products.

(72) In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases

3. L-Ilmentatur ammetta li kien midħla sew ta' pagamenti li jsiru bit-*3DSecure.*[24]

[24] P. 94

4. Ma ngabet l-ebda evidenza ta' xi ċirkostanzi speċjali li setgħu jiskużaw lill-Ilmentatur.

Iżda l-Arbitru jieħu nota li fir-risposta tal-Bank lill-Uffiċċju tal-Arbitru ġie kkonfermat li l-Bank kien għamel offerta *ex gratia* ta' 30% tat-telf, ekwivalenti għall-ammont ta' €694.[25]

L-istess offerta kienet saret mill- BOV f'ittra ta' Sandra Stevens datata 29 ta' Lulju 2025 bħala *full and final settlement of your claim.*[26] Din l-offerta ma kinetx indikata 'bla preġudizzju'.

In vista ta' dan, l-Arbitru jidhirlu li l-Ilmentatur m'għandux jiġi mċaħħad minn din l-offerta sempliċiment għax segwa dritt li jressaq dan l-ilment.

Għalhekk, filwaqt li l-Arbitru, biex ikun konsistenti mal-mudell li ppubblika, ma jsibx każ biex jordna xi kumpens skont Artikolu 26(3)(c)(iv) tal-Kap. 555 tal-Liġijiet ta' Malta, l-Arbitru jirrakkomanda bil-qawwa li l-Bank of Valletta jagħmel il-pagament offrut *ex gratia* lill-Ilmentatur.

Dan anke b'rikonoxximent ta' direzzjoni mogħtija mill-Arbitru f'deċiżjonijiet oħra li fejn ikun hemm bdil tan-numru tal-*mobile* reġistrat fuq is-sistemi tal-Bank, kif ukoll tad-*device* li fuqu jkun hemm l-Apps tal-Bank, għandha tiddaħħal il-prassi li l-pagamenti jiġu mwaqqfa temporanjament sa ma jsir kuntatt dirett mal-klijent biex jiġi kkonfermat li hu jkun awtorizza dan il-bdil.

Kull parti ġġorr l-ispejjeż tagħha.

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[25] P. 24
[26] P. 14

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