Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 095/2026

CB

('l-Ilmentatriċi')

vs

BNF Bank p.l.c.

(C 41030)

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

Seduta 06 ta' Novembru 2026

L-Arbitru,

Ra l-Ilment[1] datat 20 ta' Marzu 2026 magħmul kontra l-BNF dwar ir-rifjut li jirrifondi pagament ta' €11,712.34 li sar mill-kont tagħha nhar is-26 ta' Jannar 2026, li hija ssostni li sar mingħajr l-awtorizzazzjoni tagħha lil persuna barranija li hi qatt ma kienet tafu. Sostniet li hija infurmat lil BNF f'inqas minn sagħtejn minn x'ħin sar il-pagament imma l-Bank ma żammx il-pagament.

Sostniet li fl-istess tranżazzjoni frawdolenti hija għamlet pagament mill-kont tagħha ma' BNF għal kont tagħha ma' Revolut ta' €11,000 imma dawn ġew irkuprati fil-pront. Kien hemmhekk li ndunat li kien diġà sar il-pagament ilmentat. Kienet ukoll għamlet pagamenti oħra ta' €550 għal kont tagħha ma' WISE u €5,000 għal kont tagħha ma' ACE iżda dawn ġew irkuprati. Iżda pagament ta' madwar €1,700 li għamlet mill-*crypto wallet* tagħha sparixxa wkoll. Iżda dan ma jiffurmax parti minn dan l-ilment.

Hija kompliet tilmenta li:

[1] Paġni (P.) 1 - 8 b'dokumentazzjoni addizzjonali minn P. 9 - 38.

"The bank let me down because whenever I used to do bank transfer it always took some time (days) to be successful and since I reported the scam in less than 2 hours when it happened why did the bank did not stop the payment ? The day after I went to the file the complaint in person at Attard branch and the bank manager was not helpful at all. She said that there were other clients who had the same issue. BNF Attard manager I was chasing her frequently for any updates but she found always excuses that she was busy and kept ignoring my emails without getting some assurance that they were doing something. I also requested her copy of my bank statements since my online account was closed due to this scam and she never provided them and had to go in person at Mosta Branch.

I discussed the matter with other local banks and they confirmed that the bank should have asked me before processing the payment since the transfer was over EUR5K since my account is personal and not a business account. Also I questioned how come the scammer managed to bypass the banking system since I did not give him access and they did not say anything about. Also why the bank did not asked about the transfer since it was to a foreigner person? Usually they ask for supportive documents even for a small amount."[2]

Bħala rimedju qed titlob rimborż tal-pagament ta' €11,712.34 u spjegazzjoni kif u għala sar dan il-pagament.

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

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

[2] P. 4

- 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[3] maħruġa mill-banek u mir-Regolatur biex ma jagħfsux *links* għax il-bank ma jibgħatx *links* fil-messaġġi tiegħu, u li l-klijent għandu jikkomunika mal-bank biss tramite l-App u/jew il-*website* uffiċjali u dan permezz tal-kredenzjali li l-bank ikun ta lill-klijent, il-klijent b'nuqqas ta' attenzjoni jagħfas il-*link*.

- Minn hemm 'il quddiem, il-frodist b'xi mod jirnexxielu jippenetra l-kont tal-klijent u jagħmel trasferiment ta' flus ġeneralment fuq bażi '*same day*' li jmorru fil-kont tal-frodist, ġeneralment, f'kont bankarju f'pajjiż barrani minn fejn huwa kważi impossibbli li jsir *recall* effettiv tal-flus ġaladarba l-klijent jirrapporta lill-bank tiegħu li ġie ffrodat. Ħafna drabi, il-frodist ikun pront jiġbed jew jittrasferixxi l-flus appena jaslu fil-kont indikat.

- B'riżultat, jinħoloq nuqqas ta' ftehim bejn il-bank u l-klijent dwar min hu responsabbli jġorr il-piż tal-pagament frawdolenti. Il-klijent isostni li l-bank ma pproteġihx meta ħalla kanal ta' komunikazzjoni li normalment jintuża bejn il-bank u l-klijent jiġi ppenetrat mill-frodist, u li l-bank messu nduna li kien pagament frawdolenti għax, ġeneralment, il-klijent ma jkollux storja ta' pagamenti bħal dawn. Il-bank isostni li l-ħtija hija kollha tal-klijent għaliex permezz ta' traskuraġni grossolana (*gross negligence*), ikun ta aċċess tal-kredenzjali sigrieti tal-kont tiegħu lill-frodist u b'hekk iffaċilita l-frodi.

F'dan il-każ partikolari, dawn huma d-dettalji rilevanti:

- Fis-26 ta' Jannar 2026, għall-ħabta tal-10.45, irċeviet telefonati fuq WhatsApp minn numru +1(226)902-6614 u telefonati diretti minn numru +34632406454 minn persuni li ppreżentaw ruħhom bħala rappreżentanti ta' Revolut li riedu verifika tal-I.D. tagħha.

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

- Waqt it-telefonata fuq WhatsApp, l-Ilmentatriċi għamlet *'screen sharing'* sabiex il-persuna l-oħra jkollha aċċess għall-mowbajl tagħha u bdiet tagħtiha struzzjonijiet sabiex tidħol fil-kont tagħha ta' Revolut.

- Hija ċaħdet li waqt id-diskursata hija daħlet fl-App ta' BNF iżda xorta sar pagament ta' €11,712.34 lil xi ħadd Hassan Raza li hija ma tafux u qatt ma approvat dan il-pagament.

- Skont ir-risposta tal-Bank, dan il-pagament sar fil-ħin tat-13:32, u bejn il-ħinijiet tat-13:00 u l-14:30 kemm l-Ilmentatriċi kif ukoll il-frodist daħlu diversi drabi fil-kont onlajn biex jaraw it-tranżazzjonijiet[4].

- Xi siegħa wara li sar il-pagament ilmentat sar l-ewwel kuntatt bit-telefon ma' BNF minn persuna li kienet qiegħda mal-Ilmentatriċi biex tistaqsi jekk kienx hemm problemi ma' Revolut u biex jitwaqqaf il-pagament. Din it-telefonata damet 6:16 minuti u matulha ġie rrappurtat li l-Ilmentatriċi kienet ilha erba' sigħat fuq il-linja mas-suppost rappreżentant ta' Revolut. Fir-reġistrazzjoni tat-telefonata jinstema' l-frodist jirrabja mal-Ilmentatriċi talli qed titkellem ma' terzi.

- Saret talba biex jitwaqqaf il-pagament li kien diġà sar. Ir-rappreżentanta ta' BNF widdbet li mill-mod li kien jinstema' jkellimha l-persuna fuq in-naħa l-oħra fuq it-telefonata tal-*WhatsApp* kien ċar li kienet qed titkellem ma' frodist. Dan kien qabel ma seta' jsir il-proċess ta' identifikazzjoni tal-klijenta mill-BNF u għalhekk ma ġiex imblokkat il-kont.

- Ir-rappreżentanta tal-Bank issuġġeriet kuntatt immedjat ma' *Cyber Crime* tal-pulizija.

- Wara kien hemm diversi telefonati bejn il-Bank u l-Ilmentatriċi fejn sar proċess ta' identifikazzjoni u imblokkar tal-kont.

- Sar rapport lill-Pulizija dakinhar stess fil-ħin tal-16:04[5] li ġie aġġornat l-għada fil-ħin tad-19:55.

[4] P. 42
[5] P. 14 - 15

Għalhekk dan il-każ ivarja minn każi oħra ta' pagamenti frawdolenti għax la kien hemm SMS bil-*link* fuq il-kanal li normalment jikkomunika fuqu l-Bank, la kien hemm *links* x'tagħfas u lanqas kien hemm xi ħadd li kien qed jippersonifika lil BNF.

Risposta tal-Fornitur tas-Servizz

Fir-risposta[6] tagħhom datata 10 t'April 2026, il-BNF qalu:

> *"The transaction of €11,712.34 (hereinafter referred to as the "Transaction"), which the customer claims to be unauthorised has been investigated by the Bank.*
>
> *1. Timestamped sequence of events (as identified by the Bank)*
>
> *According to the Customer and their filed police report, on 26th January the customer received a phone call from the number +346 32406454, claiming to be from Revolut. During the phone call the third-party stated that the phone call was being carried out to verify her identity card under the pretext that her Revolut account was going to be suspended because her identity card had expired. According to the Customer, the person claiming to be from Revolut stated that to verify the Customer they would need to contact her on WhatsApp. Subsequently, the Customer received various phone calls on her WhatsApp from the number +1(226)902-6614. It is understood by the Customer, that she answered the phone call and during the phone call, the Customer was asked by the third party to carry out screen sharing with the third-party which allowed the third party to access the Customer's mobile phone. Subsequently, the third-party transferred €11,712.34 from the customer's BNF account to a third-party account.*
>
> *Between the hours of 13:00 and 14:30, the customer logged into her account and viewed her transactions. The third party also subsequently logged into the customer's account and viewed her transactions. Both the customer and the third party logged into the*

[6] P. 42 - 45

account and viewed the account and its transactions on multiple occasions.

At 13:32hr, the third-party carried out a one-time international bank transfer of €11,712.34.

Both the third-party and the Customer carried out further login attempts and viewed the customers transactions.

The third-party then added an international transfer recipient and beneficiary in the BNF account.

The Customer logged in and downloaded the log of the transaction in question amounting to €11,712.34.

Subsequently, the third party and the Customer carried out a series of logins and viewed transactions.

One hour after the transaction was carried out, the Customer phoned the Bank to inform the Bank that she had been the victim of a scam and that a sum of €11,712.34 was withdrawn from her account. During the call, the Customer requested that the payment is stopped. The customer's Internet Banking was suspended immediately.

The Customer informed the Bank on the 27th January that a police report had been filed. The Customer filed a police report pertaining to the above-mentioned incident.

On the same day, the Customer visited the Attard Branch to request a change of account number for all her accounts and to provide the police report to the Branch Manager.

On 28th January the Customer sent an email to the Branch querying whether the Bank will be able to retrieve the funds. The Branch informed the Customer that the Bank initiated a request to request a refund of the money however they were still awaiting the receiving bank's reply. The Customer sent an email to the Branch requesting them to keep her updated.

Between the 2nd February to 5th February, the Customer sent an email to the Branch requesting an update regarding the recall request. The Branch informed the Customer that they had not received a reply to the request. The Branch informed the Customer that a chaser was sent to the receiving Bank.

On 20th February, feedback from the recipient bank was provided, indicating that the beneficiary account did not have adequate funds to return the payment and that the sender should deal directly with the beneficiary to return the funds. This was notified to the Customer by means of a formal resolution letter.

On 2nd March, a resolution letter was sent to the Customer where it was indicated that a meeting was held with the Branch representative to close the account to ensure that the Customer is safeguarded from any potential fraudulent attempts. It was acknowledged that the police report was submitted to the Payments Department along with the recall request of the transaction deducted. It was also stated that although a recall of the transaction was carried out by the Payments Department, this was unsuccessful since the beneficiary did not hold sufficient funds in the account requested.

2. Use of banking credentials

Under Article 45(2) of the CBM Directive no.1 in terms of the Central Bank of Malta Act – The provision and use of payment services ("hereinafter referred to as the Directive"), the payment service user "shall in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.". By allowing the third-party access to her mobile due to the screen sharing, which is the payment instrument, the Customer was not taking all the reasonable steps to protect the payment instrument which are expected under this Article. This act of screen sharing and allowing of access allowed the third-party to view the six-digit secure code which is required as part of the Bank's two factor authentication process, to access internet banking and/or the

mobile app, allowing the user to access the Customer's full internet banking profile.

It is evident from the above-mentioned details that the third-party used the security credentials which were inputted by the Customer because the third-party carried out a login attempt five minutes after the Customer carried out the login attempt.

4[7]. Scam alerts

From time to time the Bank posts scam alerts on its social media platforms in raising awareness to the public regarding ongoing scams and may also communicate with its customers using other means, such as SMSs and banners on the Bank's website. The Bank placed social media posts on 23rd January 2025, 19th August 2025 and 1st November 2025.

On 3rd November 2025, 12th November 2025 and 23rd January 2026 the Bank sent out a direct SMS to all customers, informing them to exercise caution.

<u>Conclusion</u>

By allowing the third-party to access her mobile, it is evident that the Customer did not take all reasonable steps to keep the payment instrument safe. The third-party was able to use the Customer's personal security credentials when she inputted them to carry out the login allowing the third-party to access and use the internet banking profile.

Notwithstanding the above, following being informed by the Customer, the Bank immediately suspended the Customer's Internet banking to safeguard the Customer from any potential fraudulent attempts in the future and her personal security credentials were also reset.

The Bank exercised its maximum effort in assisting the Customer by commencing the process to recall the transaction, following the

[7] The reply of BNF does not contain point 3.

notification received from the Customer regarding the circumstances under which the Transaction took place. Despite the Bank's efforts in assisting the Customer, the recipient bank declined the recall request due to insufficient funds in the beneficiary's account."

Seduti

Fl-ewwel seduta tal-15 ta' Ġunju 2026[8], l-Ilmentatriċi spjegat li emmnet li kien kuntatt ġenwin minn Revolut għax kienet irċeviet avviż biex taġġorna l-I.D. *card.* Ċaħdet li qatt tathom id-dettalji u l-kodiċi tal-kont ta' BNF iżda ammettiet li kienet għamlet *screen sharing* fejn huma bdew jaraw x'inhi tagħmel. Iżda qalet li meta daħlet fil-kont ta' BNF sabet li l-pagament ilmentat kien diġà sar. U għalhekk staqsiet kif dan seta' jsir meta hi ma tatx kodiċi lill-*hackers*.

Qalet li hi ma kinitx taf bl-introduzzjoni tas-sistema *Instant Payments*. Iżda qalet li f'Settembru 2025 meta riedet tgħaddi pagamenti dwar konvenju il-1% taxxa ta' €3,500 u dak tal-10% depożitu ta' €35,000 kellha tmur fiżikament il-*branch* biex isiru għax ma kinitx taf x'kien il-limitu tal-pagamenti marbut mal-kont tagħha.

Waqt kontroeżami, l-Ilmentatriċi xehdet:

"Nikkonferma li meta għamilt l-iscreen sharing dħalt fl-app tal-BNF.

Mistoqsija naqbilx li waqt l-iscreen sharing, il-hacker rani ndaħħal il-Username u l-PIN, ngħid li le, ma jiġux jidhru il-Username u l-password. Ma jiġux jidhru fuq il-mobile meta tagħmilhom. Dawk invisible kienu.

Mistoqsija jekk il-keyboard tal-mobile tiġix tidher fuq l-iscreen jew għandi xi mobile li l-keyboard hija parti mid-device, ngħid li ma tiġix tidher, le.

Ngħid li l-mobile li għandi normali, però, meta nagħmel screen sharing fuq il-mobile, ma tidhirx il-keyboard fuq l-iscreen.

[8] P. 46 – 51

Mistoqsija kif bdejt indaħħal l-affarijiet, ngħid li mill-mobile tiegħi, qisni qed nuża l-laptop. Meta inti tuża l-laptop ma tarahiex il-keyboard. L-istess ħaġa fuq il-mobile, ma tkunx qed tidher il-keyboard.

Mistoqsija x'mobile għandi, ngħid li .... għandi.

Mitluba biex nuri l-mobile fuq l-iscreen u jien qed nuri l-mobile tiegħi fuq l-iscreen.

Mistoqsija naqblux li l-keyboard tiġi tidher fuq l-iscreen tal-mobile, ngħid li iva, imma meta għamilt screen sharing ma kinux qed jidhru l-ittri u n-numri. Ma kien jidher xejn.

Qed jingħad li l-keyboard kienet tidher. Ngħid li, le, ma kinux qed jidhru. Ngħid li meta bdejt nittajpja ma bdewx jidhru. Ngħid li l-keyboard ma kinitx qed tidher.

Mistoqsija kif kont qed indaħħal il-PINs jekk ma kinitx qed tidher il-keyboard, ngħid li ma bdietx tiġi fix-sharing żgur.

L-Arbitru jixtieq jiċċara dan li ġej:

- ***Jidher li t-telefonata bdiet fil-10.45 a.m.***
- ***Il-pagamenti saru fis-1.30 p.m.***
- ***Fir-rapport tal-Pulizija, l-Ilmentatriċi tgħid illi l-komunikazzjoni mal-frodisti spiċċat fl-4.00 p.m.***

Mistoqsija mill-Arbitru jekk jien domtx mill-10.45 a.m. sal-4.00 p.m. ma' dawn il-frodisti, ngħid li, iva, kien hemm ħin twil. Bqajt niġġieled magħhom biex nara x'kien qed jiġri. Ġibt ħabiba tiegħi id-dar biex inċemplu lil BNF dak il-ħin. Il-Call Centre kien hemm xi ħadd, Roberta. Qaltli biex nibqa' magħhom.

Ngħid li l-ewwel ċempilna l-bank imbagħad mort l-Għassa. Il-bank mort l-għada għax dak il-ħin ikun magħluq.

Ngħid li l-pagamenti saru fis-1.30 p.m. u sas-2.00/2.15 p.m, kont ċempilt il-bank għax ġiet ħabiba tiegħi u ċempilna minn fuq il-

mobile tagħha. It-telefonata mal-BNF damet ftit; ma kinitx ta' żewġ minuti."[9]

L-Arbitru talab kopja ta' kull SMS li kienet qed tirċievi mill-BNF waqt li kienet qed tkellem lill-frodist u kopja tal-i*statement* tal-kont tagħha għal tnax-il xahar qabel il-pagament ilmentat.

Skont il-kopji tal-SMS li forniet l-Ilmentatriċi jidher li fil-ħin tal-11:10, il-BNF kien diġà bagħat notifika b'kodiċi biex isiru pagamenti ta' AED 24008.40 u AED 108.40[10].

L-Ilmentatriċi spjegat fis-seduta ta' wara li hi ma kinitx indunat b'dawn il-messaġġi qabel ma l-Arbitru talabha tibgħat kopja. Ġie kkonfermat li dawn il-pagamenti ma sarux. Iżda la dawn il-kodiċi ħarġu minn BNF huwa ċar li sal-ħin tal-11:10:51[11] diġà kien hemm aċċess mill-frodist għall-kont tal-Ilmentatriċi ma' BNF biex jinstiga li joħroġ il-kodiċi biex isiru dawn il-pagamenti.

Skont l-i*statements* li ġew forniti jidher li kellha kont bl-IBAN jispiċċa ...00102 fejn kienet tirċievi salarju mensili ta' aktar minn €6,000 u sar pagament minnu ta' €40,000 fl-04.03.2025. Kellha kont ieħor b'numru jispiċċa ...9617 minn fejn sar il-pagament ilmentat li fih bdiet tirċievi s-salarju minn April 2025 u li minnu kienu jsiru pagamenti onlajn regolari inkluż il-pagament 1% lin-nutar għal €3,500 li sar fit-03.09.2025 u li l-Ilmentatriċi ammettiet li għamlitu hi onlajn[12]. Iżda m'hemmx traċċa tal-pagament tal-10% għal €35,000 li jidher li sar minn xi kont ieħor li kellha ma' BNF u li biex sar kellha tmur fiżikament fil-fergħa ta' BNF.

Minn dan il-kont saru kemm il-pagament ilmentat kif ukoll il-pagament ta' €11,000 lejn Revolut li saru fl-istess ġurnata li juri li l-limitu tal-pagamenti tal-kont kien jeċċedi €22,500[13].

Saret seduta oħra fid-9 ta' Settembru 2026 fejn xehed għal BNF Nathan Gatt li jmexxi d-dipartiment ta' *IT Security & Governance.* Huwa xehed:

[9] P. 50 - 51
[10] P. 56. AED huma flus Dirhams tal-Emirati Għarab.
[11] P. 56 turi li t-talba għal pagament saret fil-ħin tal-10:10:51 (ekwivalenti għall-ħin lokali 11:10:51) u SMS bil-kodiċi wasal għand l-Ilmentatriċi fil-ħin tal-11:10.
[12] P. 72
[13] P. 66

"Ngħid li l-log li bgħattilkom ovvjament fih timestamp tal-azzjonijiet kollha li saru. L-Arbitru jinnota li l-log jibda minn diversi jiem qabel. Ngħid li dan biex nispjega xi ħaġa partikolari.

L-Arbitru jgħid li fis-26 ta' Jannar, id-data li ġara dan il-każ, jidher li kien hemm l-ewwel log-in irreġistrat li sar fis-13:06. Ngħid li hemm tliet linji partikolari, dawn huma log-ins ġejjin minn device li kien diġà rreġistrat fuq l-account tal-persuna. Ir-raġuni li nkludejt tat-22 hija għax turi l-istess device ID li hija kolonna minnhom li hemm fid-dokument. Jiġifieri dak id-device kien hemm log-in minnu fis-13:06.

Meta jsir log-in minn device ħa taraw tliet linji: log-in, registered device, u account action, jiġifieri id-device daħal fl-E-BNF. Dawk huma azzjonijiet kif tirrekordjahom is-sistema.

Fis-13:11 imbagħad naraw log-in li sar mill-web. Hawnhekk tajjeb li nispjega li meta għandek log-in fuq web, għandek żewġ metodi kif inti tista' tillogja: jew iddaħħal username, password, u tirċievi OTP by SMS, jew username u secure code li jista' jkun iġġenerat biss minn fuq app li diġà attivata. Jiġifieri mhux xi ħadd ħa jaqbad jinstalla l-app fuq mobile ieħor u jiġġenera kodiċi. Dak il-kodiċi jista' jiġi biss iġġenerat minn app li tkun diġà attivata. F'dan il-każ, kien hemm app li diġà attivata li hija l-istess app li qed naraw fis-13:06 u nafu li l-log-in ma sarx by password u OTP għax anke SMSs ma ħarġux infatti. Jiġifieri l-log-in li sar fis-13:11, li hemmhekk qiegħed immarkat qed taraw żewġ linji: 13:11, log-in, u account action, il-log-in hemmhekk sar permezz ta' code, secure code li ġiet mill-app li kienet diġà attivata.

Naraw imbagħad sensiela ta' azzjonijiet. Jiġifieri fis-13:20 nerġgħu naraw log-in li sar mill-app tal-klijenta, u mbagħad fis-13:21 nerġgħu naraw attività minn fuq il-web. Jiġifieri nerġgħu naraw log-in, account action, account action. Dawn il-log-ins kollha li qed naraw mill-web huma permezz ta' secure codes. Jiġifieri vverifikajna li SMSs u SMS OTPs biex isir log-in ma ħarġux għal dawn il-log-ins. L-uniku mod kif tidħol huwa li għandek xi

ħaġa li qed tiġi ġġenerata minn ġo app. Ovvjament dak li jkun idaħħal il-username u s-secure code biex jillogja mbagħad fuq il-web.

Is-sekwenza mbagħad tkompli hekk, jiġifieri l-kolonna 'Device Model' u 'Device ID' jagħtu indikazzjoni ta' liema device kien qed jintuża. Naraw li hemm alternating pattern ta' daqqa jintuża device, dak li jibda 23090 dak huwa device li kien diġà attivat taħt id-device model, u mbagħad naraw Chrome 14 li hija s-sezzjoni tal-web.

Hemm kolonna oħra 'Platform' li tindika jekk hux minn fuq l-app jew minn fuq il-web.

Mistoqsi fuq dan li għadni kif għedt, li l-app tiġġenera codes biex tkun tista' taċċessa minn fuq il-web, jekk xi ħadd kellu l-iscreensharing għaddej minn fuq il-mobile, kif seta' jottjeni dawn il-codes, ngħid li l-code jrid jidher fuq l-iscreen, jiġifieri l-persuna trid tmur mill-app, tagħfas 'Generate Secure Code', il-code jidher fuq l-iscreen. Ovvjament il-persuna tħares lejn l-iscreen, ħa tmur fuq il-web u ddaħħal dak il-code mbagħad, apparti l-username tagħha. Però, dik l-informazzjoni hija available ġol-app innifisha. Jiġifieri biex tiġġenera secure code, mhux tagħfas il-buttuna u daqshekk, trid tagħfas 'Generate Secure Code' u skont jekk għandekx biometrics enabled jew inkella PIN, ħa ddaħħal wieħed jew l-ieħor. Imbagħad itik il-code. Jiġifieri mhux xi ħadd ħalla l-mobile hemm u xi ħadd għafas buttuna biss, le. Xorta trid tawtentika, imbagħad tagħtik il-kodiċi. Once li l-kodiċi jurihulek fuq l-iscreen, int ħa tużah biex tidħol fuq il-web ukoll.

Ngħid li, meta jkollna użu bħalma qed naraw bħalissa, hija normali li tara persuna juża l-app, eżempju biex jiċċekkja transactions, eċċetera eċċetera. Però, imbagħad ikollok klijenti li jippreferu jidħlu minn fuq kompjuter, eżempju, jew minn fuq... biex jaċċessaw il-web ħalli jagħmlu t-tranżazzjonijiet, forsi għax screen ikbar, iktar komdu. Però, din hi xi ħaġa li naraw pjuttost normali; naraw din l-attività li ssir l-ewwel minn ġol-app u,

> ***mbagħad, dak li jkun ikompli pereżempju minn ġol-web. Però, għal kull waħda minnhom, irid jawtentika.***
>
> ***Mistoqsi mill-Arbitru jekk f'dan il-każ hux qed jintużaw iż-żewġ channels ta' komunikazzjoni tagħna, kemm mill-app u kemm mill-web, ngħid li hekk hu.***
>
> ***Mistoqsi mill-Arbitru jekk jistgħux ikunu t-tnejn imqabbdin fl-istess ħin, ngħid li jistgħu jkunu. Ir-raġuni hija li, narawha f'ħafna każijiet li jkollok klijent li qed juża l-app biex jara l-informazzjoni jew jiċċekkja account jew jara dettalji ta' tranżazzjonijiet, imbagħad xħin jiġi biex jagħmel the actual action, jiġifieri transfers eżempju, jillogja wkoll minn ġol-web. Jiġifieri jkun hemm simultaneous use of two different channels."***[14]

Ma sarx kontroeżami għax-xhieda ta' Nathan Gatt.

Sottomissjonijiet Finali:

L-Ilmentatriċi qalet li ma ġietx infurmata li bis-sistema ta' *Instant Payments* li daħlet f'Ottubru 2025 li permezz tagħha l-limitu ta' pagament tagħha kien żdied minn €5,000 għal ammont ferm akbar. Saħqet li issa li saret taf li kien hemm attentat qabel biex isiru pagamenti oħra fi flus AED meta l-Arbitru talab kopji tal-SMS, allura, skont hi, l-Bank messu xamm il-frodi u waqqaf il-pagamenti[15].

Min-naħa ta' BNF, saħqu li bl-introduzzjoni tas-sistema *Instant Payments* minn Ottubru 2025 (Reg UE 2024/886), il-Bank għandu obbligu li pagament *Instant Payment*, jekk ma jkunx hemm xamma ta' xi ħaġa li mhux f'lokha, irid jiġi pproċessat fi żmien ftit sekondi u, għalhekk, il-Bank ma għandux opportunità li jagħmel monitoraġġ ta' pagamenti effettiv. Apparti minn hekk, sostnew li l-Ilmentatriċi kienet traskurata b'mod eċċessiv (*gross negligence*) li jeżenta lill-Bank skont Artikolu 74 ta' PSD 2 (Direttiva (EU) 2015/2366) milli jagħmel rifużjoni skont l-Artikolu 73 ta' l-istess PSD 2[16].

[14] P. 68 - 70
[15] P. 74
[16] P. 76 - 92

Analiżi u konsiderazzjoni

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

Iżda kif diġà ntqal qabel, dan il-każ iparti sew mill-każi kkunsidrati fil-mudell fejn il-frodist jippersonifika l-Bank permezz ta' SMS, *email* u/jew telefonata. F'dan il-każ, il-frodist ippersonifika bank ieħor (Revolut) li miegħu l-Ilmentatriċi kellha kont u b'xi mod irnexxielu jakkwista l-kodiċi tal-kont tagħha ma' BNF biex jagħmel sfreġju minn flusha.

Filwaqt li l-Ilmentatriċi tiċħad li hija żvelat il-kodiċi sigrieti rigward il-kont ma' BNF, l-Arbitru jara probabbiltà kbira li anke jekk mhux b'mod intenzjonat, kixfet il-kodiċi fil-proċess ta' *screen sharing.* Ma hemm l-ebda spjegazzjoni oħra kif il-frodist sa minn kmieni waqt it-telefonata ta' aktar minn erba' sigħat kien diġà rnexxielu jiskatta proċess biex BNF jibagħtu kodiċi li jawtorizza pagamenti fi flus AED li ma sarx għax l-Ilmentatriċi ma ntebħitx bih. Kif spjega Nathan Gatt, biex sar il-pagament ilmentat, il-kodiċi ġie muri fuq l-i*screen* u l-frodist li kellu *screen sharing* seta' jarah u jużah biex jawtorizza l-pagament ilmentat.

Persuna bħall-Ilmentatriċi li għandha edukazzjoni terzjarja, u mpjegata f'attivitajiet li jinvolvu *screen sharing,* kellha tifhem ir-riskji ta' proċessi bħal dawn, u m'għandhiex tiskanta li b'għemilha hija ffaċilitat b'doza qawwija ta' negliġenza biex il-frodi sseħħ.

L-uniku argument li jista' joffri ftit kenn lill-Ilmentatriċi huwa l-fatt li jidher li ma kinitx taf x'kien il-limitu ta' pagamenti tal-kont tagħha. Hija argumentat li dan suppost kien ta' €5,000 skont il-prattika ta' banek oħra u qalet li dan żdied b'mod awtomatiku bla ma ġiet infurmata permezz tal-introduzzjoni ta' *Instant Payments* li saret f'Ottubru 2025.

Minn deċiżjonijiet dwar ilmenti ASF 338/2025 u ASF 339/2025 (li ġew appellati mill-BNF), l-Arbitru jaf li dan mhux il-każ u li l-kont tal-Ilmentatriċi kellu limitu ta' pagamenti għoli li ma ġiex mittiefes bl-introduzzjoni tas-sistema *Instant Payments*. Peress li fil-jum ta' dan il-każ saru pagamenti ta' aktar minn €22,500,

huwa ċar li l-limitu tal-pagamenti kien jeċċedi dan il-livell u li dan kien diġà *in vigore* qabel id-dħul tas-sistema *Instant Payments.*

L-Arbitru jqis li dan kien nuqqas min-naħa ta' BNF. Dan kellu obbligi li l-klijent ikun infurmat b'mod formali x'kien il-limitu li japplika għal pagamenti mill-kont tiegħu, u li qabel l-introduzzjoni tal-*Instant Payment regulations* kellu jinforma lill-klijenti bid-dritt tagħhom li jaġġustaw dan il-limitu kif jixtiequ biex jipproteġu lilhom infushom. Min-naħa l-oħra, il-fatt li ftit xhur qabel l-Ilmentatriċi għamlet pagament ta' €40,000,[17] u li fil-jum tal-każ għamlet pagamenti li jeċċedu €22,500 bla ma kellha bżonn titlob żieda fil-limitu juri li kienet konxja li l-limitu ma kienx baxx daqs €5,000 kif allegat.

Deċiżjoni

L-Arbitru jiddeċiedi skont kif provdut f'Artiklu 19(3)(b) tal-Kap. 555 tal-Liġijiet ta' Malta, b'referenza għal dak li, fil-fehma tiegħu, ikun ġust, ekwu u raġonevoli fiċ-ċirkostanzi u merti sostantivi tal-każ.

Skont il-preamboli 71 u 72 tal-PSD 2 DIRECTIVE (EU) 2015/2366, f'każ ta' pagament mhux awtorizzat, il-Bank huwa dovut jirrifondi l-parti l-kbira tat-telf inkors ħlief f'każi ta' negliġenza estrema (*gross negligence*) min-naħa tal-klijent.

L-Arbitru jqis li fiċ-ċirkostanzi kollha ta' dan il-każ kif spjegat aktar qabel, l-Ilmentatriċi uriet *'gross negligence'* fi grad estrem li ma jobbligax lil BNF jikkumpensaha. Għalhekk jaqbel mal-argumenti ta' BNF li fiċ-ċirkostanzi partikolari ta' dan il-każ l-ebda rimborż m'hu dovut.

Għaldaqstant dan l-ilment qed jiġi miċħud u l-partijiet qed jiġu ordnati li jġorru l-ispejjeż rispettivi tagħhom.

L-Arbitru, skont l-Artikolu 26(3)(c)(i) u (iii), qed hawnhekk jagħti direzzjoni lill-BNF biex jinforma lill-klijenti tiegħu dwar il-limitu ta' pagamenti abbinat mal-kont tagħhom u jagħti faċilità biex il-klijenti jkunu jistgħu b'mod faċli jaġġustaw dan il-limitu kif ikunu jixtiequ skont il-bżonnijiet reali tagħhom.

[17] P. 61

Kumment addizzjonali

L-Arbitru iżda jieħu din l-opportunità biex isostni li filwaqt li s-sistema ta' *Instant Payments* tippreżenta sfida akbar għall-banek biex jagħmlu monitoraġġ ta' pagamenti effettiv skont kif mitlub taħt PSD2 u kif spjegat fin-Nota Teknika annessa ma' deċiżjonijiet ASF 338/2025 u ASF 339/2025, is-sistema *Instant Payments* ma eżentatx lill-banek milli jagħmlu dan it-tip ta' monitoraġġ effettiv billi jkollhom sistemi teknoloġiċi moderni li jkunu kapaċi jżommu għal aktar evalwazzjoni pagamenti suspettużi.

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. Dettalji personali tal-Ilmentatur/i jkunu anonimizzati skont l-artikolu 11(1)(f) tal-Att.