Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 020/2024

RQ

('l-Ilmentatriċi')

vs

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

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

Seduta 9 ta' Diċembru 2024

L-Arbitru,

Ra l-Ilment[1] datat 16 ta' Frar 2024 magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €6,000 rigward pagamenti li saru mill-Ilmentatriċi lil terzi mill-kont tal-*credit card* tagħha mal-Bank 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 *email*.
- 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.

[1] Formola tal-Ilment minn Paġna (P.) 1 - 6 b'dokumentazzjoni addizzjonali minn P. 7 - 25

- 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-klijenti, 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 l-frodist ikun pront jiġbed jew jittrasferixxi l-flus appena jaslu fil-kont indikat.

- B'riżultat jinħoloq nuqqas ta' fteħim 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 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 id-dettalji relevanti:

- Fis-17 ta' Marzu 2023, għall-ħabta tat-8 p.m., l-Ilmentatriċi irċeviet il-messaġġ frawdolenti fuq il-*mobile* permezz ta' SMS fejn is-soltu tirċievi notifiki mill-BOV.[2]

- Billi l-Ilmentatriċi ħasbet li dan kien messaġġ ġenwin mill-BOV, għafset il-*link* kif mitluba fil-messaġġ qarrieqi li kien għamel referenza għall-imblokk tad-*debit card* u mhux tal-*credit card.*

- Kif għafset il-*link* daħlet f'*site* fejn bdiet timla d-dettalji tal-kredenzjali sigrieti tagħha biex mingħaliha tiżblokka l-*card*.

[2] P. 15

Irċeviet telefonata fuq numru li kien jidher tal-BOV (21312020) u leħen ta' raġel jitkellem bl-Ingliż qalilha li kien mill-BOV u ried jgħinha għax kien hemm talba għal pagament ta' €1,500 fuq il-*card* tagħha li kien jidher dubjuż, u talabha l-kredenzjali sigrieti biex iwaqqaf dan il-pagament.[3]

- Irċeviet messaġġi SMS fuq l-istess kanal li s-soltu juża l-Bank biex jassigura li kienet qed titkellem ma' rappreżentant awtorizzat tal-BOV.[4]
- Wara li mxiet pass pass mal-istruzzjonijiet kollha li taha l-frodist, u kkkonfermat kollox permezz tat-*3D Secure*, qalet li b'għafsa waħda ħarġu tliet pagamenti t'€2,000-il wieħed li assorba kompletament il-*credit limit* tal-*card* ta' €6,000.
- Kif ġara hekk, il-frodist bidel minn vuċi edukata u professjonali għal ton dispreġġjattiv u b'hekk intebħet li kienet ġiet iffrodata.
- Fil-*credit card statement* jidher li dawn il-pagamenti saru lil *Binance* li hi magħrufa bħala *crypto exchange* u *digital wallet provider.*[5]
- Għamlet kuntatt mal-BOV biex tirrapporta l-frodi u qalet li ġiet assigurata li l-Bank ser jirkupra l-flus li nsterqu mill-kont tagħha. Il-BOV jiċħad dan, anzi qal li l-pagamenti la ġew awtorizzati mill-Ilmentatriċi stess permezz tat-*3D Secure* ma kienx każ li jitlob *chargeback*.
- Għamlet ukoll rapport fl-Għassa tal-Pulizija tar-Raħal il-Ġdid.[6]
- Il-BOV bagħat tliet SMSes, wieħed għal kull pagament, wara li saru biex jinforma b'dan lill-Ilmentatriċi.[7]

L-Ilment[8]

[3] P. 61 - 62
[4] P. 15
[5] P. 9
[6] P. 19 - 21
[7] P. 70
[8] P. 1 - 6 u dokumenti annessi P. 7 - 25

L-Ilmentatriċi saħqet li l-SMS frawdolenti kienet irċevietu fuq l-istess numru li s-soltu tirċievi messaġġi mill-BOV. Qalet li l-Bank qatt ma kien infurmaha direttament biex toqgħod attenta minn messaġġi bħal dawn.

Sostniet li hija ma kienet awtorizzat l-ebda wieħed mill-pagamenti konċernati li saru fl-istess ħin b'għafsa waħda kif qalilha dak li kien qed ikellimha, u li hi m'għandhiex tort taħseb li dan kien rappreżentant tal-BOV la kien qed ikellimha fuq l-SMS *chat* u n-numru tat-telefon tal-Bank.

Bħala rimedju hija talbet lill-Provditur tas-Servizz jirrifondilha l-pagament ta' €6,000 u l-ispejjeż relatati ta' €57.70.

Risposta tal-Provditur tas-Servizz

Fir-risposta[9] tagħhom, il-BOV qalu:

1. '*Whereas (''the complainant'') states that on the 17th of March 2023, she was a victim to an incident of fraud where she lost €6000. She explains that the interaction first started when she received a message informing her that her debit card had been blocked and provided her with a link to follow in order to remove the block. She explains that this SMS was received through the same thread of SMS's where she receives genuine SMS from the Bank.*[10]

2. *Whereas the complainant attached an extract showing the transactions in question; these being 3 transactions of €2,000 each which were carried out on the 17th of March 2023 to 'Binance'.*[11] *According to the Bank's records, these transactions were duly authorised on the 17th of March 2023 through the BOV 3D Secure app of the complainant. 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 transactions were carried out by the complainant, from credentials and systems registered in her name. In fact, these transactions had no indication that they were fraudulent.*

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*

[9] P. 31 - 36 u dokumenti annessi P. 37 - 60
[10] P. 3
[11] P. 9

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'.*[12]

5. *Whereas the complainant was aware of the amount of each transaction, the merchant who was receiving the money and the card from which the money would be taken. These details were visible on the 3D Secure app of the complainant, and she would have needed to authorize each payment through the use of her passcode or fingerprint (if her device supports the use of this feature). This satisfies the element of possession in strong customer authentication. This process can be seen from the document attached as **'DOC.A'** (which is easily accessible on the Bank's* website). *These phrases all clearly indicate that one is approving a transaction.*

6. *Whereas these payments were approved through the use of the card details of the complainant with the use of her BOV 3D Secure app. The Bank had no control over these transfers because they were completely in the control of the complainant without the Bank's intervention. Once the Bank receives legitimate instructions for a payment from the adequate channels, the Bank implemented 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.*

[12] Article 4(30) of PSD2

7. *Whereas the complainant was familiar with the system of approving a payment through the BOV 3D Secure app because according to the Bank's records, she had previously approved payments through the use of this app. In fact, the Bank's records show that the complainant started using the BOV 3D Secure app on her device on the 29th of December 2022 and until the 18th of March 2023, the same device was used to make all approvals through the BOV 3D Secure app (as shown in 'DOC.B'). This confirms that the complainant approved the transactions herself.*

8. *Whereas without prejudice to the above, if the complainant is alleging that these transactions were not authorised by her and has evidence of this, then the Bank is still not obliged to refund her since even if she did not have the intention to approve the payments, she still followed the necessary steps to approve them. 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.***

9. *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**.'*

10. *The fact that she provided all these details and followed all the necessary steps to approve the transactions (even if she did not have the intention to*

do them), goes against the terms and conditions of the BOV Visa Gold Card[13] *which provide the following:*

3. Your PIN/3D Secure Passcode/Verification Codes/Other Security Details

a) You may use your Card to effect transactions through various channels. For this reason you will be issued with any one, or all, of the below:

i) A PIN – personal identification number to be used for example at the ATM or at the Point of Sale;

ii) A 3D Secure passcode – to be used for example when effecting online purchase;

iii) A verification code – to be used to verify your cards when registering to an eWallet, or an app, such as the Bank's BOV Pay app or the BOV 3D Secure app.

b) 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.

11. *Whereas as a voluntary user of the BOV 3D Secure app, the complainant knows that the steps she was following were those used to approve a payment. Whereas the Bank never before requested the complainant (or any other customer) to unblock their card a link in a SMS. 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'*[14] *which amongst other provide the following:*

[13] DOC.C: Product Information Guide of the Visa Gold Card.
[14] DOC.D: 'BOV Mobile Banking – Tips for Safer Mobile Banking'.

- *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 attachment, check with them that it is legitimate before opening it."*

12. *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 and prevent customers from falling victim to spoofing/smishing/vishing where fraudsters may impersonate Banks. As will be explained throughout the proceedings, the Bank cannot control such incidents of spoofing/smishing/vishing.*

13. *Whereas the abovementioned warning is part of an ongoing educational campaign which the Bank has been carrying out for the past number of years. The abovementioned document and others similar to it are easily accessible from the Banks' 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.*

14. *Whereas the Bank also publishes information regarding scams to which customers may be vulnerable to. In fact, in **May 2021**, the Bank published the page entitled 'Warning: Scam alerts' (attached and marked as **'DOC.E'**) which explains that SMS fraud is when a fraudster sends a message where he presents himself as a bank or a known company. In fact, the Bank warns clients to not access links which do not contain the official Bank URL which is '**www.bov.com'**. Moreover, it also warns customers that fraudsters may use a combination that may look similar to the Bank's official website.*

15. *Whereas the link which the complainant received in the SMS, contained indications that it was not genuinely that of BOV since the URL was not that of BOV, but it was 'bov-mobile-security.com'. This fact could have aroused*

suspicion in the complainant which would have led her to exercise more caution before entering this link.

16. *Whereas the page entitled 'Warning: Scam alerts'[15] also informs customers that "**Bank of Valletta does NOT send text messages or messages via social media asking customers to unlock suspended or blocked accounts or provide personal or financial information**."*

17. *Whereas besides information provided by the Bank, there are various entities which make educational campaigns in order to raise awareness concerning fraud which may be directed to consumers of financial services. These include the Malta Financial Services Authority 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'[16] which provides the following:*

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

18. *Whereas despite all these warnings, the complainant still provided confidential details, such as her card details and carried out all the necessary actions for the payment to be approved, even if she did not have the intention of making a payment. Therefore, she breached the terms and*

[15] DOC.E: Webpage entitled 'Warning – Scam Alert'.
[16] https://www.mfsa.mt/publication/the-mfsas-guide-to-secure-online-banking/

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

19. *Besides this, she also acted against article 45(2) of the Directive because she did not take all the reasonable steps to keep her 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.*

20. *Therefore, any alleged fraud which occurred due to the participation of the complainant who provided confidential details and followed clear instructions which showed she was approving a payment, even if she did not have the intention to do so. All this contributed to her gross negligence.*

21. *Whereas on the 17th of March 2023 at 20:49, the complainant called the Bank to report the incident. The representative who spoke to her blocked her cards and told her what documents she needs to submit in order for the Bank to investigate her complaint. At no point did the analyst assure her that she would receive the money back.*

22. *Whereas once the complainant submitted the necessary documents for the Bank to investigate the matter, it resulted that the complainant had approved the transactions herself through the use of her 3D Secure app. Therefore, it was concluded that she is not entitled to a refund. In fact, the Product Information Guide of the BOV Visa Gold Card provides the following:*

> *14 (b) We cannot cancel a payment made using your Card once you have given consent to make the payment to a retailer or supplier or provided your PIN and/or Card/Security Details and enabled the processing of the payment. You will need to contact the retailer or supplier separately.*
>
> *14 e) We may ask you to provide information which is reasonably necessary to investigate whether or not you are entitled to the refund. In addition, you may also find it helpful to contact the person you paid using the Card. Within 10 working days of receiving your request (or of receiving further information we have*

asked for), we will either refund the payment or we will inform you of our reasons for refusing the refund.

23. *Finally, the Bank submits that it implements measures to ensure that its' 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 her actions which show gross negligence.*

Conclusion

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

25. *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.*

26. *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.*

27. *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.'

Seduti

Saru tliet seduti fil-15 ta' Lulju 2024,[17] 8 t'Ottubru[18] u d-29 t'Ottubru 2024.[19]

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

L-Ilmentatriċi twaħħal fil-BOV talli ħalla l-frodist jippenetra l-kanal tal-SMS u t-telefon li normalment juża l-Bank biex jikkomunika magħha u talli ma ndunax li l-pagament kien frodi.

Ġew ippreżentati żewġ *affidavits* ta' bint l-Ilmentatriċi[20] u ta' żewġha[21] li kienu preżenti waqt il-komunikazzjoni li l-Ilmentatriċi kellha mal-frodist u kkonfermaw dak li kienet xehdet l-Ilmentatriċi bla ma sarilhom kontroeżami mill-Bank.

Il-BOV tella' tixhed lil Shirley Scerri, *Manager* taċ-*Chargebacks Department* tal-BOV.

Shirley Scerri xehdet:

'***Ngħid li l-Ilmentatriċi awtorizzat tliet tranżazzjonijiet ta' €2,000 separatament. U dawn ġew awtentikati bl-użu tat-3D Secure App li hija installata fuq il-mobile tal-Ilmentatriċi. F'dan il-każ partikolari, l-Ilmentatriċi rċeviet Push Notification għal kull ammont fuq il-mobile tagħha. Imbagħad, hi awtorizzat billi aċċessat it-3D Secure App u awtorizzathom b'dak il-mod, jiġifieri, it-tranżazzjonijiet intużaw bl-iStrong Customer Authentication, bil-mobile tas-Sinjura u wkoll jew bil-Pass Code li hija biss taf jew inkella bil-fingerprint. Dawn huma l-modi kif jiġu awtorizzati.***

Nixtieq nagħmel referenza għal Dokument B (anness mar-risposta tal-bank, p. 41) li ġie ppreżentat. Dan id-dokument juri li t-3D Secure App kien enrolled fuq il-mobile tal-Ilmentatriċi mid-29 ta' Diċembru 2022 sat-18 ta' Marzu 2023. F'dan id-dokument ukoll jidher li anke hemm il-card il-ġdida wara din l-instance li qed tagħmel il-claim fuqha wkoll ġiet enrolled fuq it-3D Secure App fit-13 t'April, u dakinhar stess l-Ilmentatriċi awtorizzat €70.47 mal-Melita.

[17] P. 61- 63
[18] P. 69 - 72
[19] P. 73 - 76
[20] P. 65
[21] P. 66

Dan biex bażikament juri li l-Ilmentatriċi hija familjari ħafna ma' dan il-proċess u, apparti minn hekk, anke qabel ma seħħ dan il-każ, awtorizzat ukoll transactions bit-3D Secure App t'ammonti kbar ma' Revolut. Infatti għandha tnejn: wieħed fit-30 ta' Jannar u l-ieħor fis-26 ta' Frar. Dawn ġew awtorizzati bit-3D Secure Authentication bħal dawn it-tliet transactions li l-Ilmentatriċi qed tagħmel claim fuqhom.

Nixtieq ngħid ukoll li għal kull transaction li saret, l-Ilmentatriċi rċeviet il-BOV alerts kemm għat-tranżazzjonijiet tal-€2,000, għat-tranżazzjonijiet li għamlet qabel u kemm għat-tranżazzjonijiet li għamlet wara.

Ngħid li l-Push Notification li ser tirċievi fuq il-mobile tagħha tgħidilha li trid taċċessa it-3D Secure App biex tawtorizza dawn it-tranżazzjonijiet. It-tranżazzjonijiet u l-Push Notifications ser ikollhom l-ammont li ser tħallas u l-merchant. Once li ser tmur fid-3D Secure App, biex jiġu awtentikati, jiġu approved u t-tranżazzjoni tgħaddi, she needs to authenticate them, jiġifieri, għal kull waħda, daħlet fit-3D Secure App u awtentikathom. Però,kull waħda jkun hemm miktub min hu l-merchant u l-ammont. U f'dan il-każ, irċeviet tlieta u awtorizzat tlieta. Għalhekk għandha tliet SMSes mill-bank. Għandha wieħed 20:41; għandha ieħor 20:43 u għandha ieħor 20:45. Dan juri li żgur li ntbagħatu tliet Push Notifications u ġew awtorizzati tlett ammonti.

Nispjega li t-3D Secure App tintuża biex il-klijenti japprovaw tranżazzjonijiet online u normalment dawn ikunu ma' merchants li jkunu 3D Secure compliant. Wara li jaraw li hemm l-ammont u l-isem tal-merchant, huma jawtorizzawha u dak l-ammont jiġi pproċessat. Ngħid li l-uniku skop tat-3D Secure App hu biex tawtorizza tranżazzjoni. U, apparti minn hekk, hu qed jgħidlek eżatt lil min ser tħallas u b'kemm ser tħallas. Allura, ovvjament, jekk int qed tawtorizzaha, qed tagħti l-go ahead u l-flus imorru għand dak il-merchant.

Ngħid li l-Ilmentatriċi għandha availability fil-credit card tagħha ta' €6,000, jiġifieri, jekk hi għandha available €4,000, hi tista' tgħaddi €4,000.

Apparti minn hekk, l-Ilmentatriċi fil-15 iddepożitat €1,000, jiġifieri hi kellha bilanċ biex dawn it-tranżazzjonijiet jgħaddu. Ovvjament, kieku ma kellhiex dak l-ammont ma kinux ser jgħaddu. Ngħid li hi kellha €6,000 available f'dik il-card.

Biex nikkjarifika ngħid li hi għandha daily limit ta' €6,000 u ovvjament skont kemm għandha available jista' jgħaddi.'[22]

Waqt il-kontroeżami xehdet:

'***Qed jingħad li l-Ilmentatriċi fl-ebda mument ma awtorizzat xi pagament u qed niġi mistoqsija minn fejn irriżulta dan għaliex hi ma riditx tixtri xi ħaġa; dan xi ħadd ċemplilha mill-bank u qalilha li mblokkalha l-card tagħha. Mistoqsija wkoll lil min sar il-pagament, ngħid li, kif spjegajt, it-tranżazzjoni tiġi awtorizzata – la hija 3D Secure transaction, il-klijenta bilfors li rċeviet il-Push Notification.***

Ngħid li l-pagamenti saru lil Binance, però, l-klijenta meta awtorizzat it-tranżazzjonijiet bit-3D Secure App fuq il-mobile tagħha, kellha lil dan il-merchant jidher u kellha wkoll l-ammont. It-3D Secure transactions ma jistgħux jiġu awtorizzati b'mod ieħor.

Qed jingħad li hi ġiet infurmata in quick succession li saru tliet pagamenti ta' €2,000-il wieħed f'20:41, f'20:43 u f'20:45 – kull żewġ minuti l-bank qed jibgħatilha notification li sar pagament.

Ngħid li dak in-notification joħroġ wara li jsir il-pagament.

Qed jingħad li jsir pagament jekk ġie awtorizzat. Mistoqsija jekk wieħed ma jkunx awtorizzah, jista' xi ħadd jidħol fis-sistema tagħna u jagħmel din il-ħaġa, ngħid li mhuwiex il-każ. Mill-investigazzjonijiet rajna li s-Sinjura kienet ilha li kellha installata t-3D Secure App.

Fis-sistema għandna li s-Sinjura għamlet enrolment tat-3D Secure App fuq il-mobile tagħha fil-bidu nett. U hi meta għamlet hekk ukoll għażlet mod ta' kif ser tawtorizza kull pagament. Jew għażlet il-Pass Code jew għażlet il-fingerprint. Mela dik hija xi ħaġa li hija biss taf; il-bank ma jafx u ħadd ħliefha ma jaf.

Kull tranżazzjoni li ssir bit-3D Secure irid ikollok something that you own – the mobile which is yours – u xi ħaġa oħra biex tawtentika li inti biss taf. It-

[22] P. 70 - 71

tranżazzjonijiet tat-3D Secure jaħdmu b'dak il-mod u s-Sinjura RQ awtorizzathom b'dak il-mod.

Mistoqsija setax daħal xi ħadd ieħor u għamel din il-ħaġa, ngħid li le, ma jistax ikun.

Mistoqsija fit-transaction monitoring tal-bank ma jiġix iġġenerat alert li qed jiġu awtorizzati tliet pagamenti ta' €2,000-il wieħed fi ftit sekondi minn xulxin biex inkunu nistgħu inwaqqfuhom, ngħid li jekk huma 3D Secure transactions, hemm il-functionality li kemm il-merchant u kemm il-klijent jafu li qed isir dan il-pagament.

Dwar kif tiġi alerted it-transaction u jekk iċemplux lill-klijenti, naħseb jien at this point, aktar hemm lok li jagħtu l-input il-Fraud Monitoring Unit fuq dan il-każ partikolari.'[23]

Fl-aħħar seduta xehdet Sandra Stevens mill-*Fraud Section* tal-BOV. Mistoqsija jekk tliet pagamenti ta' €2,000 f'affari ta' ftit minuti favur *Binance* li ma kinux xi ħaġa solita għall-klijenta, kellux jibgħat xi sinjal lill-Bank biex iwaqqaf it-tranżazzjoni, Sandra Stevens qalet:

'***Minħabba l-awtentikazzjoni li kellhom it-tranżazzjonijiet, dawn jiġu kkunsidrati low risk u ma jiġux monitored b'dak il-mod***.'

Waqt il-kontroeżami xehdet:

'Mistoqsija dħaltx fid-dettalji ta' dan il-każ, ngħid li iva.

Mistoqsija x'irriżultali minn dan il-każ, ngħid li mill-investigazzjonijiet li saru, l-App kienet ilha installata mill-2022 u t-tranżazzjonijiet saru f'Marzu 2023. U kien hemm użu tagħha.

Ngħid li l-cards jistgħu jittellgħu ġo l-App darba biss, fuq one device only, jiġifieri jekk jiena għandi l-App bil-card tiegħi fuq il-mobile tiegħi, ħadd wara ma jista' jagħmel download tal-App u jerġa' jtella' l-card tiegħi fil-mobile tiegħu għax dik inħalluha darba biss.

Meta jien qed nagħmel tranżazzjoni bit-3D Secure, ser nirċievi notification jien għax l-App bil-card tiegħi qiegħda fuq il-mobile tiegħi. Mela jien ser nirċievi n-

[23] P. 71 - 72

notification ġol-App (mhux bħal SMS), jiġifieri nilloggja l-phone tiegħi bil-password tiegħi jew xi jkolli ssettjat, nidħol ġo l-App, nara n-notification li għandi confirmed purchase bil-merchant u bl-ammont u nikkonfermaha. Once li nikkonfermaha, hemmhekk qed nawtentikaha. Imbagħad, tibqa' għaddejja u tintbagħat l-SMS.

Mistoqsija qrajtx x'ġara u x'ma ġarax f'dan il-każ partikolari, x'inhi tgħid il-klijenta, ngħid li qrajt il-kummenti li qed jintqalu, però, s-sistema taħdem b'dan il-mod.

Qed niġi mistoqsija huwiex possibbli li xi ħadd daħal fis-sistema tagħna u għamel użu mis-sistema tagħna biex jibgħat din in-notification lill-klijenta tagħna illi, jekk hi ma tkellimx lill-Bank of Valletta, ser iwaqqfulha l-card u, allura, ma tkunx tista' tagħmel użu mill-card? U xi ħadd ser jeħdilha €1,500 mill-card?

Mistoqsija ivverifikajniex dan, ngħid li n-notification li kieku ma saritx il-confirmation tagħha kollox kien jieqaf hemmhekk. Ikollna klijenti fejn jirċievu n-notification, jgħidu 'Din mhux jien għamiltha,' u jieqfu hemmhekk u jirrapportawha xorta, jiġifieri, l-klijenta rat in-notification bl-isem u bl-ammont and she still confirmed it.

Qed jingħad li jiena ġejja mill-Fraud Section u qed niġi mistoqsija jekk hemm il-Fraud Section u xi ħadd qed jiġi ffrodat mill-klijenti tal-bank, il-bank x'sistema għandu.

Mistoqsija f'dan il-każ partikolari l-bank fejn il-klijenta tagħna ċemplet biex tistaqsi jekk huwiex mill-bank in-numru; il-bank qalilha li hu min-numru, emmnet b'bona fide, u qed jingħad li għalhekk xi ħadd daħal fis-sistema tal-klijenta tagħna biex kien jaf id-dettalji tal-klijenta tagħna biex għamel kuntatt magħha.

Qed niġi mistoqsija l-Fraud Section x'għandu xi jgħid fuq din.

Ngħid li ser nikkonferma x'sar bil-card. Bħala teknika hemm in-number spoofing, però, l-klijenta irċeviet u tat id-dettalji u rċeviet notification u kkonfermat il-payment. Jiġifieri mhux xi ħadd ieħor għamel dan kollu waħdu.

Ngħid li jiġifieri ħadd ma daħal fis-sistema tal-bank, ġol-App u kkonferma l-payments.'[24]

Billi l-avukat tal-Ilmentatriċi beda jsostni li xi ħadd kien bilfors daħal fis-sistema tal-Bank u awtorizza l-pagamenti għan-nom tal-klijenta, l-Arbitru ġibed l-attenzjoni għal dak li ppubblika fil-mudell, u li għandha ssir distinzjoni bejn li xi frodist jippenetra s-sistemi tal-Bank u jagħmel pagamenti a skapitu ta' xi klijent bla ma jkun jaf il-kredenzjali sigrieti tal-kont tal-klijent, u penetrazzjoni li ssir permezz ta' *smishing* li jippenetra l-kanal ta' komunikazzjoni u li l-Bank ma għandux mezz kif dan jista' jevitah.

L-Arbitru talab lill-partijiet jaqraw il-minuti tal-laqgħa li kellu fuq dan is-suġġett mal-*Malta Communications Authority* li fuqha l-Arbitru ma għandux kompetenza. (Ara nota aktar 'l isfel).

Sottomissjonijiet Finali

Fis-sottomissjonijiet finali tagħhom, il-partijiet sostnew l-argumenti li kienu diġà saru 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 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, ippubblika mudell dwar kif jaħseb għandha

[24] P. 74 - 75

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 bil-qawwa 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, 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 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 tal-*Facebook* tal-bank, b'daqshekk il-konsumatur jinsab infurmat. F'każijiet serji ta' frodi bħal dawn jeħtieġ li l-banek jużaw komunikazzjoni diretta mal-klijent permezz ta' SMS jew *email*. Dan l-aspett huwa wieħed mill-fatturi inklużi fil-mudell.

Min-naħa l-oħra, l-Arbitru jifhem li l-fatt li l-klijent jiżbalja billi jagħfas *link* li jkun ġie mwissi biex ma jagħfasx għax tista' tkun frawdolenti, b'daqshekk din ma tkunx awtomatikament taqa' fil-kategorija ta' negliġenza grossolana skont il-liġi.

Il-Qorti Ewropea tal-Ġustizzja (CJEU) fil-każ ta' *Wind Tre and Vodafone Italia*[25] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha anke konsumatur medju li jkun raġonevolment infurmat u attent. L-Arbitru jara ilmenti minn ilmentaturi li faċilment jaqgħu f'din il-kategorija.

Fuq kollox, il-PSD 2 tagħmilha ċara[26] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.* Għalhekk, il-banek jeħtieġ li jkollhom sistema

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

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. 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 (ġenwin) fit-12-il xahar ta' qabel. Dan jgħin ukoll biex tiġi ffurmata opinjoni jekk il-*monitoring* tal-pagamenti li l-bank huwa doveruż jagħmel (kif spjegat fil-mudell) huwiex effettiv.[27] [28]

Deċiżjoni

L-Arbitru jiddeċiedi skont kif provdut f'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:

[27] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS *supplement* ta' PSD 2 EU 2015/2366 Artikli 21(1) u 2(2)
[28] PSD 2 EU 2015/2366, Artiklu 68(2)

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	Perċentwal ta' ħtija tal-Ilmentatriċi
Ilmentatriċi li tkun wriet traskuraġni grossolona	0%	100%
Tnaqqis għax irċeviet il-messaġġ fuq *channel* normalment użat mill-Bank	50%	(50%)
Żieda għax l-Ilmentatriċi ikkoperat b'mod sħiħ biex sar il-pagament ilmentat	(30%)	30%
Żieda għax tkun irċeviet twissija diretta mill-Bank fl-aħħar 3/6 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	0%	0%
TOTAL FINALI	**40%**	**60%**

Għalhekk, skont il-mudell, l-Ilmentatriċi għandha ġġorr 60% tal-piż u l-40% l-oħra jġorrhom il-BOV.

Il-mudell isib li l-fatt li l-Ilmentatriċi baqgħet tikkopera mal-frodist billi rat l-ammont u l-isem tal-benefiċjarju (*Binance*) u xorta għal tliet darbiet ikkonfermat kull tranżazzjoni bi *3D Secure App,* iżid sew id-doża ta' *gross negligence* tal-Ilmentatriċi. Huwa ovvju li *3D Secure* qiegħda hemm biex tawtorizza pagamenti.

Lanqas jista' l-Arbitru jiskużaha għax ma għamlitx pagamenti oħra permezz ta' *3D Secure App* għax ma ċaħditx li fix-xahrejn ta' qabel kienet awtorizzat pagamenti b'dan il-mod.[29]

Iżda l-Arbitru jħoss li f'dan il-każ hemm ċirkostanza speċjali li timmerita li l-Ilmentatriċi tiġi parzjalment skużata għal 20% oħra għax mhux normali li frodist jippenetra fl-istess waqt kemm il-kanal tal-SMS u anke n-numru tat-telefon tal-Bank, u hekk iżid il-perżważjoni f'moħħ l-Ilmentatriċi li kienet verament qed titkellem mal-Bank.

B'kollox, għalhekk, qed tiġi intitolata għal kumpens ta' 40% tal-pagamenti frawdolenti li ġew debitati lill-kont tagħha.

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 systems* tiskatta biex jitwaqqfu l-pagamenti għax ma hemmx aspettattiva (s'issa) li dawn il-mekkaniżmi jaħdmu '*real time*' b'mod 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-Ilmentatriċi s-somma ta' elfejn u erba' mitt euro (€2,400).

Il-pagament irid isir fi żmien ħamest ijiem tax-xogħol mid-data tad-deċiżjoni. Altrimenti, l-imgħax bir-rata ta' 3.40% fis-sena[30] mid-data tad-deċiżjoni sad-data tal-ħlas effettiv.[31]

[29] P. 70

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

[31] 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.

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

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

<u>Nota ta' Informazzjoni relatata mad-Deċiżjoni tal-Arbitru</u>

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 wara li jiskadi l-perjodu tal-appell. Dettalji personali tal-ilmentatur/i jkunu anonimizzati skont l-artikolu 11(1)(f) tal-Att.