Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 327/2025

SD

('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 12 ta' Diċembru 2025 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €4,938.57 rigward pagamenti li saru mill-kont li Ilmentatur għandu mal-BOV, favur terzi li wara rriżulta li kien frawdolenti.

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

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

[1]Paġni (P.) 1-11 b'dokumentazzjoni addizzjonali minn P. 12 - 81.

- 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, fil-ħin ta' 12:14, l-Ilmentatur irċieva l-messaġġ frawdolenti fuq il-*mobile* permezz ta' SMS fejn is-soltu jirċievi notifiki mill-BOV, li kien jgħid:

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

> ***"We require additional verification to keep your card and account active. Login and verify at https://bovhelpcenter.com25/06/25".***[3]

- Kif għafas il-*link* daħal f'*website* li dehret identika għal tal-BOV u daħħal in-numri li s-soltu jdaħħal biex jaċċessa l-*internet banking*. B'hekk, bla ma intebaħ, kien qed jagħti aċċess biex il-frodist ikun jaf x'għandu fil-kontijiet tiegħu mal-Bank.

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

- Kellimitu bil-Malti u dehret midħla tal-proċeduri tal-Bank. Bdiet anke tikkwotalu xi informazzjoni fuq il-kontijiet tiegħu. B'hekk dehret li kienet telefonata ġenwina. Qaltlu li kien hemm xi tranżazzjonijiet suspettużi li kienet ser twaqqafhom u talbitu xi *codes* li rrifjuta li jagħtihomlha għax qalilha li la kienu pagamenti suspettużi, il-Bank m'għandux bżonn *codes* biex iwaqqafhom.

- Bl-aċċess li kellha setgħet titlob biex jiġi ġġenerat *activation code* u, fil-fatt, l-Ilmentatur irċieva SMS fuq il-*mobile* tiegħu bl-*activation code* li kienet intalbet.[4] Din l-*activation code* b'xi mod ġiet ikkomunikata lill-frodist(a) u, b'hekk, din setgħet tittrasferixxi l-*mobile app* fuq *device* ieħor u, f'għajnejn il Bank, tagħmel pagamenti daqslikieku qed jagħmilhom l-Ilmentatur.

- Mil-*logs* tal-BOV jidher li l-proċess tal-pagamenti beda fil-ħin ta' 12:24:04, u ż-żewġ pagamenti ilmentati saru fil-ħin ta' 12:25:24 għall-valur ta' €2,409.06 u f'12:26:32 għall-valur ta' €2,529.51.

- Fil-ħin ta' 12:31 ċempel lil *BOV Customer Service* biex irrapporta l-frodi u jipprova jwaqqaf il-pagamenti iżda, peress li l-pagmenti kienu fuq bażi *same day,* dawn laħqu telqu.

[3] P. 60
[4] P. 51

- Fil-ħin ta' 13:27 intbagħtu notifiki urġenti mill-BOV lill-bank ta' barra biex jippruvaw jitwaqqfu l-pagamenti iżda dawn iġġeneraw biss rimbors ta' €97.02.[5]

- Sar rapport lil Reġjun B tal-Pulizija.[6]

L-Ilment

L-Ilmentatur qed jitlob kumpens ta' €6,025.21 li jikkonsisti fl-ammount tal-pagamenti ilmentati €2,409.06 u €2,529.51 = € 4,938.57 spejjeż ta' €86.64 u €1,000 danni morali. Fil-proċess naqqas din it-talba b'€97.02 li kien ġie rkuprat mir-*recall.*[7]

BOV offrewlu kumpens ta' 50% li aktar tard l-offerta ġiet imtejba għal rimbors ta' 70%. L-Ilmentatur ma aċċettax għax ippretenda tal-anqas 90% u, għalhekk, mexxa bl-ilment mal-Arbitru.

Fl-ilment ikkwota diversi ksur tar-regolamenti taħt id-direttiva tal-EU magħrufa bħala PSD 2[8] u, peress li jsostni li huwa la kien negliġenti u lanqas kien awtorizza l-pagamenti jinsisti li għandu dritt għal rimbors sħiħ ħlief għal €50.

Risposta tal-Fornitur tas-Servizz

Fir-risposta[9] tagħhom, il-BOV qalu:

'*Whereas the Bank maintains that the disputed transactions were duly authenticated and properly executed in accordance with PSD2 and CBM Directive No. 1. As previously established, the mobile banking server logs*[10] *show the two successful authentication events at 12:25:24 and 12:26:32 with the message "Your instructions have been processed successfully", and the token audit ties both transactions to the Complainant's secure token with "Success MANUAL sign". The Bank acted promptly once notified (12:31), suspending access and initiating recalls the same day, pursuing recovery to completion. Both transactions were processed within the BOV Mobile Banking daily limit of*

[5] P. 97 - 102
[6] P. 60 - 61
[7] P. 147
[8] EU Directive 2015/2366
[9] P. 88 - 94 u dokumenti annessi p. 95 - 146
[10] Doc. A.

€15,000, confirming compliance with channel-specific thresholds and risk controls;[11]

Whereas under Article 40(1) of CBM Directive No. 1, "A payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction." The Bank's evidence establishes that the transactions bore the Complainant's channel credentials and were authenticated via his registered token, satisfying the legal threshold for authorisation;

Whereas Article 97 of PSD2 requires application of SCA whenever a payer initiates an electronic payment, and for remote transactions, SCA must include elements which dynamically link[12] *the transaction to a specific amount and a specific payee. PSD2 Article 4(30) defines SCA as "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 […] and is designed in such a way as to protect the confidentiality of the authentication data." In BOV Mobile Banking, SCA is implemented through possession (registered device/app and secure token) combined with knowledge/signing (manual token signature/PIN), and the RTS-based dynamic linking requirement is embedded in the payment flow. The server logs and token audit confirm that both transactions were successfully authenticated using the Complainant's secure token, thereby meeting PSD2 SCA (and dynamic linking) standards. Moreover, the Commission Delegated Regulation (EU) 2018/389 provides that the Bank can decide not to apply SCA for transactions considered low risk. However, the Bank always applies SCA, even for low-risk transactions, to ensure the highest level of security possible. In this case, both transactions were approved through full SCA;*

Whereas the BOV 24x7 Terms and Conditions[13] *provide that:*

> *"All payments, instructions […] submitted by you through the Channels, after entering your BOV Securekey security number or numbers ("Security Number/s"), or input your BOV Mobile*

[11] Doc. D.
[12] Commission Delegated Regulation (EU) 2018/389.
[13] Doc. E.

> *PIN ("BOV Mobile PIN"), or input your biometric data, are deemed as* ***binding***[14] *on you.*"

They further impose explicit customer duties:

> "*You must take all the reasonable precautions to prevent the loss, theft or fraudulent use of the BOV Securekey, the Security Number/s […] the BOV Mobile Application […] the BOV Mobile PIN.*"
>
> "*You undertake not to record your BOV Securekey PIN and/or BOV Mobile PIN in any easily recognizable form and to keep said PINs separate from the […] the mobile device.*"
>
> The T&Cs also state (liability):
>
> "*You will be unlimitedly responsible for all transactions carried out via the Channels prior to notification to us […] if you do not take all reasonable steps keep your […] Security Number/s […] and/or you acted in any other way with gross negligence or fraudulently.*"

Whereas Article 45 of CBM Directive No. 1 (*Obligations of the payment service user in relation to payment instruments and personalised security credentials*) imposes the following obligations on the payment service user:

> "*(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 […];*
>
> *(2) […] 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 the Complainant's admission that he entered credentials and generated an activation/signature on a spoof website runs contrary to these obligations and the Bank's T&Cs and supports the Bank's position that any loss

[14] Emphasis added.

is not attributable to a failure of the Bank's authentication, but to credential compromise outside the Bank's control. As a voluntary user of the mobile banking service, the Complainant knows or ought to have known that this service can only be accessed from the Bank's official website or the BOV Mobile App. The Bank has never requested customers to access Internet Banking via a link in an SMS and never calls customers requesting sensitive details. The Bank consistently warns customers to avoid clicking links and disclosing credentials;

Whereas Article 50(1) of CBM Directive No. 1 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.*"

Whereas given the evidence of spoof-page credential entry and manual token signing tied to the Complainant's token, the Bank respectfully submits that PSD2's refund presumption in Article 73 does not arise once proper authentication/execution is proven, and in any event, the allocation of liability is governed by Article 50(1) were the user fails obligations with gross negligence;

Fraud awareness and customer responsibility

Whereas the Bank has, since at least early 2023, sustained a multi-channel consumer-education programme warning about spoofed SMS/calls, phishing links, and bank-impersonation scams, including the "Spot the Scam" initiative and related advisories disseminated via mainstream media and the Bank's official social channels. These warnings explicitly instructed customers not to click links in unsolicited messages, not to disclose credentials or codes, and to report suspicious communications, and were widely circulated months before the Complainant's incident;

Whereas besides communication on social media, in November 2023 the Bank also launched a scheme of sending SMS's directly to its' customers in order to inform them of ongoing scams which may be directed at them. In fact, prior to this incident, the Bank issued direct communication to the Complainant warning against scams. Records confirm that an SMS alert was sent on the 15th April 2025

advising against disclosing credentials, codes, or access internet banking through links received via SMS or email;

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

Whereas the above-mentioned warnings are part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. Besides these SMS's, the Bank also publishes information regarding scams to which customers may be vulnerable to. In fact, in May 2023 the Bank published a page entitled 'Spot the Scam: Bank impersonation Scams' which explains that scammers may use a technique called 'Spoofing' where "scammers manipulate caller ID or email addresses, so they appear to be from reputable companies such as banks. It can be tough to identify and misleading because it makes people think they are communicating with a trustworthy source. Ask yourself what a bank will NEVER ask you for over the phone."[15] *It also explains what personal details such scam may ask for which indicates that the communication is not genuine;*

Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about these scams. 'Doc. G1' shows a comprehensive list of the posts made by the Bank in 2024. Moreover, the Bank coordinated TV appearances where Bank employees explained what spoofing is and how to identify it. These programmes aired on the 10th and 27th April 2023 and September 2023. The Bank also published multiple newspaper articles, on various media as can be seen from the attached list marked as 'Doc. G2;

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

[15] Doc. F

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' [16] 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."*

Whereas despite repeating warnings, public campaigns, and a direct SMS alert advising against disclosure of credentials and access through fraudulent links, the Complainant proceeded to perform all actions necessary for the disputed payments to be executed. This included entering confidential security details on a spoofed website and following instructions provided by the fraudster, culminating in the successful manual signing of both transactions using his secure token. Such conduct constitutes a clear and serious breach of the Bank's T&Cs governing mobile banking services and is in direct contravention of Article 45(1) of CBM Directive No. 1, which obliges the payment service user to use the instrument in accordance with its governing terms. Furthermore, by failing to take reasonable steps to safeguard personalised security credentials, as required under Article 45(2) of the Directive, the Complainant demonstrated a disregard for fundamental security obligations that any prudent user is expected to observe. This pattern of behaviour, voluntary disclosure of sensitive information, compliance with fraudulent instructions, and facilitation of unauthorised access, amounts to gross negligence within the meaning of Article

[16] https://www.mfsa.mt/publication/the-mfsas-guide-to-secure-online-banking/

50(1) of CBM Directive No. 1, which allocates liability for all resulting losses to the payer in such circumstances. Accordingly, any alleged fraud cannot be attributed to deficiencies in the Bank's security framework but rather to the Complainant's active participation and failure to adhere to contractual and statutory duties designed to prevent precisely this type of incident;

Conclusion

For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and law.'[17]

Seduti

Fl-ewwel seduta tas-17 ta' Frar 2026, l-Ilmentatur qal illi waqt il-proċess ta' negozjati, l-BOV aċċettaw li huwa ma kienx awtorizza l-pagamenti u, għalhekk, staqsa kif issa fir-risposta li taw lill-Arbitru ma humiex jaċċettaw dan u lanqas sostnew l-offerti li kienu għamlu.

Fil-kontroeżami kompla jgħid:

'Qed niġi referut għal dak li għidt li jien irċevejt SMS fil-25 ta' Ġunju li lili wasslitni biex nieħu azzjoni.

Mistoqsi naqbilx, ngħid, iva.

Qed jingħad li dik l-SMS kellha link fiha li jien għafast. Ngħid, iva.

Qed jingħad li dik il-link ħaditni f'website li jien assumejt li kienet tal-bank. Ngħid, iva.

Mistoqsi jekk qabel ħadt xi azzjoni fuq il-website, għamiltx il-verifiki tiegħi mal-bank, nirrepeti li qabel dħalt f'dik il-website ġimgħa qabel, kont fuq il-linja mal-Customer Care (u hemm it-transcript), qalli biex nagħmel unblocking ta' dak in-numru li kien blocked u, allura, jien fhimt li dak huwa numru li għandi nafdah.

U, fil-fatt, l-authentication code li bagħat il-bank – għax hawn importanti li ngħidu – illi dawn fi ftit sekondi, minn fuq device li mhix tiegħi, (u huwa obbligu tal-bank li jara li d-device huwa tiegħi għax dak huwa obbligu li joħroġ mill-PSD2), intalbet activation code minn device li ma kienx tiegħi, dik l-activation code intbagħtet mill-bank fuq device oħra, il-mobile tiegħi, li kien f'pajjiż

[17] P. 88 - 93

differenti. Jien daħħaltu fil-website u b'hekk, dawn setgħu jieħdu over u jiġġeneraw is-Signatures kollha.

Qed niġi mistoqsi qabel daħħalt il-kredenzjali tiegħi, ċempiltx lill-bank jew ħadtx xi azzjoni, ngħid li le.

Mistoqsi x'informazzjoni tajt meta dħalt fil-website, daħħalt in-numru li nidħol fl-Internet Banking u talabni niġġenera Signature 1. Iġġenerajt is-Signature 1, u daħħalt in-numru li jagħtik is-Signature 1 li mhijiex is-Signature li biha tagħmel it-transfers.

Mistoqsi naqbilx li t-terza persuna ottjeniet l-aċċess wara li jien tajt dawn id-dettalji, ngħid li dan ma nistax ngħidu jiena; dan x'qal il-BOV. Jien m'inix persuna teknika. Jiena naf x'tajthom.

Qed niġi referut għal li għidt li jien konxju tal-fatt li l-bank qatt ma jibgħat links b'SMS.

Ngħid li jiena m'għidtx hekk. Jiena għidt illi meta ċemplitli din Sandra, u qaltli li kien hemm dawn it-transactions u kienet ser twaqqafhomli b'code, għidt jiena konxju li l-bank mhux ser jitolbok code fuq it-telefon, aktar u aktar biex iwaqqaf transactions li huma ovvja li huma ħżiena. Huwa sens komun, ma tridx tkun għamilt xi PhD fil-Banking. Jekk il-bank jaf li t-tranżazzjonijiet huma ħżiena, ma jgħaddihomx, mela jitlob code lili biex iwaqqafhom.

Mistoqsi jekk qabel dan l-inċident kontx konxju li l-bank qatt ma jitlob klijenti biex jagħtu kredenzjali permezz ta' link, ngħid li le.

Qed niġi referut għal dak li għidt li l-persuna li ċemplitli kienet taf ċertu informazzjoni kunfidenzjali fuqi.

Mistoqsi għalxiex qed nirreferi, ngħid li din bdiet iġġib ruħha b'ċertu kunfidenza bħal persuna li taħdem il-bank; jew kienet taħdem il-bank jew toqgħod iċċempel lil dak u tieħu l-informazzjoni.

Mistoqsi jekk qaltlix xi ħaġa speċifika, ngħid li peress li kellha aċċess għall-Mobile App, milli spjegali l-bank, peress li kienet qed tara l-kontijiet, setgħet qed tikkonferma ma' dak li qed tara. Pereżempju, l-aħħar transaction li kelli, l-aħħar li xtrajt fuq il-Visa. Dawn l-affarijiet li normalment jistaqsi l-bank.

Imma, nerġa' ngħid, x'għamilt jien naf u mhux x'qed tagħmel hi.

Ngħid li l-ewwel xahar, qabel ma ltqajt ma' Kimberly Ann u s-Sur Manuel, jiena moħħi mar li it's an inside job tant kienet taf affarijiet.

Mistoqsi mill-Arbitru jekk hi tatnix informazzjoni li tappartjeni partikolarment lili, ngħid li hekk hu, bħall-bilanċ tal-kont. Però, imbagħad kif spjegatli Kimberly Ann u Manuel, jista' jkun li kellha dik l-informazzjoni għax peress li ħadu over il-Mobile App, setgħet tara dik l-informazzjoni għax fuq il-Mobile App, ikollok il-bilanċ u xi xtrajt l-aħħar, eċċ.

Qed jingħad li jien għafast il-link qabel it-telefonata. Ngħid iva, mela. Ngħid li jien għafast il-link, daħħalt dawn iż-żewġ numri li talabni l-link u għaddiet. U x'ħin ġiet din it-telefonata, qaltli li saru dawn it-transfers u għadda ftit ħin sakemm sibt il-key.

Qed jingħad li l-activation code irċevejtha fuq il-mobile normali tiegħi. Ngħid, iva, żgur. U daħħaltha fil-website. Ngħid li l-activation code intalbet mid-device tagħhom; mhux jien tlabtha l-activation code.

Ngħid li x'ħin ċemplitli, mort inġib il-key għax il-mobile ma stajtx nużah għax kienet fuq it-telefon, dħalt fil-computer u kienu diġà qed jieħdu l-flus.

Is-sekwenza hija li jien għafast il-website, il-website talbitni niġġenera activation code, iġġenerajtha, tajthielha, talbitni s-Signature 1.

L-Arbitru jiddikjara li jrid jiġi ċċarat mil-lat tekniku minn talab l-activation code.

Ngħid li skont kif spjegali l-Bank of Valletta, l-activation code intalbet mid-device tal-frodisti u jien tajthom is-Signature 1 u n-numru li jitla'. Hekk qaluli.'[18]

Fit-tieni seduta li nżammet nhar is-16 ta' Marzu 2025, il-Bank ressaq ix-xhieda ta' Michel Gatt, espert fis-sistema tal-pagamenti elettroniċi tal-BOV. Spjega kif f'għajnejn il-Bank, il-pagamenti ilmentati dehru awtorizzati mill-Ilmentatur u dan skont ir-regoli Ewropej dwar pagamenti.

Spjega li f'dan il-każ, jidher li l-Ilmentatur ikkopera mal-frodist billi daħħal il-kodiċi mitluba li huwa biss kellu fis-*Signature 1 panel* tas-sistema, u dan ippermetta lill-frodist jieħu f'idejh iċ-ċavetta li jawtorizza pagamenti daqslikieku kien l-Ilmentatur li qed jawtorizzahom.

L-Ilmentatur sostna li mhux minnu li l-Bank qatt ma jibgħat SMS li jitolbok tagħfas *link* għax meta jitolbok iġġedded l-informazzjoni dwar KYC hekk jagħmel.

[18] P. 151 - 153

Michael Gatt spjega li l-avviżi tal-Bank huwa li ma jagħfasx *links* li jwasslu biex tagħti informazzjoni dwar, jew li jwasslu għal pagamenti.

Xehed ukoll Keith Vella, uffiċjal inkarigat mis-sistemi ta' *transaction monitoring* tal-BOV. Spjega s-sistemi li joperaw u qal li ma kien hemm xejn li b'xi mod iġġenera xi twissija li l-pagamenti ma kinux awtorizzati.

Qal ukoll li kieku l-BOV ikollu sistemi li jkunu daqstant sensittivi li jżommu pagament kif qed jippretendi l-Ilmentatur, kieku tinħoloq konfużjoni sħiħa għax jitwaqqfu eluf kbar ta' pagamenti ġenwini li llum il-Bank għandu obbligu li jipproċessahom bħala *instant payments.*

Sottomissjonijiet finali

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

Konsultazzjoni mal-*Malta Communications Authority*

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

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

Analiżi u konsiderazzjoni

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

Għal dan il-għan, l-Arbitru qed jannetti ma' din id-deċiżjoni mudell li ppubblika u li ser jiġi wżat biex jasal għal deċiżjoni dwar kif ser isir '*apportionment*' tal-konsegwenzi tal-frodi. Il-mudell fih ukoll diversi rakkomandazzjonijiet biex il-

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

Iżda l-Arbitru jħoss il-bżonn 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*[19] 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[20] 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.

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

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.[21] [22]

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.

[21] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS supplement ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[22] 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	(0%)	0%
Sub-total	(20%)	(80%)
Tnaqqis għal ċirkostanzi speċjali	(20%)	20%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	(20%)	20%
TOTAL FINALI	**60%**	**40%**

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 40% tal-piż u l-60% l-oħra iġorrhom il-BOV.

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

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

L-Arbitru jinnota iċ-ċaħdiet kategoriċi tal-Ilmentatur li huwa ma kienx awtorizza l-pagamenti permezz tas-sistema *Signature 2* tal-BOV *Mobile App*. Filwaqt li dan huwa minnu, iżda l-fatt li b'xi mod ikkomunika l-*Activation Code* lill-frodist(a) kien strumentali biex il-frodist seta' japprova l-pagamenti hu/hi stess.

L-Arbitru jifhem li waqt it-telefonata konvinċenti ta' Sandra, l-Ilmentatur seta' naqqas jew warrab is-salvagwardji soliti għax mill-informazzjoni li bdiet tagħtih dehret telefonata ġenwina.

BOV isostnu li fil-15 t'April 2025, bagħtu SMS ta' twissija lill-Ilmentatur biex ma jagħfasx *links* li jkunu mibgħuta f'SMS anke jekk dan jidher li jkun ġej mil-Bank.[23] Iżda l-Ilmentatur jiċħad li rċieva dan l-SMS ta' twissija peress li kellu problemi tekniċi u ma kienx qed jirċievi SMSes mill-Bank. Id-diskursata mal-Bank fit-18 ta' Ġunju 2025,[24] ġimgħa qabel ma ġara l-każ ta' dan l-ilment, hija prova suffiċjenti li l-Ilmentatur ma kellux il-benefiċċju ta' twissija indikata u, għalhekk, mhux qed jiġi ppenalizzat 20% bħalma kien ikun il-każ kieku kellu dan il-benefiċċju.

Apparti minn hekk, l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatur jitnaqqaslu l-piż ta' negliġenza grossolana b'doża ta' 40%, jiġifieri 20% aktar mill-20% normalment spjegati fil-mudell.

Dan huwa każ fejn il-frodist mhux biss bagħat SMS qarrieq iżda sostna l-kredibbilità tal-SMS permezz ta' telefonata konvinċenti minn persuna titkellem bil-Malti li tat informazzjoni li l-Bank biss seta' jkollu.

[23] P. 91
[24] P. 63 - 68

L-Arbitru jifhem li meta l-Ilmentatur ġie ffaċċjat minn xi ħadd li tippersonifika b'mod espert lill-Bank permezz ta' telefonata '*live*', allura, l-SMS bil-*link* frawdolenti jidher anqas suspettuż, minkejja t-twissijiet li l-Bank kien ħareġ.

F'dan l-aġġustament, minħabba ċirkostanzi speċjali, l-Arbitru qed jieħu wkoll kunsiderazzjoni li huwa kien diġà esprima opinjoni f'deċiżjoni ta' każ ASF 116/2023 li meta jiġi rreġistrat *device* ġdid, irid isir proċess sħiħ ta' rikonferma mill-Bank li dan sar fuq talba ġenwina tal-klijent.

F'dan il-każ, l-Arbitru jinnota li filwaqt li ma kienx hemm bidla tal-*mobile device* u l-istess numru baqa' rreġistrat mal-Bank, iżda fil-proċess kien hemm bidla fis-*software token* li jawtorizza l-pagamenti.

L-Arbitru jirrakkomanda li meta jkun hemm reġistrazzjoni ta' *software token* fuq *device* ġdid (li jkun jinvolvi wkoll *unenrolmen*t minn fuq id-*device* ta' qabel għax il-*Mobile App* tista' tkun irreġistrata fuq *device* wieħed biss) għandu wkoll ikun hemm eżerċizzju ta' rikonferma mal-klijent li dan qed isir bil-permess tiegħu, speċjalment meta jsiru pagamenti immedjati li jiżvijaw mill-mod normali ta' kif jaħdem il-kont.

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

Hemm eżempji ta' istituzzjonijiet finanzjarji u banek li għandhom sistemi ta' pagamenti b'teknoloġija avvanzata, fejn f'każ serju ta' dubju jintbagħat SMS fuq il-*mobile* reġistrat, jinforma li qed jintalab li jsir pagament u l-klijent jintalab jerġa' jikkonferma l-pagament. Dan isaħħaħ is-sigurtà u jevita dewmien biex isir kuntatt permezz tat-telefon mal-klijent.[25]

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

[25] Din it-tip ta' sistema diġà qed topera permezz ta' *3D Secure* f'każ ta' pagamenti bil-*card* lill-*merchants* għal xiri *online*.

B'kollox, għalhekk, qed jiġi intitolat għal kumpens ta' 80% tal-pagamenti frawdolenti li ġie ddebitat lill-kont tiegħu.

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

Għaldaqstant, *ai termini* tal-Artikolu 26(3)(c)(iv) tal-Kap. 555 tal-Liġijiet ta' Malta, l-Arbitru qed jordna lil *Bank of Valletta p.l.c.* iħallas lill-Ilmentatur is-somma ta' tlett elef, disa' mija u tnejn w erbgħin ewro punt ħamsa ħamsa (€3,942.55). It-talba għal danni morali hija miċħuda.

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 2.15% fis-sena[26] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[27]

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

Fl-aħħarnett, l-Arbitru jirreferi għal rapporti mhux konfermati li l-pulizija irnexxielhom jimblokkaw xi fondi misruqa mill-frodisti u, għalhekk, eventwalment jista' jkun hemm xi rkupru minn dan is-sors.

Jekk jirriżulta rkupru bħal dan, biex ma jkunx hemm possibilità ta' arrikkament inġustifikat, l-Arbitru jordna li l-flus ta' xi rkupru jiġu allokati bl-istess mod kif ġie allokat it-telf f'din id-deċiżjoni, jiġifieri 80% għall-BOV u 20% għall-Ilmentatur.

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[26] Ekwivalenti għall-*'Main Refinancing Operations (MRO) interest rate'* kurrenti stabbilita mill-Bank Ċentrali Ewropew.
[27] 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-Ilmentatrici/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.