Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 011/2024

CI

('l-Ilmentatriċi')

vs

Bank of Valletta p.l.c.

(C-2833)

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

Seduta tal-31 ta' Lulju 2024

L-Arbitru,

Wara li ra l-Ilment li fis-sustanza tiegħu, jittratta r-rifjut tal-Provditur tas-Servizz li jirrimborża lill-Ilmentatriċi l-ammont ta' €567 rappreżentanti flus li ngibdu mill-kont tagħha mal-BOV mingħajr awtorizzazzjoni.

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

- Il-pagament ikun għal ammont ġeneralment taħt il-€5,000 biex ma jinżammx minħabba li jeċċedi d-*'daily limit'* ta' pagamenti li jkun maqbul bejn il-Bank u klijent tat-tip *'retail'.*
- Il-frodist jirnexxielu jippenetra b'mod frawdolenti il-mezz ta' komunikazzjoni normalment użat bejn il-Bank u l-klijent, ġeneralment permezz ta' SMS jew e-*mail*.
- 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-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 access 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 t'Ottubru 2023, l-Ilmentatriċi indunat li l-ġurnata ta' qabel kien sar pagament ta' €567, li ma kienx awtorizzat minnha, permezz tal-*internet banking* minn kont tagħha mal-Bank li ma kien abbinat ma' ebda (*debit* jew *credit) card* li kellha.

- L-Ilmentatriċi ssostni li ma kienet irċeviet ebda SMS li kien jitlobha tagħfas xi *link* u, għalhekk, hija tgħid li ma għafset ebda *link* frawdolenti.[1]

- Dan sar f'kont tal-bank tal-frodist fl-Irlanda (IE).[2]

[1] Paġna (p.) 47
[2] P. 3; 59

- B'mod qarrieqi, il-pagament kien jindika li l-benefiċjarju kien jismu Jordan mulligan u bħala dettalji tal-pagament indika *"Donation please enjoy xx".*[3] Indika l-indirizz tal-benefiċjarju bħala 143, Triq il-Pitkali, Attard ATD 7513, biex inaqqas xi suspett mis-sistema tal-BOV li tagħmel monitoring tal-pagamenti.[4]

- Il-pagament sar f'affari ta' ftit minuti fejn l-ewwel *login* sar fil-ħin ta' 10:44, ġie verifikat fil-ħin ta' 10:47 u *logout* sar fil-ħin ta' 10:53.[5]

- Il-BOV bagħat SMS[6] wara li sar il-pagament biex jinforma b'dan lill-Ilmentatriċi. Iżda l-Ilmentatriċi ma tatx kasha għax ħasbitha li kienet tirrelata ma' pagament simili li kienet għamlet ġurnata qabel.[7] [8]

- L-Ilmentatriċi kif indunat bil-pagament mhux awtorizzat ċemplet lill-BOV biex tirrapporta l-frodi iżda l-pagament diġà kien ġie proċessat.

- Sar *recall* mill-BOV iżda dan imblokka biss €139 li biex jiġu rritornati kienu jinvolvu spejjeż ta' €250 u, għalhekk, ma kienx ekonomiku li jsir dan ir-rimbors.[9]

- Il-każ ġie rrapportat lill-pulizija għal aktar investigazzjoni tal-frodi.[10]

L-Ilment[11]

Fl-Ilment tagħha, l-Ilmentatriċi qalet li ndunat bit-tranżazzjoni frawdolenti fuq *e-account* fil-25 t'Ottubru 2023, ġurnata wara li kien seħħ fl-24 t'Ottubru 2023.

Issottomettiet li dan il-kont m'għandu l-ebda *cards* abbinati miegħu.

L-Ilmentatriċi spjegat li minnufih ċemplet il-*customer care* tal-BOV u rreġistrat ilment dwar dan il-pagament. Issottomettiet li m'għandhiex ilment formali bil-

[3] P. 54
[4] P. 3
[5] P. 28
[6] P. 48
[7] *Ibid*.
[8] P. 62 li turi li fit-23 t'Ottubru sar pagament ta' €588.14 (?) lil *Paypal* minn kont ieħor li kellha mal-BOV.
[9] P. 69
[10] P. 10 - 11
[11] Formola tal-Ilment minn Paġna (P.) 1 - 6 b'dokumentazzjoni addizzjonali minn P. 7 - 15.

miktub għaliex il-proċess kollu seħħ fuq it-telefonata jew permezz ta' *email*. Issottomettiet ukoll li l-ħlas kien sar lil numru tal-IBAN barrani b'indirizz Malti ġewwa Ħ'Attard, u li din kienet tranżazzjoni bl-*internet banking* fl-ammont ta' €567 li għalih iridu jintużaw il-firem. Spjegat li dawn il-firem jinġiebu minn fuq il-*mobile app* fuq il-*mobile*.

L-Ilmentatriċi ssottomettiet li hi m'awtorizzat ebda tranżazzjoni, u lanqas ma għafset fuq xi *scams* jew SMS.

L-Ilmentatriċi issottomettiet li għamlet rapport mal-pulizija ġewwa l-għassa ta' Birkirkara u nbeda l-proċess biex il-flus jissejħu lura. Qalet ukoll li l-*internet banking* twaqqaf, il-*cards* twaqqfu, u oħrajn ġodda ħarġu skont kif ordna l-bank.

L-Ilmentatriċi qalet li wara diversi tfakkiriet u telefonati biex issegwi fuq l-ilment, hija rċeviet risposta xejn sodisfaċenti mingħand il-BOV permezz ta' *email* u telefonata. Issottomettiet li matul it-telefonata fis-27, hija reġgħet irrepetiet li ma kienet awtorizzat ebda tranżazzjoni u r-rappreżentant tal-BOV dehret maħsuda li dan kien il-każ u wiegħdet li tiftaħ il-każ mill-ġdid.

L-Ilmentatriċi spjegat li hija tħoss li l-BOV naqasha għax hija ġiet infurmata mir-rappreżentant tal-bank li

"*The foreign bank requested an indemnity of €139, however the charge to cover the indemnity is much higher than this amount. In this regard, the case is considered closed."*.

L-Ilmentatriċi issottomettiet li ġaladarba huwa fatt li hi m'awtorizzatx it-tranżazzjoni, ma taħsibx li huwa ġust li tibqa' mingħajr flusha. Qalet li jidher ċar li s-sistema tal-*internet banking* ġiet megħluba peress li ma setgħet issir ebda tranżazzjoni mingħajr ma hi tawtorizzaha permezz tal-firem tagħha minn fuq il-BOV *app* mill-*mobile* tagħha. Tenniet ukoll li hi ma kienet irċeviet ebda messaġġi jew *emails* li kienu *scam* li hija fetħet.

Rimedju mitlub

L-Ilmentatriċi qalet li trid flusha lura, *cioè*, l-ammont ta' €567, peress li din it-tranżazzjoni ma kinitx awtorizzata u hi ma għafset fuq ebda *link* u ma fetħet ebda messaġġ jew *email* frawdolenti.

Ikkunsidra wkoll, fl-intier tagħha, ir-risposta tal-Provditur tas-Servizz[12]

Fejn il-Provditur tas-Servizz spjega u ssottometta kif ġej:

1. *"Whereas Ms. CI ("the complainant") states that 'I noticed a fraudulent transaction on an e-account on the 25th October 2023". She states that "it was an Internet banking transaction, amount of €567, for which signatures need to be used. ... I did not authorise any transactions, nor click on any scams or SMS.'*

2. *Whereas the complainant attached the details of the transaction in question, bearing reference number 2329703038821000-1607958398. According to the Bank's records, this transaction was duly authorised on the 24th of October 2023 at 10:47. 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 her name. In fact, this transaction had no indication that it was 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 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 kn**owledge (something only***

[12] P. 22 - 27, b'annessi fuq p. 28 - 45.

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'.*

5. *Whereas apart from strong customer authentication, the Bank implements also 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;*

   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 the complainant was not only aware of the amount of the transaction, but also input it herself in her 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, she also inputted 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. The customer accesses this section from the section entitled 'Transaction Signing 'Signature 2' and then sees a section entitled 'Amount' and another entitled 'Payee Code'. This can be seen*

*from the document attached as **'DOC.B'** (which is easily accessible on the Bank's website). These phrases all clearly indicate that one is approving a transaction. Therefore, it is completely unfounded for the complainant to say that 'I did not authorise any transactions.'*

7. *Whereas this payment was approved by the confidential details of the complainant with the use of her 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 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. In fact, this is outlined in the terms and conditions of the Internet Banking system (attached and marked as **'DOC.C'**) 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."

   *"All payments, instructions, orders, applications, agreements, other declarations of intent and messages submitted by you through the Channels, after entering your BOV Securekey security number or numbers ("Security Number/s"), or input your BOV Mobile PIN ("Boy Mobile PIN"), or input your biometric data, are deemed as **binding** on you!"*

8. *Whereas in fact, every token used to generate codes 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 she has previously used to make other payments which she is not contesting the legitimacy of. This can be seen from the document attached and marked as **'DOC.D'**.*

9. *Therefore, it is completely unfounded for the complainant to refer to the Bank and say that "clearly their Internet banking system was breached since a transaction could be made without me authorizing it with*

signatures via the BOV app on my mobile." It is impossible that the transaction was made without her authorising it, since as shown in 'DOC.D' the token of Ms. CI was used and if she did not use it herself, then she left it in the hands of 3rd parties or generated the necessary codes herself and passed them on to third parties. Both these actions would breach the terms and conditions of internet banking service.

10. *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.E'*** *(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.*

11. *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. 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.*

12. *Whereas without prejudice to the above, if the complainant is alleging that this transaction was 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 a payment, she 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**.*

13. *Whereas article 50(1) of the Directive provides:*

*The payer shall bear all of the lasses 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**.*

14. *Whereas if the complainant is alleging that the transaction was not authorised by her, this means that she either left her token in the hands of third parties or 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, she had to insert the amount of the transaction and the last 5 digits of the recipients' IBAN. This fact should have raised suspicion within the complainant since if she had no intention of approving a payment, then it would have been reasonable for her to take action and ask why he was being asked to input an 'amount'.*

15. *The fact that she 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 BQV Mobile PIN, as applicable, from falling into the hands, or coming to the knowledge, of any third party."

Timeline of Events

16. *Whereas the payment was approved on the 24th of October 2023 at 10:47. This kind of payment is processed immediately as can be clearly seen in the terms and conditions marked as **'DOC.C'**, 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'.*

17. *Therefore, when the complainant called the Bank on the 25th of October 2023, the representative blocked the cards and internet banking of the complainant. The Bank also made a recall request to the beneficiary banks, which request is made through a digital, internal system between Banks.*

18. *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.*

19. *Whereas the beneficiary Bank informed BOV that it managed to recover the sum of €139, however, it requested an indemnity for the same amount, which along with Bank charges, would have amounted to a higher amount than that which would have been recovered.*

20. *Finally, the Bank submits that it implements measures to ensure that its internet banking systems are secure (in line with EU law). In fact, the Bank received legitimate instructions to process a payment which was*

authorised in line with the security measures stipulated in the PSD 2 and thus, it was obliged to process it accordingly.

Conclusion

21. *For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and law because as explained above, the transaction was approved through the credentials of the complainant and through her token.*

22. *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.*

23. *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.*

24. *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

Fl-ewwel seduta li nżammet fl 10 ta' Ġunju 2024, l-Ilmentatriċi sostniet dak li kienet diġà rrapportat fl-Ilment.

Fil-kontroeżami hija żiedet:

"***Ngħid li skont ma qaluli l-bank, din it-transaction ħarġet bħala bank transfer.***

Qed jingħad li fl-ilment tiegħi għidt li din it-transaction tista' ssir bis-Signatures u mistoqsija niftakarx li ktibt hekk, ngħid li tawtorizza ruħha bis-Signatures.

Ngħid li iva, ġieli għamilt pagamenti bis-Signatures. Naf li trid tuża l-App li tinsab fuq il-mobile, però, jiena dakinhar, f'dak il-ħin tat-transaction, ma awtorizzajt xejn.

Mistoqsija x'nagħmel meta nawtorizza pagamenti ta' dan it-tip fuq l-App, xi informazzjoni għandi ndaħħal, ngħid li trid iddaħħal l-account number; l-aħħar ħames numri tal-account ta' min ser jirċievi, min ser jibbenefika u l-ammont.

Mistoqsija x'jiġri imbagħad, ngħid li l-App jidhirli li tagħtik a six-digit number u inti ddaħħlu fis-sistema tal-Internet Banking li int tkun qed tuża.

Ngħid li, iva, jien familjari ma' kif tintuża din is-sistema.

Ngħid li le, fl-24 t'Ottubru jien ma mxejtx ma' dawn il-passi. Ngħid li ma għamilt xejn minn dawn.

Ngħid li le, ma tajtx id-dettalji tiegħi tal-Internet Banking lil xi ħadd.

Mistoqsija inix familjari mat-Terms and Conditions tal-Internet Banking, ngħid li għandi idea tagħhom.

Mistoqsija għamiltx follow-up tar-rapport tal-Pulizija, jekk tawnix informazzjoni ulterjuri, ngħid li le, ma tawnix informazzjoni.

Mistoqsijiet mill-Arbitru:

Ngħid li le, jien ma rċevejt l-ebda messaġġ li b'xi mod invitani biex nagħfas xi link. Ma rċevejt xejn.

Mistoqsija qattx irċevejt xi messaġġi mingħand il-Bank of Valletta, ngħid li iva, għandi l-function fuq l-Internet Banking li tirċievi meta jkun daħal xi credit jew pagament minn fuq il-cards.

L-Arbitru qed jitlobni sabiex nibgħat kopji ta' xi SMSes li rċevejt minn fuq xi channels li jidhru li ġejjin mill-Bank of Valletta matul ix-xahar t'Ottubru.

Ngħid li ma nistax nagħmel dan għax sadanittant tajtu factory reset il-mobile. U meta tlabt lis-service provider tiegħi biex inkun nista' nakkwista log tal-messages, qaluli li ma ssirx u, if anything, it has to be through an official channel, tipo, mill-Pulizija biex tinġabar data, avukati u affarijiet minn dawn.

Ngħid li għandi logs minn Ottubru (?) 'l hawn imma qabel le.

Mistoqsija niftakarx kontx irċevejt notifika mill-bank dwar dan il-pagament, ngħid li kont irċevejt notifika li onestament I did not acknowledge it għas-sempliċi raġuni li on Monday kont xtrajt xi ħaġa u ħsibtu hu. Imma, on Wednesday, l-għada li saret it-transaction, kont dħalt fl-Internet Banking biex nagħmel xi ħaġa li mhix relatata ma' din it-transaction u ndunajt li hemm ammont inqas milli suppost hemm f'dan it-tali account.

Ngħid li fl-24 t'Ottubru, meta sar dan il-pagament, ma kont irċevejt l-ebda SMS qabel. Ngħid li wara li saret it-transaction, irċevejt message li ħargu l-€567 minn ġo l-account imma l-ammont tant kien simili għat-transaction li saret Monday, 23, li onestament ħsibtu hu. Imbagħad, indunajt bit-transaction on Wednesday fejn hemm gie triggered il-proċess tal-Pulizija, tal-Customer Care, nagħlqu l-accounts u hekk.

Qed jingħad li meta għamilt it-transaction ta' qabel Monday, it-transaction ġenwina, mhux diġà kont irċevejt SMS biex jinfurmawni li saret din it-transaction, ngħid li ma nafx ngħidlek."[13]

It-tieni seduta nżammet fil-25 ta' Ġunju 2024, fejn tela' jixhed Michael Gatt, uffiċjal eżekuttiv fl-*Electronic Payments Section* tal-BOV li qal:

"***Ngħid li ili naħdem 30 sena mal-Bank of Valletta u 12-il sena minnhom fl-Electronic Payments Section.***

[13] P. 47 - 48

Ngħid li jiena rajtu l-ilment ta' CI.

Ngħid li din it-tranżazzjoni, bħal kwalunkwe tranżazzjoni li jkollu l-Bank of Valletta, biex tiġi awtorizzata hemm ċertu steps li wieħed irid jagħmel biex fl-aħħar tiġi awtorizzata.

Bażikament, inti tuża l-mobile tiegħek, tagħżel il-BOV Mobile App tiegħek, iddaħħal il-PIN. Once li ddaħħal il-PIN, tagħżel Transaction Signing, Signature 2, iddaħħal l-ammont, il-Payee Code u l-PIN u jiġi ġġenerat il-One-Time Password. Dan il-One-Time Password jiġi ġġenerat skont l-aħħar digits tal-IBAN li inti tkun daħħalt fix-Schedule tal-pagament. Iddaħħal il-One-Time Password u jiġi awtorizzat il-pagament. Mingħajr dawn l-isteps, il-pagament ma jistax jiġi awtorizzat.

Ngħid li skont il-logs li għandu l-Bank of Valletta, (Doc. D, fejn juri sample ta' pagamenti, paġna 43 tal-proċess), dawn l-isteps ġew magħmula kollha mill-ilmentatriċi. Dan jiġi kkonfermat minħabba li l-App għandu serial number li hu uniku u li huwa l-istess serial number li intuża fil-passat għal tranżazzjonijiet oħra.

Il-Login ID huwa s-6-digit number li jkun jafu biss il-user. Li jkollok il-Login ID biss inti ma tista' tagħmel xejn u għandek bżonn is-Signature 1 biex taċċessa l-internet banking tiegħek. Ma tista' tagħmel l-ebda tranżazzjoni ħlief tara l-bilanċi, jiġifieri bil-Login biss ma tista' tagħmel xejn, it-tranżazzjoni lanqas biss tibda.

Fl-aħħar seduta l-ilmentatriċi semmiet li ġurnata qabel kienet għamlet pagament b'ammont simili u, allura, meta rċeviet l-SMS tal-bank jgħidilha li għamlet pagament ma tatx każu. Ngħid mill-istatement li ħriġna ma kienx hemm pagament simili minn dan il-kont."[14]

Sottomissjonijiet finali

L-Ilmentatriċi bagħtet kopja ta' *statement*[15] ta' kont ieħor tagħha minn fejn ġurnata qabel il-pagament ilmentat kienet għamlet pagament għal ammont

[14] P. 49 - 50
[15] P. 62

viċin ta' dak ilmentat u, għalhekk, tgħid ma tatx kas l-SMS tal-Bank biex javżaha li sar il-pagament ilmentat nhar l-24 t'Ottubru 2023.

Fis-sottosmissjonijiet finali tagħhom, il-BOV saħqu li s-sistema tal-pagamenti tagħhom kienet konformi mar-regoli tal-PSD 2 u li l-pagament seta' jsir biss billi jiġi awtorizzat mill-Ilmentatriċi permezz tat-2 *factor authentication.* Għalhekk, biex sar il-pagament bilfors li kien hemm negliġenza grossolana *da parti* tagħha.

"Illi pagament bħal dan jiġi approvat permezz tal-istrong customer authentication in linea mal-Payment Services Directive 2 (PSD2). Din id-Direttiva titlob li biex ikun hemm strong customer authentication, irid ikun hemm il-preżenza ta' zewġ elementi (għaldaqstant tissejjaħ ukoll 2 factor authentication) minn tlieta li ssemmi d-Direttiva. Dawn huma in-'knowledge', li hija xi ħaġa li jaf il-klijent biss, il-'possession', xi ħaġa li għandu l-klijent biss u l-'inherence', xi ħaġa li huwa l-klijent.

Illi fil-każ tas-Sinjura CI, l-elementi tal-istrong customer authentication kienu preżenti għaliex il-pagament ġie approvat bit-'token' tagħha. Dan jidher mill-fatt li t-token serial uniku tat-token li intuża biex tiġi approvata t-tranżazzjoni in kwistjoni kien l-istess wieħed li ġieli użat is-Sinjura CI biex tagħmel tranżazzjonijiet oħra li m'humiex jiġu kkontestati. Dan jidher f'DOK.D anness mar-risposta tal-Bank u ġie spjegat ukoll mix-xhud tal-Bank waqt is-seduta ta' nhar il-25 ta' Ġunju 2024.

Għaldaqstant, huwa impossibli li s-Sinjura CI ma mexietx mal-passi meħtieġa biex jiġi approvat il-pagament kif qalet fis-seduta ta' nhar l-10 ta' Ġunju 2024.

Illi l-artiklu 40 tad-Direttiva Numru 1 tal-Bank Ċentrali ta' Malta (li hija bbażata fuq il-Payment Services Directive 2) tipprovdi li:

(1) 'A payment transaction is considered to ***be authorised*** *only if the payer has given* ***consent to execute*** *the payment transaction.*

(2) ***Consent to execute a payment transaction*** *or a series of payment transactions* ***shall be given in the form agreed between the payer and the payment service provider.*** *Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider.'*

F'dan il-każ, il-Bank kellu l-kunsens tas-Sinjura CI sabiex il-pagament, liema kunsens il-partijiet qablu dwaru fit-Terms and Conditions, kif ġia ġie spjegat fir-risposta tal-Bank.

Għaldaqstant, meta l-Bank irċieva struzzjonijiet leġittimi mingħand is-Sinjura CI fejn approvat pagament skont il-metodi elenkati fit-termini u kundizzjonijiet, il-Bank kien obbligat li jipproċessahom immedjatament."[16]

Żiedu wkoll:

"*Illi kif ġia spjegat, is-Sinjura CI mhux talli ma żammitx il-kredenzjali tagħha sabiex taċċessa l-internet banking sikuri, iżda oltre minn hekk, ipprovdiet id-dettalji neċessarji sabiex il-pagament jiġi approvat u kienet parteċipanta attiva f'dan il-proċess. Għaldaqstant, anke jekk ma kellhiex l-intenzjoni tagħmel pagament, hija uriet negliġenza grossolana għaliex injorat l-indikazzjonijiet li kellha sabiex tinduna li qiegħda tawtorizza pagament.*

Illi tul il-proċess, is-Sinjura CI kellha kliem bħal 'Transaction Signing', 'Amount', u 'Payee Code' quddiemha. Dawn huma kollha kliem li jindikaw li wieħed qiegħed fil-proċess li jagħmel pagament u għandhom irawmu dubju serju jekk persuna ma jkollhiex l-intenzjoni li tagħmel pagament, li jwassluh biex jaħseb għalfejn qiegħed idaħħal dettalji f'sections b'dawn l-ismijiet. Dan huwa kliem ċarissimu u huwa intenzjonat sabiex kwalunkwe konsumatur jifhem xi jkun qed jagħmel. Il-fatt li s-Sinjura Mallia Azzopadi injorat dawn il-kliem jikkontribwixxi b'mod serju għan-negliġenza grossolana li uriet dakinhar tal-inċident. Għaldaqstant, hemm bżonn attenzjoni adegwata min-naħa tal-klijent, li kull wieħed għandu juża meta qiegħed juża flusu, għaliex kif il-Bank għandu l-obbligu jissalvagwardja lill-klijenti, il-klijenti għandhom ukoll responsabbiltajiet min-naħa tagħhom meta jiġu biex jużaw servizz li abbonaw għalih b'mod volontarju. Oltre minn hekk kien fl-interess u d-dmir tagħha li tifhem kif jaħdem u x'inhi tagħmel b'dan is-servizz."[17]

[16] P. 68
[17] P. 70 - 71

Analiżi u konsiderazzjoni

L-Arbitru għandu quddiemu żewġ verżjonijiet kuntrastanti dwar kif ġie awtorizzat dan il-pagament.

L-Ilmentatriċi ssostni li hi la rċeviet messaġġi frawdolenti biex tagħfas xi *link* u wisq anqas għafset xi *link* li permezz tagħha kixfet il-kredenzjali sigrieti li jagħtu aċċess għall-kont tagħha lil terzi.

Min-naħa l-oħra, l-Bank spjega kif dan il-pagament ġie awtorizzat permezz tat-*token* li jispiċċa b'*serial number* … 96310, li huwa *token* fil-pussess tal-Ilmentatriċi li permezz tiegħu kienet għamlet pagamenti ġenwini.[18]

Għalhekk, il-Bank ressaq prova li kienet l-Ilmentatriċi li kellha fil-pussess tagħha dan it-*token* li bih għamlet jew għenet lill-frodist biex jagħmel dan il-pagament skont it-*two factor authentication* stipulat fir-regolamenti tal-pagamenti bankarji.

L-Ilmentatriċi ma għenitx il-każ tagħha meta qalet li ma setgħetx tippreżenta evidenza tal-SMS li kienet tirċievi mill-BOV fiż-żmien li sar dan il-pagament għax skont hi:

"ma nistax nagħmel dan għax sadanittant tajtu factory reset il-mobile."[19]

Fuq bażi t'evidenza pprovduta, l-Arbitru huwa tal-fehma li pagament seta' jsir biss jekk l-Ilmentatriċi jew approvat hi stess minn jeddha dan il-pagament, jew aktar probabbli, hija għafset xi *link* qarrieqa li permezz tagħha tat aċċess lill-frodist għall-kont tagħha, u wara baqgħet b'xi mod tikkopera biex il-pagament jiġi speċifikament approvat minn sistemi li hija stess ammettiet li kienet familjari magħhom.[20]

L-asserzjoni tagħha li ma għafsitx il-*link* u ma awtorizzatx il-pagament trid tiġi kkonfrontata mal-prova dokumentata tal-BOV li l-pagament seta' jsir biss għax intużat it-*token* fil-pussess tal-Ilmentatriċi. Dan jitfa' l-bilanċ ta' probabbilità ixaqleb sew fuq in-naħa tal-Bank.

[18] P. 43
[19] P. 47
[20] *Ibid*.

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 jistghu 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 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*[21] tagħmel referenza li ma tkunx negliġenza fi grad grossolan jekk jaqa' għaliha

[21] Deċiżjoni 13 ta' Settembru 2018 C-54/17

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[22] li l-konsumatur irid jagħti l-kunsens tiegħu biex isir il-pagament speċifiku u mhux biżżejjed kunsens ġenerali li jkun kontenut f'xi *Terms of Business Agreement.*

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

Il-mudell jagħti wkoll konsiderazzjoni għal xi ċirkostanzi partikolari tal-każ. Jista' jkun hemm ċirkostanzi partikolari fejn il-messaġġ tal-frodist ikun anqas suspettuż. 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.[23] [24]

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.

[22] *Article 64 of PSD 2*
[23] (EU) 2018/389 tas-27 ta' Novembru 2019 RTS *supplement* ta' PSD2 EU 2015/2366 Artikli 2(1) u 2(2)
[24] PSD 2 EU 2015/2366 Artiklu 68(2).

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

	Perċentwal ta' ħtija tal-Provditur tas-Servizz	Perċentwal ta' ħtija tal-Ilmentatur
Ilmentatur li jkun wera traskuraġni grossolona	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-Ilmentatriċi għandha ġġorr 80% tal-piż u l-20% l-oħra iġorrhom il-BOV.

Il-mudell isib li l-fatt li l-Ilmentatriċi bilfors li baqgħet tikkopera mal-frodist billi mliet l-ammont u l-aħħar 5 ċifri fis-*Signatures* tal-*App* u anke daħħlet is-6-*digit code* li tagħti l-aħħar awtorizzazzjoni biex isir il-pagament, iżid id-doża ta' negliġenza tal-Ilmentatriċi.

Il-mudell isib lill-Bank responsabbli jġorr 20% tat-telf għax kien naqas milli jinforma b'mod dirett lill-Ilmentatriċi fl-aħħar 3 xhur qabel ma ġara l-każ, biex toqgħod attenta li ma tagħfasx fuq *links* inklużi f'xi SMS li tista' tidher li tkun ġejja mill-Bank għax dan ikun *scam* peress li l-Bank qatt ma jibgħat *links* permezz ta' SMS.

Lanqas jista' l-Arbitru jiskuża lill-Ilmentatriċi għax ma għamlitx pagamenti *online* simili għax hi stess ammettiet li kienet midħla ta' kif isiru dawn il-pagamenti *online* bl-*internet*. L-Arbitru lanqas sab xi ċirkostanzi speċjali li jiskużaw lill-Ilmentatriċi f'dan il-każ.

B'kollox, għalhekk, l-Arbitru qed jordna kumpens ta' 20% tal-pagament frawdolenti li ġie debitat lill-kont tagħha.

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' mija u tlettax-il ewro punt erbgħa zero (€113.40).

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.

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.