Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 012/2024

ZN

('Ilmentatur')

Vs

Bank of Valletta p.l.c.

Reg. Nru. C 2833

('Provditur tas-Servizz' jew 'BOV' jew 'Bank')

Seduta 28 ta' Ġunju 2024

Dan huwa ilment li jirrigwardja pagament frawdolenti li sar għan-nom tal-Ilmentatur lil terzi mill-kont li għandu mal-Provditur tas-Servizz.

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-mezż ta' komunikazzjoni normalment użat bejn il-bank u l-klijent, ġeneralment permezz ta' SMS jew e-*mail*.

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

- Minkejja diversi twissijiet 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'xi 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, l-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 li kanal ta' komunikazzjoni normalment użat bejn il-bank u l-klijent jigi 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:

- Fis-7 ta' Novembru 2023, l-Ilmentatur irċieva l-messaġġ frawdolenti permezz ta' *email* li ħaseb li kienet ġejja mill-BOV għalkemm l-*email address* ta' min bagħat l-*email* kien mhux dak li s-soltu juża l-BOV iżda kien 'member@outbound.research.net' li, apparti mill-Ilmentatur, kien indirizzat ukoll lil *'signatures@BOV.com.maler-diel.de'.*[1]

- Billi l-Ilmentatur ħaseb li dan kien messaġġ ġenwin, għafas il-*link* u daħal f'*website* li huwa ħaseb li kienet tal-BOV għax dehret identika. Biex daħal uża il-*One-Time Password* li ġġenera mill-BOV APP.

- L-Ilmentatur isostni li wara li għamel dan, telgħet *window* tgħidlu '*Wait a moment'.* Qal li barra minn hekk ma għamel xejn iżjed u ma approva l-ebda pagament bit *2-Factor Authentication.* Meta pprova joħroġ mill-*website* u jidħol b'mod normali fil-*website* tas-soltu tal-BOV *online*, ma

[1] Paġna (p.) 8

rnexxilux għax ġie infurmat *'I was already logged in'*. Hemmhekk induna li kien hemm xi frodi għaddej.[2]

- Wara xi ħames jew sitt tentattivi, irnexxielu jaqbad bit-telefon mal-Bank biex jirrapporta l-każ. Wara li rrapporta, irċieva SMS mill-Bank li kien sar pagament ta' €4,321 li hu ma kienx awtoriżża. Wara rriżulta li dan sar f'kont bankarju fl-Italja.[3]

- Dan sar f'kont tal-bank tal-frodist li kien poġġa struzzjonijet biex il-pagament isir '*same day*'.[4]

- B'mod qarrieqi, l-pagament kien jindika li l-benefiċjarju kien jismu Amir Namrani,[5] u bħala dettalji tal-pagament indika *"THANK YOU FOR LOAN AMINE XXO".*

- Sar *recall* mill-BOV[6] iżda dan ma ġiex aċċettat mill-Bank tal-Italja.

- Il-każ ġie rrapportat lill-pulizija tal-Portugall, fejn jgħix l-Ilmentatur, għal aktar investigazzjoni tal-frodi,[7] wara li l-Bank rega' tah aċċess għall-*internet banking* biex ikun jista' jippreżenta *statement* li juri l-pagament frawdolenti.

L-Ilment

L-Ilmentatur saħaq li :

> "*No Consent or 2-Factor Authentication: It is crucial to note that no payments or authorizations were initiated by me. What is even more concerning is the absence of any 2-factor authentication requests for such a significant transaction, which deviated from the standard security practices I have come to expect from the bank.*

[2] P. 113
[3] P. 124
[4] *Ibid*.
[5] Is-sistema SEPA timxi strettament skont l-IBAN *number* u s'issa ma tagħmilx konnessjoni mal-isem u l-indirizz tal-benefiċjarju kif dikjarat fit-trasferiment. Għalhekk, għall-frodist, faċli jagħti isem u ndirizz fittizju biex jevita xi mblokk mill-*monitoring systems* tal-Bank. Huwa ntiż li meta tidħol il-PSD 3 jew PSR 1, dan il-*linkage* bejn l-IBAN u l-identità tal-benefiċjarju tkun tassattiva.
[6] P. 110 - 111
[7] P. 21 - 26

Immediate Reporting: As soon as I realized the fraudulent nature of the transaction, I took immediate action by contacting the bank's fraud unit within minutes of the incident. My prompt reporting reflects my commitment to safeguarding my account and cooperating with the bank.

Inadequate Response: Despite my swift reporting and clear indication of fraudulent activity (within minutes of the incident), the bank's response was not commensurate with the gravity of the situation. The unauthorized transaction was allowed to proceed without further security measures or verification, raising questions about the bank's security protocols.

SMS Notification Post-Fraud: It's worth noting that I received an SMS notification of the transaction after I had already informed the bank's fraud unit about the theft. The sequence of events demonstrates the Bank does not have in place an effective notification system and response to suspicious transactions.

Transaction Security: The unauthorized transaction not only lacked 2-factor authentication but has also been affected by the hackers/fraudsters who managed to steal the money within seconds of my entering the fraud email link (bov false site). This incident highlights a gap in the bank's security measures and the need for enhanced vigilance for substantial transactions. I need to highlight that I have not made or authorized any transactions or made any payments from my end.

I feel that the Bank's security measures are not adequate and have not protected my money from this theft.

As I already mentioned previously, I have not made any payments or transactions from my end. However, the fraudsters managed to transfer the money by themselves. Having said this, the money was transferred without the need for the usual protocol, i.e., a 2-factor authentication code. This for me is a complete letdown, since I have always relied on this 2-factor authentication protocol in the past for any of my transfers, yet, someone can hack into my account and manage to steal the money (within seconds) without the same need of this 2-factor authentication

protocol, and before a valid alert text message is even sent by the bank itself that could have prevented the theft in the first place."[8]

Bħala rimedju, l-Ilmentatur talab li l-Bank jirrifondi l-pagament li huwa ma awtoriżżax għal €4,321.

Risposta tal-Provditur tas-Servizz

Fir-risposta tagħhom, il-BOV qalu:

"Respectfully submits:

1. *Whereas in his claim Mr. ZN ('the complainant') states that he 'was deceived by a fraudulent email that meticulously mimicked the BOV website.'[9] He states that he received an email where he 'followed the fraudulent instructions (of entering the website to self-remove the mobile signature restrictions) provided in the email.'*[10]

2. *Whereas the complainant attached the details of the transaction in question, bearing reference number 2331103045532000-1623642718. According to the Bank's records, this transaction was duly authorised on the 7th of November 2023 at 12:39 from credentials associated with Mr. ZN.[11] As part of the Bank's security system which is in line with the Payment Services Directive 2 (PSD 2), there are various levels of authentication to ensure that the transaction was carried out by the complainant, from credentials and systems registered in his name. Therefore, it is completely incorrect and unfounded for the complainant to repeatedly claim that the transaction 'lacked 2-factor authentication.'[12]*

3. *Whereas article 40(1) of Directive 1 of the Central Bank of Malta (which Directive is based on the PSD2) provides that a payment transaction is*

[8] P. 3 - 4
[9] P. 3 *of the complaint.*
[10] *Ibid*.
[11] *DOC. A – Internet Banking log showing the transaction.*
[12] P. 3 *of the complaint.*

considered to be authorised only if the payer has given consent to execute the payment transaction. As explained, the Bank received legitimate instructions from credentials associated with the complainant and therefore has no obligation to refund the complainant.

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

   *'**strong customer authentication'** means an authentication based on the use of two or more elements categorised as **knowledge (something only the user knows), possession (something only the 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'.*[13]

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

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

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

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

[13] *Article 4(30) of PSD2*

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

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

6. *Whereas Mr. ZN was not only aware of the amount of the transaction, but also input it himself in the token which is either the BOV app or the physical internet banking key (this is the element of possession of strong customer authentication). Besides this, he also input the last 5 digits of the IBAN number of the recipient, and this satisfies the element outlined in article 5(c) above mentioned. Upon entering these details, a code would have been generated which needs to be used to approve the transaction.*

7. *Whereas this payment was approved by the confidential details of Mr. ZN with the use of his token. The Bank had no control over this transfer because it was completely in the control of the complainant without the Bank's intervention. Once the Bank receives legitimate instructions for a 'third party payment' from the adequate channels, the Bank implements them, as it is reasonably expected that the only person who has access to such confidential details and systems is the person with whom they are associated. In fact, this is outlined in the terms and conditions of the Internet Banking system (attached and marked as **'DOC.B'**) which provide the following:*

> *'You authorise us to act on any instruction that we receive through the Channels which has been, or reasonably appears to have been, sent by you and which, where applicable, has been sent using your Security Number/s or BOV Mobile PIN or biometric data.'*[14]
>
> *'All payments, instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your BOV Securekey*

[14] *DOC.B: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 5.*

*security number or numbers ("Security Number/s"), or input your BOV Mobile PIN ("BOV Mobile PIN"), or input your biometric data, are deemed as **binding** on you.'*[15]

8. *Whereas in fact, every token used to generate codes in order to approve a payment has a certificate associated with it. In fact, the certificate number associated with the token with which the payment in question was approved is the same one associated with the token of the complainant which he previously used to make other payments, the legitimacy of which is not being contested. This can be seen from the document attached and marked as **'DOC.C'.***

9. *Whereas besides the fact that the payment was duly authorised, there is also the fact that the transaction amount was within the limit imposed for these kinds of transactions. With respect to the transaction in question in this arbitration, which is a 'third-party transaction', the limit is five thousand euro, as can be seen in the highlighted section in the document attached and marked as **'DOC.D'** (this document is accessible from the Bank's website.) Therefore, there were no suspicious signs for the Bank with respect to this transaction. One should also note that the PSD 2 does not oblige the Bank to impose any limit on transactions. It only stipulates that if there is the possibility to put in place spending limits, the customers should be informed of this*.[16]

10. *Moreover, the above-mentioned Commission Regulation provides that the Bank can decide to not apply strong customer authentication for transactions which are considered to have a low level of risk.*[17] *Therefore, one can conclude that when a transaction is considered to be of a higher risk, (because for example it is not of an amount normally done by the* customer), *the Bank should implement the use of strong customer authentication, which was in fact done in this case.*

11. *Whereas without prejudice to the above, if the complainant is alleging that this transaction was not authorised and he has evidence of this, then the Bank is still not obliged to refund him since even if the complainant did not*

[15] *Ibid*, *page* 4.
[16] *Article 28(2) of Directive 1 of the Central Bank of Malta which reflects article 52(2) of the PSD 2.*
[17] *Article 18 of Regulation (EU) 2018/389.*

*have the intention to approve a payment, he still followed the necessary steps to approve it. In this respect the Bank refers to article 45 of Directive 1 of the Central Bank of Malta, particularly to the article entitled '**Obligations of the payment service user in relation to payment instruments and personalised security credentials'** which provides the following:*

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

12. 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**.'*

13. *Whereas if the complainant is alleging that the transaction was not authorised, this means that he generated the necessary codes for the payment to be approved and passed them on to a third party. In order to generate such a code, he had to insert the amount of the transaction and the last 5 digits of the recipient's IBAN. This fact should have raised suspicion within Mr. ZN since if he had no intention of approving a payment, then it would have been reasonable for him to take action and ask why he was being asked to input an 'amount' and a 'payee code' which they accessed from a section entitled 'transaction signing'[18]. He could have confirmed this doubt with the Bank who would have immediately informed them that the email was not genuine.*

[18] *DOC.E – Visual of sections used for approval of transaction*

14. *The fact that he provided all these details and followed all the necessary steps, goes against the terms and conditions of the internet banking service which provides the following:*

> *'You must take all the reasonable precautions to prevent the loss, theft or fraudulent use of the BOV Securekey, the Security Number/s, the BOV Securekey PIN, and/or the BOV Mobile Application, the BOV Mobile Authentication Software, biometric data, the BOV Mobile PIN, as applicable. You undertake not to record your BOV Securekey PIN and/or BOV Mobile PIN in any easily recognizable form and to keep said PINs separate from the BOV Securekey and/or the mobile device. You must make every effort to prevent the BOV Securekey, the Security Number/s, the BOV Securekey PIN and/or the BOV Mobile Application, the BOV Mobile Authentication Software the BOV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party.'*[19]

15. *Whereas as a voluntary user of the internet banking service, the complainant knows or ought to know that this service can only be accessed from the Banks' website or from the BOV Mobile App. Whereas the Bank never before requested the complainant (or any other customer) to access their internet Banking from a link in an email, 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. In fact, in May 2014, the published 'Tips for Safer Mobile Banking'*[20] *which amongst other provide the following:*

- *'Watch what you send: never disclose, either via text, email, or through a website, any personal information such as account numbers, passwords, or personal info that could be used by unscrupulous persons to gain unauthorised access to your bank accounts.*
- *Do not trust links or attachments that originate from people you do not know. If a person you do know has sent you a link or*

[19] *DOC.B: 'BOV 24X7 Services – Important Information and Terms and Conditions of Use' Page 7*
[20] *DOC.F 'BOV Mobile Banking – Tips for Safer Mobile Banking'*

attachment, check with them that it is legitimate before opening it.'

16. *Whereas as can be seen from this extract, the Bank warns customers to be careful and confirm if a link is genuine, even if they know the person who sent it to them, and this to avoid incidents of fraud.*

17. *Whereas the above-mentioned warning is part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. The above-mentioned document and others similar to it are easily accessible from the Bank's website and every customer should have an interest of keeping themselves informed and updated on the terms and conditions which regulate a service they voluntarily subscribed to, something which is reasonably expected from all consumers.*

18. *Whereas 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.'*[21] *It also explains what personal details such scam may ask for which indicates that the communication is not genuine. As will be explained throughout the proceedings, the Bank cannot control such incidents of spoofing.*

19. *Whereas the email address from which the customer received communication had clear indications that it was not the genuine since the recipient name was signatures@bov.com-maler-diel.de via research.net and the actual email address was member@outbound.research.net.*[22] *This fact could have raised suspicion in the complainant which would have led him to use more caution before accessing the link, providing confidential details on it and following instructions provided by this website.*

20. *Whereas the Bank has also been making numerous campaigns on newspapers, social media and television in order to raise awareness about*

[21] *DOC.G: 'Spot the Scam: Bank impersonation Scams'*
[22] *P. 27 of the complaint*

*these scams. **'DOK. H1'** shows a comprehensive list of the posts made by the Bank on social media in the 6 months preceding the incident in question. Moreover, the Bank coordinated TV appearances where Bank employees explained what spoofing is and how to identify it. These programmes aired on the 10th of April 2023, 27th of April 2023 and September 2023. The Bank also published multiple newspaper articles, on various media as can be seen from the attached list marked as **'DOC.H2'**.*

21. *Whereas besides information provided by the Bank, there are various entities which make educational campaigns in order to raise awareness concerning fraud which may be directed to consumers of financial services. These include the Malta Financial Services Authority who provide information on how a person can identify a system where a payment is to be made. Of particular relevance is the page 'The MFSA's Guide to Secure Online Banking'*[23] *which provides the following*:

- *Use the genuine internet website of the bank. Never access the bank's website through links contained in emails or SMS, unless you are sure of the identity of the sender. It is always best to access the bank's website by **typing in the web address, as provided by the bank, directly in the browser.***
- *Follow the **information and guidelines provided by your bank** on how to use digital banking services.*
- *Take the necessary time to **read the terms and conditions provided by your bank**.*
- *Ensure that you always **protect all personal details** such as card details, passwords, and other confidential data to access the bank's online platform or mobile app.*

22. *Whereas despite all these warnings, Mr. ZN still carried out all the necessary actions for the payment to be approved and therefore, breached the terms*

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

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

23. *Besides this, he also acted against article 45(2) of the Directive because he did not take all the reasonable steps to keep his personalised security credentials safe. It is reasonably expected that a consumer is aware of the terms which regulate the contractual relationship by which they are bound and adhere to them.*

24. *Therefore, any alleged fraud which occurred due to the participation of Mr. ZN who provided confidential details on a fraudulent website and followed instructions provided by this website. All this contributed to his gross negligence. Therefore, the fraud occurred due to the gross negligence of the complainant and not 'due to a lack of bank protection measures'*[24] *because as outlined above, the Bank's security measures for the approval of a payment are in line with the law.*

Timeline of Events

25. *Whereas the payment was approved on the 7th of November 2023 at 12:39. This kind of payment is processed immediately as can be clearly seen in the terms and conditions marked as* ***'DOC.B'****, particularly in the section entitled 'Cancelling or changing a payment instruction' which provides 'If you ask us to make a payment immediately, we cannot change it or cancel the payment instruction because we start processing it when we receive it.' The Bank submits that this clause is in conformity with article 80 of the Payment Services Directive 2, entitled 'Irrevocability of a payment order'.*

26. *Whereas when Mr. ZN informed the Bank of the situation, he was informed that the Bank may initiate a recall request for which a €20 charge is associated, to which Mr. ZN consented. He was also informed that there is no guarantee that the funds will be returned and was also told this his internet banking will be blocked. The complainant was also informed of the need to file a police report regarding his case.*

27. *In fact, the Bank initiated a recall request on the same day, i.e., on the 7th of November 2023 at 13:36 to the beneficiary bank where the funds were*

[24] *P.4 of the complaint*

received. Multiple reminders were also sent by BOV, and an eventual negative reply was also received as can be seen from ***'DOC.I'***.

28. *The outcome of the recall process depends completely on the bank where the funds were received since they would have their internal procedures and rules and BOV has no control over other banks and therefore cannot dictate how long they take to answer the recall request or what kind of answer they give.*

29. *Therefore, the Bank respectfully submits that it did its' utmost to recover the funds and give them to the complainant. However, this was not successful, and the Bank informed the complainants of this as seen from the email attached by the complainant*.[25]

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

<u>Conclusion</u>

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

32. *Chapter 555 of the Laws of Malta vests the Honourable Arbiter with the authority to decide a case on the basis, inter alia, of the Complainant's legitimate expectations and what he deems fair and equitable in the circumstances of the case. The Bank very respectfully submits that such element of fairness and a customer's legitimate expectations are founded and pivot on a balance between rights and obligations whereby a customer most certainly has rights but also an inherent interest and obligation to faithfully abide with all terms, conditions as well as guidelines issued by the Bank, as these are ultimately intended to serve and protect the customer.*

[25] *P. 14 of the complaint*

33. *The Bank reserves the right to bring oral and documentary evidence in order to substantiate the defenses raised in this reply, as well as to make submissions both verbally and in writing pursuant to the provisions of Chapter 555 of the Laws of Malta.*

34. *The Bank reserves all rights/actions pertaining to it at law, and respectfully requests the Arbiter to reject and dismiss the complaint's claims.*

With expenses."[26]

Seduti

Saru żewġ seduti nhar is-7 t'April 2024[27] u t-28 ta' Mejju 2024.[28]

Il-partijiet waqt ix-xhieda u s-sottomissjonijiet żammew il-pożizzjoni kif spjegata fl-ilment u fir-risposta tal-BOV.

L-Ilmentatur kompla jinsisti li huwa ma kienx awtoriżża l-pagament:

> ***"Ngħid li kont nużah l-internet banking u naf kif nagħmel pagament mill-online banking lil terzi; fejn kont irrid nerġa' mmur fil-Mobile App, inġib il-kodiċi, nimla l-ammont, indaħħal l-aħħar kodiċi.***
>
> ***Mistoqsi mill-Arbitru jekk f'dan il-każ dan l-aħħar pass għamiltux, ngħid li mhux talli m'għamiltux, imma ma għamilt l-ebda pagament. Jien m'għamilt l-ebda pagament."***[29]

Min-naħa l-oħra, l-BOV isostni li huwa kien għal kollox konformi mal-liġi kif tipprovdi l-PSD 2[30] u l-*Banking Directive* 1[31] maħruġa mill-Bank Ċentrali ta' Malta.

Il-BOV saħaq li huwa kellu sistema robusta u għal kollox konformi mat-*two-factor authentication provisions* tal-PSD 2 u, allura, la l-pagament kien awtentikat b'mod sħiħ mill-Ilmentatur bilfors kien hemm negliġenza grossolana

[26] P. 50 - 57
[27] P. 112 - 115
[28] P. 121 - 123
[29] P. 114
[30] *Directive (EU) 2015/2366 commonly referred to as PSD 2meant to safeguard the consumer (PSU) from having responsibility for payments which are not properly authorised.*
[31] *Directive 1 – THE PROVISION AND USE OF PAYMENTS SERVICES ref CBM 01/2018 which is modelled on the requisites of Directive (EU) 2015/2366.*

min-naħa tiegħu li tagħmlu għal kollox responsabbli biex iġorr il-konsegwenzi tal-frodi li ġarrab.

Il-Bank tella' jixhed lil Michael Gatt, *Senior Manager* fil-*Payments and Multi-Channel Banking*. Huwa spjega t-*transaction log*[32] li hemm annessa mar-risposta tal-Bank.

Din turi li biex saret it-tranżazzjoni kien hemm *log-in* validu fil-ħin ta' 12:34. U, mbagħad, f'affari ta' sitt minuti, min daħal kellu aċċess jiċċekkja l-bilanċi u jifformula pagament lil terzi billi daħħal il-kodiċi kollha neċessarji skont it-2-*factor authentication* li kollha kienu korretti mal-ewwel, u l-pagament ġie awtoriżżat fil-ħin ta' 12:39 u kien hemm *log-out* fil-ħin ta' 12:40.

> ***"Ngħid li biex sar il-pagament kellu jkun hemm l-authorisation code. Dan l-authorisation code ma setax ġabu l-frodist mingħajr l-għajnuna ta' (Ilmentatur) ... Il-bank jista' jkollu s-sistemi kollha tad-dinja u l-aktar ħaġa sikura għax il-weakest link ikun l-end user. Jekk inti għandek dar u jien tajtek l-ewwel ċavetta, it-tieni ċavetta u t-tielet ċavetta, inutli li jkollok il-locks tajbin".***[33]

Fil-kontroeżami, l-Ilmentatur staqsa jekk is-sistema tal-BOV għadhiex turi l-istess ħaġa li kemm l-ammont li nsteraq daħħlu l-Ilmentatur u kemm in-numri ħariġhom l-Ilmentatur u mhux li l-frodist irnexxielu jidħol u jisraq mingħajr l-awtoriżżazzjoni tal-Ilmentatur.

Dokument C[34] anness mar-risposta tal-BOV turi li *token serial* FEB9932609 intuża biex ġie awtoriżżat dan il-pagament li kien l-istess *token* li ntuża mill-Ilmentatur biex għamel pagamenti simili u ġenwini qabel (fis-16 t'Ottubru 2016 u l-20 ta' Ġunju 2023).

Michael Gatt spjega li kieku l-frodist seta' waħdu jiġġenera l-*authorisation code,* kieku kien jerġa' jidħol biex jagħmel pagamenti oħra imma dan ma ġarax.

[32] P. 59
[33] P. 122
[34] P. 71

Sottomissjonijet finali

Fis-sottomissjonijiet finali tagħhom, il-partijiet reġgħu sostnew il-pożizzjoni tagħhom.

L-Ilmentatur jiċħad li huwa ta l-kodiċi neċessarji ġġenerati mit-*token* tiegħu biex il-frodist seta' jagħmel il-pagament.[35]

Il-BOV isostni li l-pagament ma kienx isir kieku l-Ilmentatur ma għamilx hekk.

Il-Bank sostna wkoll li l-Ilmentatur messu mill-ewwel induna li l-*email* li rċieva ma kinetx mill-Bank għax kellha indirizzi foloz.[36]

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 lil 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 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, ikun floku li jippubblika 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.

[35] P. 125 - 126
[36] P. 128 - 133

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 jemfasiżża bil-qawwa li, filwaqt li huwa minnu li l-banek ma għandhomx mezż kif jipprojbixxu li jsir *spoofing/smishing* fil-mezżi ta' komunikazzjoni li jużaw mal-klijenti, m'humiex jagħmlu biżżejjed biex iwissu b'mod effettiv lill-klijenti biex joqgħodu attenti; biex ma jagħfsux *links* li jkunu f'dawn il-messaġġi avolja jkunu jidhru li ġejjin mill-bank konċernat fuq il-mezż 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*[37] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara ilmenti minn ilmentaturi li faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[38] 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 awtoriżżat 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

[37] Deċiżjoni 13 ta' Settembru 2018, C-54/17
[38] *Article 64 of PSD 2*

involviment tal-klijent/ilmentatur, jagħmel awtoriżżazzjoni 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. Ċirkostanzi fejn il-klijent ikun f'negozjati għal xi self mill-bank jew li l-klijent ikun imsiefer u jkun qed jagħmel tranżazzjonijiet li mhux soltu jagħmilhom u, b'hekk, inaqqsu s-suspett tal-klijent li l-messaġġ li rċieva jista' jkun frawdolenti.

Il-mudell għandu wkoll għarfien dwar jekk l-ilmentatur ikunx midħla tas-sistemi ta' pagamenti *online* mal-bank billi jkun għamel xi pagament simili (ġenwini) 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.[39] [40]

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.

Mix-xhieda tal-partijiet, il-pożizzjoni tal-BOV li kien l-Ilmentatur li b'negliġenza kompla jikkopera mal-frodist sal-punt li awtoriżża l-pagament ilmentat, hija aktar kredibbli miċ-ċaħda tal-Ilmentatur li huwa kulma għamel kien li għafas il-*link* u daħħal il-*One-Time Password* iżda ma kienx aktar involut biex seta' jsir il-pagament ilmentat.

Anke l-fatt li l-*email* frawdolenti kellha indizzji ċari li juru li ma kinetx ġenwina, juri livell ogħla ta' traskuraġni min-naħa tal-Ilmentatur. Każijiet simili fejn jintuża l-kanal tal-SMS li normalment juża l-Bank biex jikkomunika mal-klijent, ikollhom indizzji anqas evidenti minn dan il-każ li l-messaġġ huwa frawdolenti.

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

[39] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS *supplement* ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[40] PSD 2 Eu 2015/2366, Artiklu 68(2).

	Perċentwal ta' ħtija tal-Provditur 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	0%	0%
Tnaqqis għal assenza ta' pagamenti simili ġenwini fl-aħħar 12-il xahar	0%	0%
TOTAL FINALI	20%	80%

Għalhekk, skont il-mudell, l-Ilmentatur għandu jġorr 80% tal-piż u l-20% l-oħra iġorrhom il-BOV.

Il-mudell isib li l-Ilmentatur bilfors li baqa' jikkopera mal-frodist billi mela l-ammont u l-aħħar 5 ċifri fis-*Signatures* tal-App u fl-aħħar iġġenera l-kodiċi li awtoriżżat il-pagament. Dan iżid id-doża ta' negliġenza tal-Ilmentatur.

Iċ-ċaħda li huwa fil-fatt għamel dan hija kontradetta b'evidenza ċara li l-kodiċi li awtoriżża l-pagament ħareġ mit-*token* li normalment juża biex jagħmel pagamenti simili, u li l-frodist ma setax iġib din il-kodiċi ħlief mingħand l-Ilmentatur.

Il-mudell jiskużah biss għax ma kienx irċieva twissija diretta mill-BOV dwar dawn l-iskemi frawdolenti fix-xhur ta' qabel dan il-każ u, għalhekk, joffrilu kumpens ta' 20%.

L-Arbitru ma jsibx li l-BOV naqas b'xi mod u ppreġudika l-pożizzjoni tal-Ilmentatur għax ir-*recall* tal-pagament konċernat ma tatx riżultat. L-ewwel nett, la l-pagament jiġi approvat fuq bażi *same day,* dan jitlaq mill-ewwel u l-ebda *recall* ma twaqqfu.

Kif ukoll, il-Bank ressaq provi li fi żmien qasir wara li l-klijent ċempel biex jirrapporta l-frodi (li seħħet fil-ħin ta' 12:39), il-Bank bagħat *recall* fil-ħin ta' 13:38.[41]

Il-fatt li l-SMS tal-BOV li sar il-pagament l-Ilmentatur irċevih fil-ħin tal- Portugall, 12:03,[42] ħin lokali ta' 13:03, ma jfisser xejn avolja l-Ilmentatur isostni li qabel irċieva dan l-SMS kien diġà rrapporta l-frodi. Il-Bank ma għandux obbligu regolatorju li jibgħat SMS biex jinforma dwar il-pagament u, ntbagħat x'ħin intbagħat, il-pagament kien sar fil-ħin 12:39 fuq bażi *same day* u, għalhekk, ma setax jiġi mwaqqaf.

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' tmien mija u erbgħa u sittin ewro punt tnejn zero. (€864.20)

[41] P. 110
[42] P. 118

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 4.25% fis-sena[43] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[44]

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

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

Nota ta' Informazzjoni relatata mad-Deċiżjoni tal-Arbitru

Dritt ta' Appell

Id-Deċiżjoni tal-Arbitru legalment torbot lill-partijiet, salv id-dritt ta' appell regolat bl-artikolu 27 tal-Att dwar l-Arbitru għas-Servizzi Finanzjarji (Kap. 555) ('l-Att'), magħmul quddiem il-Qorti tal-Appell (Kompetenza Inferjuri) fi żmien għoxrin (20) ġurnata mid-data tan-notifika tad-Deċiżjoni jew, fil-każ li ssir talba għal kjarifika jew korrezzjoni tad-Deċiżjoni skont l-artikolu 26(4) tal-Att, mid-data tan-notifika ta' dik l-interpretazzjoni jew il-kjarifika jew il-korrezzjoni hekk kif provdut taħt l-artikolu 27(3) tal-Att.

Kull talba għal kjarifika tal-kumpens jew talba għall-korrezzjoni ta' xi żbalji fil-komputazzjoni jew klerikali jew żbalji tipografiċi jew żbalji simili mitluba skont l-artikolu 26(4) tal-Att, għandhom isiru lill-Arbitru, b'notifika lill-parti l-oħra, fi żmien ħmistax (15)-il ġurnata min-notifika tad-Deċiżjoni skont l-artikolu msemmi.

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

[44] [44] 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.

Skont il-prattika stabbilita, id-Deċiżjoni tal-Arbitru tkun tidher fis-sit elettroniku tal-Uffiċċju tal-Arbitru għas-Servizzi Finanzjarji wara li jiskadi l-perjodu tal-appell. Dettalji personali tal-ilmentatur/i jkunu anonimiżżati skont l-artikolu 11(1)(f) tal-Att.