

ZJ

(‘l-Ilmentatriċi’)

vs

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

(‘BOV’, ‘il-Bank’ jew ‘il-Fornitur tas-Servizz’)

Seduta tat-30 ta’ Jannar 2026

L-Arbitru,

Ra l-Ilment¹ magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta’ €8,000 rigward pagamenti li saru lil terzi (mill-kont tagħha mal-Bank permezz tad-debit card abbinata mal-kont) li wara rrizulta li kienu frodisti.

Issostni li rat reklam fuq Facebook dwar kif investiment f’Tesla kien qed jgħin lil familji Maltin jagħmlu investment vantaġġjuż u tħajret tinvesti €250. Tat id-dettali tagħha inkluż in-numru tal-card tal-Bank, u minn hemm sar l-ewwel pagament ta’ €250 li ma jiffurmax parti minn dan l-Ilment peress li kien awtorizzat kif suppost.

Wara xi jiem, giet ikkuntatjata bit-telefon biex iħajjruha tinvesti iżjed iżda peress li bdiet tiżviluppa dubji talbet li ssir rifużjoni tal-investment. Iżda l-frodsti qalulha li l-investment kien diġà żdied għal €440.24 u biex issir ir-rifużjoni trid tiftaħ kont ma’ Binance.

Nhar it-18 t’April 2023, ċemplulha u qalulha biex iżżid il-flus fil-kont tal-BOV u meta staqsiet għalfejn qalulha:

¹ Formola tal-Ilment minn Paġna (P.) 1 - 8 b’dokumentazzjoni addizzjonali minn P. 9 - 227.

“they need to confirm that I actually had some money, prior to give (giving) me the refund. So I transferred €10,000 into the account.”²

Minn hemm 'il quddiem, il-frodisti għamlu festa bi flusha u żarmawliha l-kont f'affari ta' ftit sigħat.³

Din hija l-iskeda tal-pagamenti li saru u oħrajn li ppruvaw jieħdu izda ġew miżmuma mill-Bank, f'ordni kronoloġika⁴:

Data	Ħin	Ammont € Imħallas	Ammont € Miżmum	Raġuni	Favur/Card No
18.04.1023	13:30:29		4500	Restrizzjoni tas-sistema BOV	simplex.com 6004
“	13:31:15		4500	“	“
“	13:36:12		1500	“	Revolut 6004
“	14:16:13		4500	“	simplex.com 9836
“	14:16:51		4500	“	“
“	14:20:36		700	“	Revolut 9836
“	14:24:13		700	“	Revolut 6004
“	14:50:24	1500			Revolut 9836
“	14:52:02	1500			“
“	15:11:37		4500	Limitu	simplex.com 9836
“	15:12:28		4500	“	“
“	15:48:47		50	“	Binance 9836
“	16:08:21	50			“
“	16:10:06	950			“
“	16:11:54	2000			“
“	16:13:15		3800	“	“
“	16:34:26		3800	“	“
“	16:37:20		3500	“	“
“	16:45:57		3000	“	“

² P. 3; 9; 300

³ P. 300

⁴ P. 240 - 241

Data	Hin	Ammont € Imħallas	Ammont € Miżmum	Raġuni	Favur/Card No
"	16:47:26	2000			"
"	16:48:55		1000	Limitu	"
"	17:06:17		1800	"	"
"	17:19:25		800	"	"
18.04.2023		8000	47650		

Dan juri li f'jum wieħed, f'anqas minn tlett sigħat, saru sitt pagamenti li flimkien jammontaw għall-ammont ilmentat ta' €8,000 u twaqqfu sbatax attentat li ppruvaw iħallsu €47,650.

Johroġ ċar ukoll li bejn il-ħin ta' 14:52:02, meta sar it-tieni pagament, u bejn it-tielet pagament li sar 16:08:21, kienu twaqqfu tliet pagamenti għax kienu jeċċedu l-pagamenti li jistgħu jsiru f'għurnata waħda li, normalment, għal klijent tip retail ikun ta' €5,000. Allura, huwa kredibbli li biex kien possibbli jsiru tliet pagamenti li jammontaw għal €3,000 kien hemm xi kuntatt bejn il-Bank u l-Ilmentatriċi biex jizzied il-limitu biex jippermettu pagamenti oġhla. Sa dak il-ħin, il-kumulu tal-ħames pagamenti li kienu saru kien jammonta għal €6,000.

Wara dan, saru u twaqqfu erba' attentati oħra bejn il-ħin ta' 16:13:15 u 16:45:57. Izda l-aħħar pagament ta' €2,000 reġa' sar fil-ħin ta' 16:47:26. Dan juri li jew sar xi arrangament ieħor biex jerġa' jogħla l-limitu, jew li l-limitu li ma kienx għoli biżżejjed biex jakkomoda pagamenti li ġew imwaqqfa (€3,800, €3,800, €3,500, €3000) kien għoli biżżejjed biex jakkomoda pagament ta' €2,000 li ġab it-total ta' trasferimenti f'għurnata waħda għal €8,000.

Wara dan, twaqqfu tliet pagamenti oħra (€1,000, €1,800, €800) għax jidher li l-limitu ġie eżawrit għal dak il-jum.

Jidher li fil-jum tal-ġhada, 19 t'April 2023, saru erba' pagamenti żgħar kollettivament għal €83 li mhumie x inkluzi f'dan l-Ilment, probabbli għax €53 kienu rkuprati,⁵ u għax l-Ilmentatriċi riedet tiffoka fuq it-€8,000 tal-ġurnata ta' qabel. Fl-istess jum, il-BOV waqqaf ħdax-il attentat ieħor biex isiru pagamenti

⁵ P. 17

kollettivament għal €5,610 għal raġunijiet tekniċi,⁶ probabbli għax ma kienx fadal flus fil-kont abbinat mal-card.⁷

L-Ilmentatriċi għamlet rapport dwar il-każ lill-pulizija fl-10 t'April 2023.⁸

Għamlet ilment mal-BOV fis-26 t'April 2023⁹ fejn talbet il-Bank jgħinha biex tirkupra flusha. Wara dan, il-Bank għamel diversi attentati biex jagħmel talbiet ta' *chargebacks* skont ir-regoli tal-VISA, iżda dawn ma rnexxewx peress li l-pagamenti kienu jidhru approvati mill-Ilmentatriċi. Skont l-email tal-BOV tal-11 ta' Jannar 2024,¹⁰ wara li *chargebacks* taw frott ċkejken ta' €53, il-każ kien ikkunsidrat magħluq.

Iżda, fl-ilment mal-Arbitru li gie rreġistrat fis-17 t'April 2025, bħala kumpens talbet:

*"I am seeking the compensation of the €8,000 to attached (refer to bank transfer Aptil 2023, highlighted parts) which I have been 'allowed' to transfer to third parties, without any warning or flagging from the bank that such transactions were potential scams, and for which I fell victim to fraud."*¹¹

Qalet li l-Bank messu nduna bil-frodi li kien għaddej u missu waqqafha milli tkompli bil-pagamenti ilmentati. Għalhekk qed titlob li l-Bank jagħmel tajjeb għat-€8,000 li tilfet mill-pagamenti ilmentati.

Risposta

Fir-Risposta¹² tal-Bank qalu:

'Whereas the Bank respectfully submits that prior to executing the above transactions, it had received legitimate instructions from the complainant through the necessary channels.

Whereas all of these transactions were done through the complainants' card ending -9836, through her 3D Secure app, by virtue of which the Bank

⁶ P. 245

⁷ P. 300 statement juri li wara l-pagamenti li rnexxew, kien fadal fil-kont €63.68 biss.

⁸ P. 194 - 196.

⁹ P. 9 - 10

¹⁰ P. 17 - 18

¹¹ p. 4

¹² P. 234 - 238 u dokumenti annessi p. 239 - 258

implements Secure Customer Authentication. This confirms that the transactions were carried out with the cardholder's explicit authentication and authorization. This system is in line with the Payment Service Directive 2 which provides the following:

*'strong customer authentication' means an authentication based on the use of two or more elements categorised as **knowledge (something only the user knows)**, **possession (something only the user possesses)** and **inherence (something the user is)** that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;¹³*

Whereas after each transaction, the Bank sent [the Complainant] SMS's to inform her that the transactions were affected¹⁴. However, [the Complainant] did not contact the Bank to complain that the transactions were not genuine. Therefore, when [the Complainant] affected similar transactions to the same merchant, the Bank did not have any indication that they were not genuine.

Respectfully, the Bank submits that the money was transferred upon the express instructions and due authorization of [the Complainant] herself, and she was fully aware of the amounts she was transferring, the recipient of such money and where this money was being received. Therefore, she was an active participant in these transfers.

Whereas on the 15th of June 2023, [the Complainant] contacted the Bank requesting the return of the funds for the transactions in question in this arbitration. At this point, the Bank informed her that the transactions effected through Revolut needed to be disputed directly with Revolut.¹⁵

Whereas with respect to the rest of the transactions effected on her card, the Bank raised a dispute for each transaction with the foreign bank of the merchant. This bank informed BOV that its' merchant provided [the Complainant] with a service, and that she had accepted the terms and conditions of this service which was fully rendered. Furthermore, these terms and

¹³ Article 4(30) of PSD2.

¹⁴ **DOC.A:** List of SMS's regarding transactions affected on the 18 - 19 of April 2023.

¹⁵ **DOC.B:** Email dated 28 September 2023.

conditions clearly stated that the payments cannot be cancelled, recalled or refunded.¹⁶ This can be seen from the chargeback replies of the merchant bank which BOV provided to [the Complainant]. Thus, the chargeback claims for the amounts of €2,000, €2,000, €950, €50, €30 were all rejected. Moreover, BOV informed [the Complainant] that in respect to the amounts of €20, €18 and €15 the foreign bank did not make the necessary dispute within the respective time limit and therefore these amounts had been credited to her card.¹⁷

Whereas when [the Complainant] made the payments, she did not indicate or make some condition that she wanted the choice to cancel the payment, months after it was made. Obviously, the Bank would have rejected this condition *ab initio* because it is not reasonable to expect to cancel duly authorised payments, months after they were authorised. Even when making the payments, [the Complainant] received emails (attached with her complaint) stating that the payments 'cannot be cancelled, recalled or refunded.'¹⁸ Thus, she was fully aware of the risk that her money may not be refunded once she affected the transactions.

Whereas on the 18th and 19th of April 2023, [the Complainant] attempted to affect 34 total transactions to the financial services platforms Revolut, Binance and Simplex for a total value of **€50,143**. Out of the 34 transactions, 24 transactions were **declined due to the Bank's fraud monitoring systems**. Some were declined since they exceeded the daily transaction limit and others due to certain restrictions imposed by the Bank which can be explained further during the proceedings. The rest of the approved transactions (which are being contested in this Arbitration) fell within a low-risk score, however, the Bank still sent an SMS informing the customer that the transactions were made. A detailed outline of the declined and approved transactions of card ending 9836 between the 18th and the 19th of April 2023 can be seen in '**DOC.D**' and '**DOC.E**' respectively.

Whereas in view of the number of declined transactions, the Bank attempted to call [the Complainant] on the 18th of April 2023 at 16:15:07 to confirm the transactions being made to [HTTP//WWW.BINANCE.COM](http://www.binance.com), [the Complainant] did

¹⁶ Fol. 039 - 040, 057 - 058, 075 - 76, 093 - 094, 111 - 112 of the complaint.

¹⁷ **DOC.C**: Email of 11 of January 2024.

¹⁸ Fol. 173 - 176, 179, 182, 185 of the complaint.

not answer and therefore the Bank **temporarily blocked** her card on the 18th of April at 16:14:06, until confirmation was acquired from the cardholder about the transactions.

Whereas on the 18th of April 2023 at 16:32:53 [the Complainant] called the Bank and confirmed that she was knowingly carrying out the transactions and that they were genuine. Thus, the Bank unblocked the card.

Whereas within 20 minutes (at 16:55:37) [the Complainant] called the Bank once again and requested that the limit on her card is increased to €12,000 so that she could affect payments to Binance. This further confirmed to the Bank that she had the intention to make the transactions.

Whereas in view of the above, it is completely unfounded and unjustified for [the Complainant] to say that she “was not protected at all by the bank”¹⁹ since the Bank’s security mechanisms acted as expected and flagged transactions with a high-risk score so that the Bank could contact the customer.

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 and systems associated with the complainant, and therefore has no obligation to refund the complainant.

Whereas in this context, the Terms and Conditions of the BOV Cashlink Visa²⁰ which [the Complainant] voluntarily accepted, provide the following regarding a cancellation of a payment:

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

¹⁹ Fol.004 of the complaint.

²⁰ **DOC. F:** Product Information Guide of the BOV Cashlink Visa, page 6.

supplier separately. This includes payments made on a regular basis (recurring transactions) from your Account.²¹

Whereas [the Complainant] had the choice to decide with whom to invest her money and cannot expect the Bank to take responsibility for actions which resulted from her own choices. Moreover, the Bank only provided [the Complainant] with the service of processing payments she duly authorised. BOV never provided her with any advice regarding investing and [the Complainant] never requested such advice. Therefore, she cannot now expect the Bank to bear any liability for her investment choices. Moreover, the Bank cannot prohibit its' customers from willingly affecting investments or financial transfers. The Banks' obligation in this respect is to ensure that the transactions are duly authenticated and authorised by the customer. The responsibility to confirm the reliability and the soundness of the investment remains with the customer. Thus, it is completely unfounded and unjustified for [the Complainant] to expect the Bank to refund her the amount lost because it 'allowed'²² her to make the transactions, since that is the exact scope of a payment instrument provided by a financial institution.

Whereas the Bank was not cognisant of any communications [the Complainant] had with third parties which led her to carry out these investments. Nor was the Bank aware that the fraudsters had access to her mobile.²³ In this respect, it is important to note that the transactions were approved through the 3D Secure app, thus [the Complainant's] biometrics or unique code were used, meaning that she was an active participant in the transactions. Therefore, it is unfounded for her to say that the Bank should have warned her that she was "possibly being scammed"²⁴ since the transactions were duly approved and she confirmed they were genuine. Respectfully, the Bank submits that at first [the Complainant] herself did not realise that she was talking to a scammer, therefore it is not reasonable for her to expect that the Bank should have realised this, when all the Bank had visibility to were the duly authorised transactions. Moreover, even when she realised that she was being scammed, she still continued communicating with

²¹ Article 6(b) of the Terms and Conditions of the BOV Cashlink Visa.

²² Fol.004 of the complaint.

²³ Fol.003 of the complaint.

²⁴ Fol.004 of the complaint.

the third party and authorising the transactions instructed, instead of immediately contacting the bank. This highlights the gross negligence shown by [the Complainant]. In view of this it is unjustified for her to now expect the Bank to take responsibility for her actions.

A. Conclusion

For the reasons articulated above, the Bank respectfully submits that the Complainant's claims are unfounded.”²⁵

Seduti

Fl-ewwel seduta li saret fit-23 ta' Settembru 2025, l-Ilmentatriċi xehdet:

“Ngħid li rajt advert fuq Facebook fl-14 t'April 2023, u kkonsidrajt li kien ġenwin u realistiku. Fih stajt tinvesti l-inqas €250 sa xi €2,500 (ma nafx eżatt) u jien għażilt l-aktar wieħed baxx.

Tajt id-dettalji, u ċaqlaqt il-flus li kelli f'dan l-account u ħallejt €250 biss f'dan l-account biex jekk jinqala' xi ħaġa ma jkunx hemm il-kwantità.

Fil-15 t'April 2023, kont ikkuntattjata fuq WhatsApp, u kif rajt it-Terms and Conditions, qisni biddilt il-ħsieb għax dawn kienu qalu li kien ser ikun fil-cryptocurrencies, li jiena ma nifhimx, u kien ikun ta' ħasra għalija bħala anzjana li nkun naf ċerti affarijiet. U għidtilhom li ridt il-flus lura.

Meta għidtilhom li biddilt l-idea, qaluli li l-investment diġà żdied. Dan kien fil-weekend. Fit-18 t'April 2023, meta sar il-każ, kont ikkuntattjata minn wieħed jismu, Adam, fuq WhatsApp għax kelli l-laptop bil-ħsara. Meta għidtlu li ridt ir-refund, qalli li ried ikolli ċertu ammont ta' flus inkella ma jagħtunix il-flus lura.

Staqsieni għandix Revolut u għidtlu li le u ordnali waħda temporanja. Qal li temporanja fuq ismi.

Ngħid li fetaħli kont mar-Revolut u kelli nagħtih xi informazzjoni. Ngħid li kont tajtu kollox, li talabni tajtulu.

Sadanittant, dan bil-ħsieb li jagħtini l-€250 lura. Kieku kont naf x'inhu ġej, żgur ma kontx nidhol għal dan il-pass.

²⁵ P. 234 - 238

Ngħid li beda jibgħat emails fuq is-Simplex u r-Revolut u jsemmi l-Binance.

Hawnhekk jintervjeni l-Arbitru biex jistaqsini jekk tajtux informazzjoni fuq il-kont li għandi mal-Bank of Valletta.

Ngħid li iva, tajtu kollox.

Mistoqsija mill-Arbitru għalfejn tajtu l-informazzjoni fuq il-kont tiegħi mal-Bank of Valletta jekk jien mingħalija ser ipogġihomli fir-Revolut, ngħid li ma nafx. Hu talabhomli u jien għamilt kif qalli hu.

Peress li ma kellix Revolut, hu kellu jikkuntattja lill-Bank of Valletta u r-Revolut.

Ngħid li dan ix-xogħol kollu sar fuq il-mobile. U l-mobile ġie hacked.

Mistoqsija mill-Arbitru meta semmieli l-Binance kontx naf li ser jeħodli l-flus mill-kont tiegħi biex jinvestili mal-Binance, ngħid li le ma kontx naf. Jien għalija kien qisu qed jittellem biċ-Ĉiniz għax jien dawn l-affarijiet ma nifhimx fihom.

Li kieku kont naf x'ser jigri, żgur li ma kontx nagħmel din il-biċċa xogħol; biex jagħtini €250 ser jidhol fl-affarijiet tiegħi. Sadanittant, jien qed nemmen li dawn il-flus li qed isemmi, li beda jipprova jieħu mill-kont tiegħi – li sadanittant ma nafx li qed jieħu – bdejt naħseb li qed jagħtini.

L-Arbitru jigbed l-attenzjoni li skont ir-records li għandu, fit-18 t'April dan beda billi ħadli żewġ pagamenti ta' €1,500 biex tefali l-flus fir-Revolut.

L-Arbitru jgħid li jien indunajt li ħadli €1,500 għal darbtejn, ngħid li le, le ma ndunajtx.

Qed jingħad li l-Bank of Valletta bagħatli SMS. Ngħid li l-problema kienet li jien kont qed nikkomunika fuq il-mobile u l-mobile tiegħi ġie hacked. Bdejt nara l-apps telgħin fuq il-mobile tiegħi. U jgħidli fejn huma, fejn għandi nagħfas u x'għandi nagħmel. Ngħid li ma kellix kontroll tal-mobile. Il-mobile kien f'idejha. Jekk telgħu xi messaġġi, rahom hu u jien ma rajt xejn għax il-mobile kien hacked. Anke l-emails, xejn xejn ma bdejt nara.

Qed jingħad li jien allura tajtu l-awtorità biex jidhol fil-mobile. Ngħid ma nafx x'awtorità tajtu; naħseb ħadha hu.

Mistoqsija mill-Arbitru jekk semmilix xi ħaġa bħal AnyDesk, ngħid li le, kollox fuq WhatsApp li bdejna nagħmlu.

L-Arbitru jispjega li sadanittant saru żewġ tranzazzjonijiet li permezz tagħhom hu, b'xi mod ġibidli żewġ pagamenti ta' €1,500 mill-Bank of Valletta u marru fil-kont tar-Revolut li fetaħ hu stess. Imbagħad, mill-kont tar-Revolut għosfru.

L-Arbitru jkompli jispjega li l-Bank of Valletta ma jkunx jaf x'sar mill-flus wara r-Revolut. Dwar dawn iż-żewġ pagamenti, l-bank sa r-Revolut jaf. X'sar minnhom il-flus wara li jkunu marru fir-Revolut, il-bank ma jkunx jaf.

L-Arbitru jispjega li l-bank qed jgħid li għal kull pagament li sar bagħatli SMS u li jien ngħid li qatt ma rajthom.

Ngħid li rajthom fis-6.00 p.m. meta indunajt x'ġara. Naħseb ma rrealizzajt li kelli l-SMSes. Hadt qatgħa meta rajt il-kont vojt. Ngħid li ma nafx jekk rajthomx, għax issa għaddew sentejn u nofs.

L-Arbitru jgħid li fit-18 t'April 2023, minbarra ż-żewġ pagamenti lir-Revolut, jien għamilt ħafna pagamenti oħra lill-Binance direttament, allura, hemmhekk il-Bank of Valletta kien jaf li kienu sejr in fil-Binance.

Mistoqsija mill-Arbitru x'għamilt meta bdew isiru dawn il-pagamenti, ngħid li jien ma kontx naf li qed isiru dawn il-pagamenti, li qed jeħodli. Ninsisti li ma kontx naf x'inhu jagħmel.

L-Arbitru jgħid li jien, f'xi ħin, ċempilt lill-Bank of Valletta biex nitlobhom jgħolluli l-limits biex inkun nista' nagħmel dawn il-pagamenti. Jgħid li jien kelli telefonati mal-bank li fihom il-bank ġibidli l-attenzjoni li kienu qed isiru dawn il-pagamenti u jiena għidtlu alright.

Ngħid li l-bank ma ġibidlix l-attenzjoni li dawn setgħu kienu scam għax kieku kont nieqaf.

Mistoqsija mill-Arbitru x'qalli l-bank, ngħid li ma niftakarx x'qalli ezatt sentejn u nofs ilu.

Ngħid li meta s-soltu nċempel lill-bank għal xi ħaġa, jistaqsu fejn għandek il-kont, l-aħħar ħaġa li nfaqt; u nistaqsi, allura, dakinhar lili ma staqsewnix biex jidentifikawni? Jistaqsuni, 'Taf x'inti tagħmel?!'

Mistoqsija mill-Arbitru niftakarx li f'ħin minnhom xi ħadd mill-bank ċempilli u jien għidtlu, 'Le, daww alright, naf bihom', ngħid li jien kont ċempilt lill-bank u l-bank kien fid-dmir li jistaqsi daww il-mistoqsijiet biex jidentifikani.

L-Arbitru qed jirreferini għar-risposta tal-bank, punt 12, li jgħid:

‘Whereas on the 18th of April 2023 at 16:32:53 [the Complainant] called the Bank and confirmed that she was knowingly carrying out the transactions and that they were genuine. Thus, the bank unblocked the card.’

L-Arbitru jispjega li l-bank qed jgħid li l-ewwel waqqafli l-card għax beda jidhollu suspett, imbagħad, jiena ċempilt fl-16:32 (għax il-bank kien għalaq il-card fl-16:15) u għidtilhom li dawk kienu ġenwini u, għaldaqstant, fetħuli l-card.

Ngħid li jien kont qed nistenna li nieħu l-€250 lura.

Apparti minn hekk, il-bank jgħid li wara għoxrin minuta, jien ergajt ċempilt il-bank u għidtilhom biex jgħolluli l-limit għal €12,000.

Ngħid li ma stajtx ngħidilhom hekk għaliex ma kellix €12,000 fil-kont.

Ngħid li fil-bidu staqsieni kemm għandi flus u għidtlu €10,000. Dawn it-€12,000 ma nafx bihom għax jien ma kellix €12,000. €10,000 kelli f’dak l-account dak iż-żmien.

Mistoqsija mill-Arbitru jekk qed ngħid li jien ma ċempiltx dakinhar fl-16:30 biex ngħidilhom jgħolluli l-limit għal €12,000, ngħid li ma jidhirlix, tat-€12,000 għax ma kellix €12,000. Ma stajtx ngħolli sa €12,000 għax jiena €10,000 kelli.”²⁶

Fil-kontroeżami xehdet:

“Qed jingħad li biex sar hekk jien tajthom aktar min-numru tal-kont tiegħi.

Ngħid li kulma talabni kollox tajtu għax jiena kont taħt seher. Kont hypnotised. Lanqas kont kilt dakinhar.

Ngħid li jiena l-għada ċempilt il-bank għax meta indunajt x’għara la ridt nitkellem, tgħidx kemm bkejt, u lanqas lit-tfal ma ridt inkellem, lil hadd.

Jien ċempilt lill-bank l-għada, Wednesday, on the 19th u kont mort l-Għassa.

Qed jingħad li jien kont suspettuża fit-18 t’April b’dak li kien qiegħed jìgri, u mistoqsija għamiltx aktar tranżazzjonijiet wara t-18 t’April, ngħid li mbagħad ma nafx kif reġa’ daħal fihom, imma baqa’ jieħu. Però, dawk kienu tawhomli l-bank. Kienu xi €18, €30 ...

Hu baqa’ jieħu, imbagħad, il-bank reġa’ bblukkja l-card.

²⁶ P. 259 - 262

Ngħid li fit-18 t'April ċempilt kemm-il darba meta kont għadni bil-kuntatt miegħu (il-frodist), imma ma ċempiltx wara biex ngħidilhom x'kien ġara.

Mistoqsija inix familjari mal-BOV 3D Secure App, ngħid li dik għamilhieli hu għax ma kontx naf xi tfisser. Qatt ma kont użajtha qabel. Qalli x'għandi nagħmel biex noħloqha.

Mistoqsija x'rajt waqt li bdew jiġu approvati dawn it-tranzazzjonijiet, x'kien qed jidher fuq l-iscreen, ngħid il-logo tal-BOV 3D Secure u x'għandi nagħmel biex nidhol fuqha bl-instructions tiegħu.

Mistoqsija x'għamilt biex irreġistrajtha jekk hux b'PIN, jekk hux b'wiċċi jew bil-fingerprint biex naċċessaha, ngħid li ma niftakarx imma jista' jkun li għamilt il-wiċċ jew hekk għax għamiltu kemm-il darba.

Mistoqsija jekk kienx fl-18 t'April li qed ngħid li għamiltu kemm-il darba, ngħid li iva.

Mistoqsija meta għamiltu niftakarx x'kont qed nara fuq l-iscreen, x'kont qed nagħmel jien bil-facial recognition, ngħid li le.

Mistoqsija nikkonferma l-email address tiegħi, ngħid xxxxxxxx@gmail.com.

Mistoqsija dakinhar li ġraw dawn it-tranzazzjonijiet kelli access għall-inbox tal-emails tiegħi, nerġa' ngħid li ma stajtx narahom l-emails għax il-mobile kien totalment f'idejh. Anke biex nidhol fuq xi haġa, kien jgħidli, 'Aghfas hemm, aghfas hemm,' u qabel ma nara jiena kien jgħidli fejn hu. U tara l-mobile sejjer hekk.' Tal-bliġh! Trid tiġrilek biex tkun taf x'jiġifieri.

Qed niġi referuta mill-Arbitru għal ittra mibgħuta minni lill-bank fis-26 t'April 2023, fejn fiha tlabt lill-bank biex jgħinni nirkupra dawn il-flus.

Qed jingħad li jien m'għidtx lill-bank f'din l-ittra li dan kien htija tiegħu u, għaldaqstant, irrid il-flus lura bħalma qed nagħmel f'dan l-ilment.

Qed niġi mistqosija kif inbidel id-diskors minn meta tlabtu biex jgħinni nirkupra dawn il-flus - qisni qed nammetti li li ġara kien htija tiegħi – għal dak li qed ngħid issa li dak li ġara kien htija tal-bank għax missu waqqafni.

Ngħid li meta l-għada ċempilt u tkellimt ma' waħda mill-bank fuq dak li ġara u ma ġarax, qaltli biex nikteb ittra biex nieħu l-cash back. Jien qgħadt fuq l-instructions ta' din il-persuna biex isir iċ-chargeback.²⁷

²⁷ P. 262 - 264

Wara din is-seduta, l-Arbitru talab lill-Bank jibgħat evidenza dwar l-aħħar KYC li sar fuq l-Ilmentatriċi u *statement* għall-perjodu ta' sena sa April 2023 tal-kont minn fejn saru il-pagamenti.

Dokumenti KYC²⁸ mibgħuta mill-BOV juru li kienu *'Simplified Due Diligence'* b'informazzjoni skarsa għax l-Ilmentatriċi giet ikkunsidrata bħala klijenta normali.

Mill-istatement²⁹ jirriżulta b'mod ċar li l-pagamenti li fuqhom huwa bbażat l-Ilment kienu b'mod ċar inkompatibbli mal-istorja tal-kont fejn pagamenti ta' aktar minn elf ewro kienu sostanzjalment trasferimenti bejn il-kontijiet tagħha stess.

Fis-seduta tat-13 Novembru 2025, xehdet f'isem il-BOV, Sandra Stevens li qalet:

"Nikkonferma li bgħatna SMS alerts għal kull tranzazzjoni li giet ikkontestata f'dan il-każ inkluż il-pagament ta' €1,500 u ta' €2,000 tat-18 t'April 2023. Aħna nibgħatu SMS għal kull tranzazzjoni online li ssir.

<OMISSIS>

Ngħid li f'dan il-każ kien hemm tranzazzjonijiet oħrajn li ġew attempted u m'għaddewx minħabba rules oħra li għandna ssettjati fuq is-sistema.

<OMISSIS>

<OMISSIS>

Mistoqsija mill-Arbitru kienx hemm xi talba aktar qabel għal increase in limits peress li mill-informazzjoni li ngħata l-Arbitru, l-increase in limit sar tard ħafna meta t-tranzazzjonijiet kienu diġà għaddew u talbet li jogħla iżjed.

L-Arbitru jirreferi għal punt 13 tar-risposta tal-bank li jgħid:

'Whereas within 20 minutes at 16:55:37, [the Complainant] called the bank once again and requested that the limit on her card be increased to €12,000 so she could effect payments to Binance.'

L-Arbitru jgħid li at 16:55:37, il-pagament li semmejt tad-€9,000 kien diġà sar. U wara dan il-ħin ma sarux pagamenti kbar.

²⁸ P. 267 - 270

²⁹ P. 271 - 304

Għaldaqstant, l-Arbitru qed jistaqsi f'dik il-ġurnata tat-18 t'April kien għaddew €9,000, kien hemm xi increase in limit jew il-limit kien diġà kbir li seta' jakkomodaw l-pagament mingħajr increase in limit, ngħid li għal din il-card partikolari jista' jkollok kemm ikollok flus, jgħaddu biss it-tranzazzjonijiet sad-daily limit.

Ngħid li jien ma nistax nikkonferma bl-amment kemm kien id-daily limit. Irrid irrid nikċekkja, però, għandi nota li fis-2.00 p.m. kien hemm increase ta' €6,000 biex jgħaddu tranzazzjonijiet minn Revolut għal Simplex.

Nikkonferma li kien hemm talba għal increase. Hemm nota li rrekordja l-user tal-Customer Care fis-2.03 p.m.

L-Arbitru jiġbed l-attenzjoni li din in-nota mhijiex imsemmija fir-risposta tal-bank u jitlob lil Dr Luana Vella biex tinformah x'kien id-daily limit ta' dik il-ġurnata u biex tikkonferma kienx hemm talba għal żieda fil-limit li mhijiex imressqa fir-risposta tal-bank.

L-Arbitru jitlob lill-bank biex jiskopri t-telefonati kollha li għamlet l-Ilmentatriċi fit-18 t'April u jipprovdu r-recordings tagħhom.”³⁰

Fil-kontroezami, Sandra Stevens ikkonfermat li l-card kienet registrata fit-3D Secure fil-jum stess tat-18 t'April 2023 permezz ta' verification code li ntbagħat lill-Ilmentatriċi fuq il-mobile registrat mal-BOV. Qalet ukoll la t-tranzazzjonijiet kienu approvati permezz tat-3D Secure, għall-Bank it-tranzazzjonijiet kienu normali.

Meta mistoqsija mill-Arbitru għalfejn ċerti pagamenti ġew approvati wara li tranzazzjonijiet qabel kienu ġew rifjutati, Sandra Stevens qalet:

“Qed niġi mistoqsija, meta tranzazzjonijiet ġew declined, imbagħad, approvati u tranzazzjonijiet oħrajn li wara ġew approvati, is-sistema tal-bank hijiex sensittiva biex tirreġistra li hemm affarijiet mhux tas-soltu, ngħid li <OMISSIS>.”³¹

Mistoqsija mill-Arbitru jekk meta jsir il-moniteragg tal-pagamenti s-sistema tiħux konsiderazzjoni l-fatt li t-tranzazzjonijiet kienu totalment mhux soltu paragnat ma' kif kien jaħdem il-kont qabel, Sandra Stevens qalet:

³⁰ P. 305 - 308

³¹ P. 310

“Le. Is-sistema ma tiffilaggjahomx bħala riskjużi lanqas minħabba r-risk score.”³²

L-Arbitru talab lill-Bank biex jipprovdi reġistrazzjoni tat-telefonati li saru mal-Ilmentatriċi fit-18 t’April 2023, iżda l-Bank informa li minħabba raġunijiet tekniċi dawn ir-recordings mhumiex disponibbli.³³

B’digriet tas-27 ta’ Novembru 2025, l-Arbitru talab konferma tal-ħin li saru telefonati fit-18 u d-19 t’April mal-Ilmentatriċi u xi noti li ġew irreġistrati dwar x’kien l-iskop ta’ dawn it-telefonati.³⁴

BOV wieġbu:

“Għalkemm ma nstabux call logs jew noti fis-sistemi tal-Bank, jidher illi l-card tal-Ilmentatriċi ġiet blocked u unblocked diversi drabi f’dan il-perjodu, probabbilment minħabba alerts ta’ frodi wara tranzazzjonijiet ta’ valur għoli (€50, €950, €2,000 fi ftit minuti, u oħra ta’ €2,000 ftit wara). Dawn l-azzjonijiet jissugġerixxu li kwalunkwe telefonata li saret kienet dwar l-istatus tal-card jew adjustments fil-limiti tal-card in vista ta’ dawn l-alerts.”³⁵

Sottomissjonijiet finali

Il-partijiet bażikament ikkonfermaw dak li kien diġà ġie espost fl-Ilment, fir-Risposta u fix-xhieda waqt is-seduti.

Analizi u kunsiderazzjoni

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

Dan il-każ jinvolve żewġ aspetti:

1. Jekk il-pagamenti ilmentati kinux verament awtentikati u awtorizzati mill-Ilmentatriċi li b’negligenza grossolana, awtorizzat lill-frodist biex ikollu aċċess sħiħ għall-kontijiet tagħha mal-Bank u jagħmel dawn il-pagamenti

³² P. 311

³³ P. 312

³⁴ P. 313

³⁵ P. 320

b'mod li l-Bank kellu għax jaħseb li dawn kienu pagamenti normalment awtorizzati mill-Ilmentatriċi.

2. Jekk skont (1.) jirriżulta li dawn il-pagamenti kienu awtorizzati b'negligenza grossolona min-naħa tal-Ilmentatriċi, jekk il-BOV kellux ħtija li skont l-obbligi dwar moniteraġġ ta' pagamenti ma waqqafx dawn il-pagamenti u jiftaħ diskussjoni serja mal-Ilmentatriċi dwar il-possibilità li kienet qed tiġi ffrodata.

Dan il-każ ma jinkwadrix mal-ilmenti li għalihom l-Arbitru ħareġ mudell dwar kif għandha tiġi allokata r-responsabbiltà bejn il-bank u l-klijent għax dan mhux każ fejn l-ilmentatur għafas xi link fuq xi SMS jew email li deheru li kienu ġejjin mill-Bank.

Lanqas ma hu każ dwar 'pig butchering' li dwaru l-Arbitru ħareġ noti tekniċi dwar ir-responsabbiltà tal-banek biex jipprevenu dawn it-tip ta' frodi (scams). Pig Butchering isir fuq perjodu pjuttost twil fejn il-frodista jikseb il-kunfidenza tal-vittma li tittrasferilu flus biex mingħaliha tagħmel xi gwadann.

Dan il-każ jinvolvi pagamenti li ġraw f'affari ta' ftit sigħat u ma kienx hemm relazzjoni ta' kunfidenza bejn il-vittma u l-frodista.

Jekk l-Arbitru jsib li ma kienx hemm negligenza grossolana min-naħa tal-Ilmentatriċi skont il-preamboli 71 u 72 ta' PSD 2 (Directive EU 2016/2366) (riprodotti hawn taħt), allura, il-każ jieqaf hemm bla ħtieġa ta' kunsiderazzjoni tat-tieni punt.

"Preamboli ta' Direttiva EU 2105/2366 (PSD2)

(71) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to

provide an incentive for the payment service user to notify, without undue delay, the L 337/46 Official Journal of the European Union 23.12.2015 EN payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount, unless the payment service user has acted fraudulently or with gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products.

(72) In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases."

Jekk min-naħa l-oħra, jirrizulta lill-Arbitru li l-Ilmentatriċi wriet negligenza grossolana, allura, jieħu kunsiderazzjoni wkoll tat-tieni punt.

Kunsiderazzjoni dwar jekk kienx hemm negligenza grossolana mill-Ilmentatriċi

L-Ilmentatriċi ammettiet żewġ affarijiet ta' ċertu importanza:

- a. L-Ilmentatriċi ammettiet li hija intelqet għal kollox f'idejn il-frodista u għamlet dak kollu li talabha u tagħtu aċċess biex jidhol fil-kont tagħha u jiġbed il-flus kollha li sab. Ikkonfermat li anke tagħtu approvazzjoni tal-pagamenti li jeħtieġ biex issir l-awtorizzazzjoni ta' 3D Secure. Ikkonfermat li rċeviet l-SMS li bagħat il-Bank għal kull attentat jew twettiq ta' pagament, iżda tant kienet konfuża, li ma tatx kashom ħlief meta kien tard wisq.
- b. Li tant intelqet f'idejn il-frodista, li aċċettat li tmexxi €10,000 f'dan il-kont bħala prova li għandha x'jagħmel tajjeb biex ikun jista' jirrifondilha l-ewwel pagament ta' €250.

L-Arbitru jsib li hemm provi biżżejjed biex jasal għall-konklużjoni li l-Ilmentatriċi kkommettiet negligenza grossolana li kienet il-kaġun prinċipali tat-telf li ġarrbet. X'sens jagħmel li biex xi ħadd jibgħatlek ftit mijiet ewro flusek lura jrid jara li fil-kont għandek €10,000? Dan biss kellu jqajjem suspett qawwi lill-Ilmentatriċi li kienet qed tiddilja ma' frodist.

Preambolu 72 ikkwotat qabel, jagħti biss eżempju wieħed ta' *gross negligence*:

"keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties."

Dan l-eżempju jgħodd ħafna għal dan il-każ għax meta l-Ilmentatriċi tat aċċess għall-kont tagħha biex terzi frodisti jkunu jistgħu jippersonafikawha mal-Bank, allura, neħħa kull protezzjoni li joffri għaladarba l-frodista seta' huwa stess japprova n-notifiki ta' 3D Secure.

Huwa stramb ukoll li waqt li kien għaddej dan il-frodi, fi żmien ftit sigħat, l-Ilmentatriċi ċomplet lill-Bank biex jgħollilha l-limitu u biex isserraħ moħħ il-Bank li hi kienet taf u tapprova dawn il-pagamenti.³⁶

Filwaqt li l-BOV għal raġunijiet teknici naqas milli jipprovdi reġistrazzjoni jew noti dwar x'intqal f'dawn it-telefonati, hemm evidenza biżżejjed li ċerti pagamenti setgħu jgħaddu biss, wara li oħrajn kienu twaqqfu, jekk l-Ilmentatriċi kkonfermat li taf bil-pagamenti li kienu għaddejja u li tablet żieda fil-limitu biex dawn il-pagamenti jkunu jistgħu jgħaddu.

Għal dawn ir-raġunijiet, l-Arbitru jsib negligenza grossolana min-naħa tal-Ilmentatriċi u, għalhekk, jgħaddi biex jeżamina t-tieni punt dwar jekk l-obbligi ta' moniteragg ta' pagamenti ġewx rispettati mill-BOV biex jintervjeni u jwaqqaf dawn il-pagamenti.

Obbligi tal-Bank dwar moniteragg ta' pagamenti

Fin-nota teknika li ħareġ l-Arbitru dwar l-allokazzjoni ta' responsabbiltà bejn il-bank u l-vittma ilmentatur, intqal:

“Nota 4: PSP (inkluż banek) huma obbligati li jkollhom sistemi effettivi ta' sorveljanza ta' pagamenti biex jiproteġu lill-PSU minn pagamenti frawdolenti. Ir-Regolament Delegat tal-Kummissjoni (UE) 2018/389 tas-27 ta' Novembru 2017 jistabbilixxi standards tekniċi regolatorji għall-awtentikazzjoni qawwija tal-konsumatur u standards miftuħin ta' komunikazzjoni, u jissupplimenta d-Direttiva (UE) 2015/2366.”³⁷

Dan jipprovdi fl-artikolu 2(1) li:

‘Il-fornituri ta' servizzi ta' pagament għandu jkollhom fis-seħħ mekkaniżmi li jimmonitorjaw it-tranzazzjonijiet li jippermettulhom jaqbd u tranżazzjonijiet tal-pagament mhux awtorizzati jew frodulent ... Dawn il-mekkaniżmi għandhom ikunu msejsa fuq l-analiżi tat-tranzazzjonijiet tal-pagament, filwaqt li jqisu elementi li huma tipiċi tal-utent ta' servizzi ta'

³⁶ P. 236, punti 12 u 13

³⁷ <https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32018R0389>

pagament fiċ-ċirkustanzi ta' użu normali tal-kredenzjali personalizzati ta' sigurtà."

L-artikolu 2(2) jipprovdi li s-segwenti fatturi bbażati fuq riskju għandhom jitqiesu fil-mekkaniżmi li jissorveljaw it-tranzazzjonijiet:

- a. Listi ta' elementi tal-awtentikazzjoni kompromessi jew misruqa;*
- b. L-ammont ta' kull tranzazzjoni ta' pagament;*
- b. Xenarji tal-frodi magħrufa fl-għoti ta' servizzi ta' pagament;*
- d. Sinjali ta' infezzjoni tal-malwer fi kwalunkwe sessjoni tal-proċedura ta' awtentikazzjoni;*
- e. F'każ li l-apparat jew is-softwer tal-aċċess jingħata mill-fornitur ta' servizzi ta' pagament, log tal-użu tal-apparat tal-aċċess jew tas-softwer mogħti lill-utent ta' servizzi ta' pagament u l-użu anormali tal-apparat tal-aċċess jew tas-softwer.*

Ġie ċċarat li l-obbligazzjoni ta' sorveljanza ta' mekkaniżmi ta' pagament m'għandux ikun 'sorveljanza ta' riskju f'hin reali' u solitament isir 'wara' l-eżekuzzjoni tat-tranzazzjoni ta' pagament. Għadu ma ġiex definit kemm wara, imma ovvjament għal kwalunkwe valur reali ta' tali mekkaniżmi, d-differenza bejn il-hin reali tal-pagament u dak tas-sorveljanza effettiva ma tridx tkun wisq.

Aktar minn hekk, l-artikolu 68(2) tal-PSD2 jawtorizza PSP li jimblokka pagament:

"Jekk maqbul fil-kuntratt qafas, il-fornitur ta' servizzi ta' pagament jista' jirriżerva d-dritt li jimblokka l-użu tal-istrument ta' pagament għal raġunijiet oġġettivament ġustifikabbli relatati mas-sigurtà tal-istrument ta' pagament, is-suspett ta' użu mhux awtorizzat jew frodulenti tal-istrument ta' pagament jew, fil-każ ta' strument ta' pagament b'linja ta' kreditu, riskju sinifikattivament akbar li l-pagatur jista' ma jkunx kapaċi jissodisfa r-responsabbiltà tiegħu li jhallas."

F'dan il-każ partikolari jirriżulta li:

- Il-pagamenti ilmentati saru fuq medda qasira ta' tliet sigħat.
- Matul dawn it-tliet sigħat, il-Bank waqqaf diversi pagamenti kif spjegat qabel, jiġifieri twaqqfu sbatax-il attentat li ppruvaw iħallsu €47,650. (ara tabella paġna 2)
- Fir-Risposta u waqt ix-xhieda ta' Sandra Stevens, il-Bank qal li waqt li kienu qed jiġu miżmuma dawn il-pagamenti, sar attentat biex isir kuntatt mal-Ilmentatriċi bit-telefon u billi ma wegħbitx, il-*card* ġiet ibblokkjata b'mod temporanju.³⁸

In vista ta' dan, l-Arbitru jidhirlu li l-Bank għamel moniteraġġ ta' pagamenti effettiv li, fil-fatt, ipprevena milli l-Ilmentatriċi tinkorri telf akbar. Tant il-pagamenti saru fi żmien qasir, fost oħrajn li ġew ibblokjati, li l-Arbitru jifhem li l-Bank għamel li seta' biex jippreveni t-telf tal-Ilmentatriċi tant li wara li pprova jċemplilha bla risposta u waqqaf il-*card* temporanjament, l-Ilmentatriċi minn jeddha tat assigurazzjoni lill-Bank li kollox kien sew u b'hekk il-frodist seta' jkompli jżarmalha l-kont.

Deċiżjoni

Għar-raġunijiet hawn spjegati, l-Arbitru qed jiċċad dan l-Ilment u jordna li l-partijiet iġorru l-ispejjeż rispettivi tagħhom.

Alfred Mifsud

Arbitru għas-Servizzi Finanzjarji

³⁸ P. 236, punt 11

Nota ta' Informazzjoni relatata mad-Deciżjoni tal-Arbitru

Dritt ta' Appell

Id-Deciżjoni 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-Deciżjoni jew, fil-każ li ssir talba għal kjarifika jew korrezzjoni tad-Deciżjoni 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-Deciżjoni skont l-artikolu msemmi.

Skont il-prattika stabbilita, id-Deciżjoni 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.