Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 130/2025

TG

('l-Ilmentatur')

vs

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

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

Seduta tat-23 ta' Jannar 2026

L-Arbitru,

Ra l-Ilment[1] magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta' €9,076.34 rigward pagamenti li saru lil terzi mill-kont tal-*credit card* tiegħu mal-Bank, li wara rriżulta li kienu frawdolenti.

Isostni li kien tħajjar jagħmel investiment ta' €499 fuq pjattaforma diġitali PIX*MTFEDUCATION li kien għamel bil-credit card u wara li awtorizza l-pagament bit-3D Secure.

Wara ġie kkuntattjat minn xi ħadd jirrappreżenta l-pjattaforma indikata u ggwidah biex iniżżel it-'*TeamViewer*' deskritt bħala '*remote aċċess software*' biex b'hekk dan it-terza persuna jkollu kontroll sħiħ fuq il-kontijiet tiegħu mal-BOV.

L-Ilmentatur ma rrealizzax li permezz tat-Teamviewer kien qed jawtorizza lil terza persuna jisraqlu flusu, iżda ġara li bejn it-30 t'Ottubru 2023 u l-1 ta' Novembru 2023 saru ħdax (11)-il pagament mill-kontijiet tiegħu mingħajr l-għarfien jew il-kunsens tiegħu u, b'hekk, insterqulu €9,076.34.

[1] Formola tal-Ilment minn Paġna (P.) 1 - 9 b'dokumentazzjoni addizzjonali minn P. 10 - 40.

Qal li kien biss tard fl-01 ta' Novembru li nduna b'dan, u l-għada blokkja l-VISA *card* iżda kien tard wisq għax il-flus kienu diġà għosfru.

Huwa qiegħed jitlob rifużjoni mill-BOV għal dan it-telf għax isostni li huma naqsu milli jipproteġuh biex dan is-serq ma jsirx għax huwa ma awtorizzax dawn il-pagamenti.

'Under Directive (EU) 2015/2366 (PSD2), in particular preambles 71 and 72, a payment service user (PSU) may only be held liable for unauthorised transactions up to a maximum of €50, unless it is proven that the user acted fraudulently or with gross negligence. Gross negligence entails a serious degree of carelessness and not mere oversight. PSD2 clearly states that it is the provider who bears the burden of proving that the PSU has acted with gross negligence. In online payments, where the payment instrument is not physically present, this burden is especially onerous on the PSP, given the consumer's limited ability to detect or prevent the misuse.

In this case, [the Complainant] denies having personally authorised or authenticated the impugned transactions through 3D Secure or any equivalent method. The Bank has failed to produce any evidence that such Strong Customer Authentication (SCA) was applied or completed in accordance with its obligations under PSD2 and the Commission Delegated Regulation (EU) 2018/389, which supplements it. This notwithstanding, and without prejudice to the aforementioned, even if the impugned transactions were indeed authenticated via 3D Secure, [the Complainant] would have still not authorised such transactions.

The Arbiter for Financial Services has, in his own guidance, rightly emphasised that authentication and authorisation are distinct concepts. The mere technical fact that a transaction was authenticated, if at all, does not mean that it was authorised by [the Complainant]. The Arbiter's position is that authorisation requires conscious and informed consent by the PSU. Therefore, a payment that may appear authenticated is not validly authorised if obtained through deception or fraud.

May the claimant quote from the Arbiter's guidance:

'It is important that PSPs understand that there is a difference between authentication and authorisation of payments. The general approach taken by PSPs is that once a payment is authenticated then it is automatically authorised through the gross negligence of the PSU. This is not the case, and one needs to keep separate the concepts of authentication and authorisation.

...

SCA is an authentication process that validates the identity of the PSU or of the payment service. More specifically, the SCA indicates whether the use of the payment instrument is authorised. SCA is based on the use of at least two elements of the following three categories:

Knowledge, being something only the PSU knows (such as PIN or password);

Possession, being something only the PSU possesses (such as a credit card or a registered device); and

Inherence, being something which the PSU is (such as the use of fingerprint or voice recognition).

Given the control systems operated by Banks through two factor authentication (except for small payments below €50) it seems a given that payments can only be affected after being properly authenticated. However, the journey from authentication to authorisation, in case of fraud payments, requires proof by the PSP that the PSU has been grossly negligent in making available to the fraudsters the payment access credentials given by the PSP as part of their terms of business relationship. The Arbiter maintains there is no automaticity that once a fraud payment is authenticated then it is also authorised by the PSU. In fact, there may be evident circumstances when the degree of gross negligence by the PSU is diminished, if not totally eliminated. One has to bear in mind the provisions of preamble 71 of PSD2 which states that "there should be no liability where the payer (PSU) is not in a position to become aware of the loss, theft or misappropriation of the payment instrument". Fraudsters are indeed getting more sophisticated in making their devious schemes hard to distinguish from innocent reality.

In this respect, the complainant maintains that strong customer authorisation (SCA) as per Article 4(30) of Directive 2015/2366/EU (PSD2) is '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'.

In relation to this, Paragraph 33 of the EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) clarified that the two authentication elements 'need to belong to two different categories'.

Article 9 of the Commission Delegated Regulation (EU) 2018/389 further specifies requirements on how to ensure independence of the authentication elements, including the adoption of security measures in the case where the authentication elements are used through a multi-purpose device.

[The Complainant] was the victim of a deceptive scheme involving the use of remote access software, through which third parties gained access to his device and accounts without his knowledge. He did not initiate or approve the transactions in question, nor did he share his credentials knowingly.

Under Articles 2 and 18 of the Commission Delegated Regulation (EU) 2018/389, the Bank is under a duty to:

- Maintain real-time transaction monitoring mechanisms;

- Assess transactions for risk-based indicators;

- Apply SCA unless a payment is objectively low-risk.

According to Article 2(2), the Bank was required to evaluate factors such as:

- Abnormal transaction patterns or amounts;

- Known fraud scenarios;

- Suspicious use of the payer's device or software;

- Signs of malware or unauthorised remote access.

In the claimant's case, multiple transactions of unusually high value were made within a short time frame, directed to Revolut and Wise accounts. Such accounts are known channels frequently exploited in scams. These transactions deviated

markedly from his normal payment behaviour.Yet, no risk alerts were triggered, and no SCA appears to have been enforced. This constitutes a serious failure of the Bank's monitoring and fraud prevention obligations.

Moreover, remote transactions may only be exempt from SCA when all the following are satisfied:

- Fraud rates are demonstrably below threshold;

- Transaction amounts fall below exempt thresholds;

- No abnormal risk indicators are present.

None of these preconditions were met in [the Complainant's] case. The Bank has not shown that the transactions were of low risk or exempt under law. As such, it was obliged to apply SCA — and failed to do so.

Moreover, under Article 68(2) PSD2, the Bank is indeed authorised and dutybound to block payment instruments if it suspects unauthorised or fraudulent use. Given the large, repeated transactions to foreign accounts inconsistent with [the Complainant's] history, the Bank should have intervened.

[The Complainant] did not act with gross negligence. He was the victim of a sophisticated scam, involving psychological manipulation and unauthorised remote access. He did not voluntarily disclose his credentials, nor could he have reasonably detected or prevented the fraud once remote access was obtained covertly. In light of the multiple regulatory and statutory failures, the bank is to be held liable for the unauthorised payments.'[2]

Din hija l-lista tal-pagamenti suġġett ta' dan l-ilment:

DATA	**AMMONT €**	**REFERENZA**
30.10.2023	10.00	REVOLUT p. 37
30.10.2023	3000.00	REVOLUT P. 37

[2] P. 4 - 6

DATA	AMMONT €	REFERENZA
31.10.2023	5.02	WISE P. 37
31.10.2023	2000.00	REVOLUT P. 37
01.11.2023	1000.00	REVOLUT P. 39
01.11.2023	502.35	WISE P. 39
01.11.2023	32.15	WISE P. 39
01.11.2023	2511.75	WISE P. 39
01.11.2023	15.07	WISE P. 39
TOTAL	**9076.34**	

Kien hemm ukoll żewġ pagamenti ta' €3,217 u €2,900 (p. 38) li saru mill-kont normali tal-Ilmentatur (jispiċċaw bin numri 224 u 851) għall-kont tal-*card* biex setgħu isiru l-pagamenti ilmentati fit-tabella ta' hawn fuq. Għalhekk, għalkemm b'xollox kien hemm 11-il pagament li allegatament għamlu l-frodisti, l-aħħar tnejn kienu għall-kont tal-*card* tal-Ilmentatur stess.

L-ilmentatur jikkonferma li l-kont tar-Revolut huwa tiegħu u jużah regolarment u bagħat kopji ta' dan il-kont annessi mal-ilment.[3]

Risposta

Ikkunsidra wkoll ir-Risposta[4] tal-BOV[5] fejn ċaħad l-ilment fl-intier tiegħu u, fost affarijiet oħra, sostna:

> 8. '*Whereas following a thorough internal investigation, and as will be confirmed throughout the proceedings, the Bank confirms that the complainant had the 3D Secure application installed on his device since the 24 November 2022 and remains enrolled on the same device to date. Furthermore, the complainant has successfully registered his*

[3] P. 23 - 24
[4] P. 48 - 57 u dokumenti annessi p. 58 - 101
[5] p. 28 -34, b'annessi fuq p. 35 - 48.

*new VISA Gold card within the same application and has recently authorised a transaction using 3D Secure authentication ("**Doc. B**"). This demonstrates both continued use and familiarity with the Bank's secure authentication systems;*

9. *Whereas the complainant's card ending in 5822 is a BOV Visa Gold Card, governed by the applicable Terms and Conditions, which include the following provisions*[6]*:*

   i. *Clause 3 – Security credentials: The Cardholder may be issued with a PIN, a 3D Secure passcode, and/or a verification code to effect transactions through various channels, including ATMs, Point of Sale terminals, online purchases, and mobile applications such as BOV Pay and the BOV 3D Secure app.*[7]

   ii. *Clause 4(a) – Duty of care: The Cardholder is obliged to take all reasonable precautions to prevent the loss, theft, or fraudulent use of the Card and associated security credentials. The Cardholder must notify the Bank without undue delay upon discovering or suspecting any unauthorised use, loss, or compromise of the Card or its security details.*[8]

   iii. *Clause 4(b)(i) – Liability and reimbursement: Subject to the above, the Bank will investigate unauthorised transactions and reimburse the Cardholder if it is reasonably satisfied that the transaction was not authorised and that the Cardholder is not liable. However, the Cardholder remains fully liable for all transactions carried out prior to notification if they failed to take reasonable steps to safeguard the Card and its credentials.*[9]

   iv. *Clause 4(b)(ii) – Notification Obligations: The Cardholder must notify the Bank immediately upon becoming aware of any*

[6] Refer to "Doc. C".
[7] Page 6 of the Terms and Conditions.
[8] Ibid.
[9] Ibid.

unauthorised use, loss or irregularity. Failure to do so may result in unlimited liability.[10]

v. *Clause 4(b)(iv) – Gross negligence: The Cardholder shall be held liable for all transactions if found to have acted with gross negligence or fraudulently.*

10. *Whereas the Bank reiterates that all disputed transactions were executed following legitimate instructions received through secure and authenticated channels. As expressed above, the complainant's credit card was enrolled in the Bank's 3D Secure system since November of 2022, which implements SCA in full compliance with the Payment Services Directive 2 ("PSD2")*[11] *and the Commission Delegated Regulation (EU) 2018/389 (the "Commission Delegated Regulation")*[12]*. The system was fully operational and functioning at the time of the disputed transactions;* [13]

…

12. **'***Whereas the Bank also sends real-time SMS alerts for every card transaction. Therefore, the complainant received these alerts but did not contact the Bank to report any unauthorised activity or to object to the transactions. This lack of timely objection strongly supports the conclusion that the transactions were voluntarily initiated and authorised by the Complainant, and the Bank acted in accordance with its contractual obligations;*

13. *Whereas the Bank respectfully submits that the complainant was an active participant in the disputed transactions. He was fully aware of the amounts being transferred, the recipients and the platforms involved. The use of remote access software and engagement with the investment scheme were deliberate actions by the complainant.*

[10] Ibid.
[11] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
[12] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
[13] P. 50 - 51

The Bank reserves the right to substantiate this position with technical logs, device enrolment records and transaction metadata.

14. *Whereas reference is made to Article 40(1) of Directive No. 1 of the Central Bank of Malta ("CBM Directive 1"), which transposes PSD2 into Maltese law. Such article establishes that a payment transaction is deemed authorised only if the payer has given consent to execute it. In the case at hand, the Bank received instructions through secure credentials and systems associated with the complainant, thereby satisfying the requirements at law for authorisation. It must be emphasised that the Bank acted in good faith and in accordance with its legal and contractual obligations:*

> *"40. (1) A payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction.";*

15. *Whereas in relation to the 24x7 transactions made by the claimant, apart from SCA, the Bank also implements a system of 'dynamic linking' as required under Article 5 of Commission Delegated Regulation (EU) 2018/389, which supplements PSD2, ensuring that the authentication code is uniquely tied to the transaction amount and the identity of the payee. This means that any change in the transaction details would invalidate the authentication code, thereby preventing manipulation:*

> *"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."

16. *Whereas the Bank maintains robust fraud detection and transaction monitoring systems, as required under Articles 2 and 18 of the Commission Delegated Regulation, which include real-time monitoring, risk scoring, and escalation protocols;*

17. *Whereas as will be explained throughout the proceedings, in the present case, it is pertinent to state that:*

    i. Certain transactions were declined due to exceeding the Card daily limit or failing SCA rules;

    ii. Two transactions were flagged by the Bank's system due to high-risk scores and were restricted;

    iii. Three additional attempts triggered alerts and were escalated to a Bank analyst who subsequently attempted to contact the complainant and even requested him to revert back, however, to no avail;

    iv. SMS alerts were sent to the complainant for all transactions;

18. Whereas these actions demonstrate that the Bank's systems were functioning as intended and that it took reasonable and timely steps to mitigate potential fraud;

19. Whereas the complainant's own actions contributed to the loss suffered by him;

20. Whereas the complainant admits to installing TeamViewer and granting remote access to his device:

> "*Following this initial transaction, [the Complainant] was contacted by another individual claiming to represent the same platform, who instructed him to download a mobile application, and [the Complainant] adhered to his request. This app was 'TeamViewer' a remote access software, designed to grant third parties direct control over his mobile device.*"[14]

This action, whether intentional or otherwise, constitutes a serious breach of personal security and enabled third parties to access his banking credentials and authorise the transactions;

21. Whereas under Recital 72 of the PSD2, the burden of proof lies with the Bank to demonstrate either fraud or gross negligence by the use and in this regard, the Bank respectfully submits that granting remote access to unknown third parties, failing to report suspicious activity immediately despite receiving SMS alerts, and not contacting the Bank until after the transactions were completed, collectively amount to gross negligence, thereby shifting liability unto the complainant.'[15]

BOV spjegaw li l-pagamenti li saru fil-kont tiegħu ma' Revolut ma jistgħux jagħmlu talba għar-rifużjoni tagħhom għax dawn marru fil-kont tiegħu stess, u jekk minn hemm marru x'imkien ieħor huma Revolut li jridu jagħmlu 'recall' bħal dan.[16]

[14] Fol. 003 of the complaint.
[15] P. 52 - 54
[16] P. 101

Bagħtu wkoll lista tat-tranżazzjonijiet li saru mill-kont tal-*card* fiż-żmien imsemmi li juri li BOV permezz tas-sistema ta' moniteraġġ ta' pagamenti waqqfu diversi pagamenti jew għax ma kienx hemm awtentikazzjoni tajba, jew għax kien qed jinqabeż il-limitu tal-ammont ta' pagamenti jew għal raġunijiet tekniċi oħra fil-moniteraġġ li joħroġ riżultat ta' *risk score* għoli.[17]

Seduti

Inżammu żewġ sessjonijiet ta' smigħ.

L-ewwel seduta tad-29 t'Ottubru 2025[18] kienet għall-provi tal-Ilmentatur u l-kontroeżami dwar ix-xhieda tiegħu.

Huwa qal:

'Ngħid li l-ironija hija din. Jien qatt ma rċevejt la t-3D Secure u lanqas informazzjoni mill-bank li qed jitteħduli l-flus. Flus li jiena m'awtorizzajtx biex inħallas. Qatt ma rċevejt; m'għandi l-ebda indikazzjoni li kienu qed jitteħduli l-flus. Li kieku ma ħsibtx ħażin jiena, u fl-għaxija meta mort id-dar dħalt fl-Online Banking, kieku jien ma kontx inkun naf li tteħduli l-flus.

Ngħid li hemm xi ħaġa ħażina fil-BOV li lili mhux qed jinfurmawni.

Nikkonferma li l-ewwel pagament li għamilt fil-25 t'Ottubru 2023 kien dak ta' €500. Ma nistax ngħid bl-eżatt meta mort id-dar niċċekkja u sibt li ħaduli l-flus mill-kont. Naħseb li kien it-2 jew it-3 ta' Novembru u mort inwaqqaf il-VISA Card immedjatament.

Nikkonferma li meta dħalt u ndunajt li tteħduli l-flus, kienu diġà saru l-pagamenti kollha. U jiena qatt ma rċevejt notifikazzjoni mill-bank, bit-3D Secure.

Meta mort il-bank għidtilhom, 'Waqqfu din il-VISA immedjatament għax ġejt hacked.'

U bagħtuli VISA Card oħra xi erbat ijiem wara.

Ngħid li fil-passat, qabel dan l-avveniment t'Ottubru 2023, it-tranżazzjonijiet li kont nagħmel huma baxxi ħafna għaliex jiena naħdem fuq classic cars u daqqa nġib xi spare part 'l hawn u daqqa spare part 'l hinn u l-ammonti huma żgħar

[17] P. 71 - 72
[18] P. 102 - 108

ħafna. Fil-fatt, għandi erba' tranżazzjonijiet li saru bejn is-6 t'Awwissu 2025 u s-7 ta' Settembru 2025 li jammontaw għal €61.34, €102.87, $25 u $25 oħra. U dawn qatt ma ġejt avżat mill-bank, bit-3D Secure, jew b'email. Kont naf li l-ordni għaddiet, għax bagħtuli konferma mingħand min ordnajt. U vera rċevejthom il-parts.

Ngħid li jiena qatt ma għamilt tranżazzjonijiet fuq cryptocurrencies. Dik kienet l-ewwel darba u spiċċajna ħażin. Ngħid li qatt ma għamilt tranżazzjonijiet fuq cryptocurrencies jien; għamilt dik id-darba għax rajt Elon Musk u daħku bija.'[19]

Fil-kontroeżami, l-Ilmentatur qal:

'Mistoqsi meta nstallajt it-Team Viewer jekk iċċekkjajtx għalxiex jintuża, ngħid li jien qatt ma nstallajt it-Team Viewer għax li kieku ssemmiet il-kelma 'Team Viewer', jien kont naf x'inhi Team Viewer u qatt ma kont ser nagħmilha t-Team Viewer. Ma tarax! Imma semma' xi kelma oħra. Xi app oħra li apparentement kienet bħat-Team Viewer. Imma jiena qatt ma smajt biha din l-app.

L-Arbitru qed jiġbed l-attenzjoni għall-fatt li fl-ilment jien speċifikament ktibt li l-app kienet it-Team Viewer, u li issa qed ngħid li kienet xi ħaġa oħra u mhux Team Viewer.

Ngħid li kienet bħal Team Viewer imma ma konniex nafu biha.

Mistoqsi mill-Arbitru kinitx 'AnyDesk', ngħid li jiddispjaċini imma assolutament ma niftakarx.

Dr Ian Barbara jintervjeni biex jikkonferma li hemm bżonn korrezzjoni fl-ilment għax l-Ilmentatur jaf x'inhi Team Viewer u li kieku qalulu biex iniżżel l-app tat-Team Viewer, ma kienx jaċċetta li jagħmel Team Viewer fuq il-mobile.

L-Arbitru jiddikjara li qed jieħu nota ta' din il-korrezzjoni fl-ilment.

Mistoqsi għalfejn m'għamiltx xi verifiki jekk ma kontx naf x'inhi din l-app, ngħid li jien ma kontx naf li dan kien ser jidħolli fuq il-mobile. Ngħid li ma kontx naf x'inhi.

Qed jingħad li minkejja ma kontx naf x'inhi din l-app, jien xorta għamilt download tagħha.

[19] P. 103 - 104

Ngħid li għamilt download ta' din l-app għax ma kontx naf li ser jidħol fuq il-mobile tiegħi. Jien ħsibtu biex jikkomunika miegħi. Ma kontx naf assolutament x'inhi din l-app.

Ngħid li ma kellix ċans niċċekkja x'kienet din l-app. It was too late! Jien kien moħħi biex nirkupra l-flus li ħriġt.

Mistoqsi għamiltx xi verifiki fuq il-persuna li tkellmet miegħi, ngħid li m'għamilt xejn għax jien kien mingħalija li dik kienet is-site ta' Elon Musk. Ma kellix x'nivverifika.

Mistoqsi ġejtx b'xi mod mhedded jew imġiegħel biex ninstalla din l-app, ngħid li le, jien għażiltha.

Mistoqsi għamiltx kollox minn jeddi, ngħid eżattament.

Ngħid li l-persuni li kont qed nikkuntattja magħhom identifikaw ruħhom bħala impjegati tal-bank ta' Elon Musk. Ngħid li mhux tal-BOV, ta' Elon Musk.

Ngħid li jien mhux ma fhimtx xi bdew jistaqsuni; ma fhimtx il-kumplessità ta' xi trid tagħmel biex tidħol f'din il-cryptocurrency investment. Hemmhekk għidtlu biex iwaqqaf kollox għax ma ridtx naf. Ma ridtx dawn l-affarijiet.

Mistoqsi meta jien tajt depożitu ta' €500 u bdew il-kuntatti jekk kellix biżżejjed ħin biex nagħmel xi verifiki, ngħid li malli ddepożitajt il-€500, bdew iċempluli huma.

Mistoqsi kellix il-mobile f'idejja meta bdew jitteħduli l-flus, ngħid li meta bdew jitteħduli l-flus ma stajtx nara, nidħol fuq il-laptop.

Ngħid li meta daħluli fuq il-mobile, bdejt nara l-iscreen sejjer 'l hemm u 'l hawn. Qatt ma rajtu jiċċaqlaq daqshekk. Dik biss. U ma kelli xejn biex nara x'inhu jiġri.

Mistoqsi rajtux dieħel fuq l-apps, ngħid li assolutament le għax kieku kont nitfi l-mobile.

Let's say, jien kelli ċans ninduna li daħal fuq il-BOV fuq l-accounts, kieku nitfi l-mobile immedjatament. Imma dawn in-nies tant huma ħallelin serji illi trid tkun ħalliel bħalhom biex tinduna.

Mistoqsi rċevejtx xi SMS mill-bank wara li għamilt il-€500 deposit, ngħid li le. Dik hi l-problema li jien qatt ma rċevejt li tajt €500 deposit. Ngħid li kont irċevejt telefonata mill-platform tas-suppost Elon Musk.

Mistoqsi rċevejtx meta bdew jitteħduli l-flus, ngħid li jiena, peress li ħallast bil-VISA Card, mort filgħaxija d-dar fuq il-laptop, dħalt fuq l-Online Banking, u meta ndunajt li l-VISA Card ġiet hacked, li ħaduli l-flus mill-VISA Card, kważi ħaduli l-maximum tal-VISA Card, għidt, 'Le, dan qed jeħodli l-flus mhux qed jagħtini l-flus!' Ngħid li dak il-ħin, ċempilt lill-BOV u avżajthom u waqqfu immedjatament il-VISA Card.

L-għada, mort il-bank, qattgħuli l-card u qaluli li ser nirċievi oħra within two or three days. U hekk ġara.

Mistoqsi inix familjari mat-termini u kundizzjonijiet tal-BOV, ngħid li ma tantx jien familjari. Nixtieq li kont familjari għax kieku dan ma ġarax.

Qed jingħad li aktar kmieni f'din is-seduta, meta kont qed nispjega l-verżjoni tiegħi, għidt li filgħaxija wara li saru dawn it-tranżazzjonijiet u jien ma kontx naf, filgħaxija kelli xi suspett u hemmhekk dħalt fuq l-Internet Banking u ndunajt li tteħduli l-flus.

Mistoqsi x'wassal għal dan is-suspett, ngħid peress li ħallast bil-VISA Card u tajthom id-dettalji kollha tal-VISA Card, għidt, 'Ilallu, dan jista' jeħodli l-flus mill-VISA Card!' U hekk kien għax kif dħalt indunajt li ġew meħudin ħafna flus minnha. U din li ma nistax nifhem, li mingħajr l-awtorizzazzjoni tiegħi.

Qed jingħad li jien kont konxju li tajthom xi dettalji. Ngħid li fuq is-site, trid tagħti d-dettalji tal-VISA Card biex huma jieħdu l-pagament bħalma qisni qed nixtri xi spare part. Dan li ġara.

Ngħid li jiena dejjem ħallast bil-VISA Card.

L-Arbitru għandu bżonn xi kjarifiki mill-Ilmentatur u jixtieq konferma ta' dak li qed jifhem:

Li l-ewwel pagament l-Ilmentatur għamlu fil-25 t'Ottubru ta' €500 jew €499; mela d-dettalji tal-card imma ma ntalab jagħmel l-ebda awtorizzazzjoni oħra; m'għaddiex mit-3D Secure biex jawtorizza t-tranżazzjoni.

[L-Ilmentatur] iwieġeb:

Ngħid li xejn. Ma rċevejt xejn lanqas informazzjoni li jiena bgħatt dawk l-€499.

L-Arbitru jkompli:

Imbagħad, jirriżulta, fil-ġranet ta' ftit wara, mit-30 t'Ottubru sal-1 ta' Novembru, jiġifieri fi tlett ijiem, saru ħafna pagamenti li jammontaw għad-

€9,000 li qed jikklejmja l-Ilmentatur, li għalihom la awtorizzahom l-Ilmentatur, la għamel it-3D Secure u lanqas irċieva SMS mill-bank.

[L-Ilmentatur] iwieġeb:

Kif qed tgħid inti eżatt, Onorabbli. Qatt ma rċevejt xejn. Nikkonferma li fhimtni, Onorabbli.

L-Arbitru jkompli:

Fi stadju minnhom, dakinhar jew f'dawk il-ġranet, l-Ilmentatur beda jara l-mobile jilgħab u jassumi li dan kien fit-30 t'Ottubru, fil-31 t'Ottubru u fl-1 ta' Novembru, għax il-pagamenti f'dawn il-ġranet jidhru li kienu saru.

[L-Ilmentatur] iwieġeb:

Il-mobile beda jilgħab meta suppost il-Financial Controller kien qed jitkellem miegħi fit-30 t'Ottubru, fil-31 t'Ottubru u fl-1 ta' Novembru. Ngħid li jiena mort niċċekkja fit-2 jew fit-3 ta' Novembru meta kien sar kollox. In the meantime, waqqaft il-VISA Card. X'għamel? Daħalli fuq l-accounts tal-bank u ħadli l-flus minn żewġ accounts tiegħi.

L-Arbitru jkompli:

L-Ilmentatur waqqaf il-VISA Card għax avża lill-bank li kien hemm xi ħadd qed jilgħab magħha, però, meta waqqaf il-VISA Card, imbagħad, il-pagamenti bdew isiru mill-kontijiet tiegħu.

[L-Ilmentatur] iwieġeb:

Ngħid li iva, beda jeħodli l-flus mingħajr ma ninduna.

L-Arbitru jistaqsi jekk meta waqqaf il-VISA Card, l-Ilmentatur ċempilx jew mar il-bank.

[L-Ilmentatur] iwieġeb:

Ngħid li filgħaxija ċempilt il-bank u l-għada filgħodu mort il-bank. Irrapportajt li xi ħadd qed jisraqli l-flus.

Naħseb li mort il-bank fit-2 jew fit-3 ta' Novembru. Naħseb aktar fit-2 ta' Novembru.

Ngħid li kienu diġà ħaduli kollox. Ngħid li mhux mill-card biss kienu ħaduli.

Mistoqsi mill-Arbitru għaliex ma mortx il-bank fit-30 t'Ottubru, ngħid li għax kont għadni ma ndunajtx. Kien għadu għaddej il-proċess. Kont għadni ma rrealizzajtx li qed jeħodli l-flus. Jien kont mingħalija li dan ser jibgħatli l-flus lura.

Mistoqsi jekk fit-30 t'Ottubru l-mobile bediex jilgħab, ngħid li iva, beda jilgħab.

Mistoqsi għalfejn ma mortx il-bank dakinhar, ngħid li għax ma rrealizzajtx mill-ewwel. Dak li ġara!

Ngħid li meta dħalt fl-Internet Banking sibt il-flus neqsin kemm mill-VISA Card u kemm mill-bank accounts tiegħi.

Ngħid li, iva, kien wara l-1 ta' Novembru, naħseb kien fit-2 ta' Novembru.

Mistoqsi jekk dak iż-żmien kellix diġà kontijiet ma' Revolut u ma' Wise, ngħid li Wise qatt ma smajt bihom. Imma ma' Revolut, iva.

Ngħid li l-Wise fetħu l-iscammer.

Qed jingħad li biex l-iscammer fetaħ il-Wise, jien tajtu xi kopji tal-ID Card. Ngħid li jien ma tajtu xejn.

Mistoqsi staqsinix għal ritratt tal-passaport, ngħid li hu qalli li hemm bżonn nieħu ritratt imma ma qallix għalxiex. Ir-ritratt ħadu, iva.

Ngħid li le, ma talabnix passaport.

Ngħid li meta jien ktibt lill-Wise u għidtilhom x'ġara u x'ma ġarax, qaluli, 'M'hawn l-ebda kont tiegħek hawnhekk.' U semmieli isem qisu Afrikan. Qalli l-flus qegħdin f'isem dan it-tali. U jien ħadt nota u nista' nsibu x'isem tani.

Ngħid li jien m'għandix statement ta' Wise.'[20]

Fit-tieni seduta li saret fit-13 ta' Novembru 2025,[21] l-Arbitru talab konferma mingħand l-Ilmentatur li huwa ma kellux kont ma' WISE peress li dokumenti[22] annessi mar Risposta tal-Bank juru li kellu kont f'ismu ma' WISE.

L-Ilmentatur qal li dan fetħu l-iscammer u mhux hu u reġa' kkonferma li qatt ma bagħat kopja tal-ID card lill-iscammer.

[20] P. 104 - 108
[21] P. 165 - 170
[22] P. 78 - 83

Sostna li anke t-trasferimenti ta' €2,900 u €3,200 mill-kontijiet normali tiegħu għall-kont tal-card għamilhom l-iscammer u mhux hu.

Xehdet Sandra Stevens, imressqa mill-BOV li qalet:

'Ngħid li jiena responsabbli mill-Card Fraud Section u t-Transactions Monitoring ġewwa l-Bank of Valletta. Ilni naħdem fil-Cards għal 29 sena u ili nokkupa r-rwol ta' Manager tal-Fraud Section għal tmintax-il sena.

Ngħid li jiena familjari mal-każ tal-Ilmentatur.

Nikkonferma li bgħatna SMS għal kull tranżazzjoni li saret f'dan il-każ inkluż id-depożitu inizjali ta' €499.

<....>

Ngħid li dawn it-tranżazzjonijiet għaddew bit-3D Secure ukoll. Ngħid li l-enrolment tal-card tal-Ilmentatur kienet saret f'Novembru 2022, jiġifieri kienet diġà eżistenti.

Ngħid li t-tranżazzjoni ta' €499 għaddiet ukoll bit-3D Secure.

Ngħid li l-ewwel parti <....>.

Ngħid li t-transaction details nirċevuhom fis-sistema u jkun hemm indicators fil-log tat-tranżazzjoni li jindikaw humiex 3D Secure jew le.

Ngħid li l-bank juża <...>.

Is-sistema talloka <....>.

Ngħid li f'dan il-każ <.....>.

Ngħid li l-SCA tfisser Strong Customer Authentication. Hemm regoli fis-sistema tal-bank li fi tranżazzjonijiet partikolari l-SCA trid tintalab. Jekk dik tkun nieqsa fit-transaction request, din tiġi declined. Eżempju, kien hemm tnejn minnhom ġew declined għax l-SCA kienet neċessarja.

Kien hemm tnejn minnhom li <....>.'[23]

Waqt il-kontroeżami xehdet:

'Mistoqsija s-sistema taqbadx it-tranżazzjonijiet fl-ammonti li saru li ma kinux fil-patterns normali tal-klijent, ngħid li l-użu tal-card huwa wieħed mill-fatturi

[23] P. 166 - 168

li jiġi kkunsidrat meta s-sistema tal-Visa talloka r-risk score. Ir-risk score jiġi ikkalkolat b'diversi fatturi. L-użu huwa wieħed biss. Fattur ieħor huwa l-authentication tat-tranżazzjoni. Jekk hi 3D Secure dik ser tbaxxi r-risk score.

Mistoqsija f'dan il-każ ġiex evalwat il-pattern tat-tranżazzjonijiet tal-[Ilmentatur], ngħid li ġie evalwat meta ġie kkalkolat ir-risk score.

Mistoqsija x'irriżulta, ngħid li ħafna mit-tranżazzonijiet kellhom risk score baxx minħabba l-authentication.

Qed jingħad li fl-istess ħin jien għidt li kien hemm oħrajn li kellhom riskju għoli u li dawn twaqqfu.

Ngħid li tnejn biss kellhom riskju għoli u skont is-set rules li għandna, dawn ġew declined mill-ewwel.

Nikkonferma li dawn saru fl-istess perjodu bejn il-31 t'Ottubru u l-1 ta' Novembru.

<....>

Mistoqsija meta kien hemm tentattiv min-naħa tal-bank biex jikkuntattja [lill-Ilmentatur] hemm log li l-bank ċempel imma ma qabadx din it-telefonata, jekk il-bank reġax ipprova jikkuntattjah, ngħid li għandi nota li ppruvaw iċemplulu fl-1 ta' Novembru f'11:29 a.m.

Mistoqsija meta ġew imwaqqfa dawk it-tranżazzjonijiet ta' riskju għoli meta saru, ngħid li dawk saru fl-1 ta' Novembru. Ippruvaw iċemplulu wara li kien hemm dawk l-attempts u ġew declined.

Mistoqsija f'liema ammonti kienu dawk l-attempts, l-Arbitru jintervjeni biex jinforma li l-informazzjoni qiegħda fis-Schedule f'paġna 71 mar-Risposta tal-Bank of Valletta fejn turi li kien hemm żewġ pagamenti ta' €5,000-il wieħed favur Revolut li ġew declined għar-raġuni li ma kellhomx Strong Customer Authentication u dawn kienu bejn 10:47:48 a.m. u 10:47:59 a.m.

Il-bank ċemplulu f'11:29 a.m. meta dawn saru fil-ħin ta' 10:47 a.m.

Kien hemm pagament ieħor ta' €100.47 lil Wise li ġie declined fl-istess ħinijiet u wara nofs siegħa jidher li l-bank ipprova jċempillu.'[24]

[24] P. 168 - 169

Analiżi 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 jinvolvi żewġ aspetti:

1. Jekk il-pagamenti ilmentati kinux verament awtentikati u awtorizzati mill-Ilmentatur li b'negliġenza grossolana awtorizza lill-frodist biex ikollu aċċess sħiħ għall-kontijiet tiegħu mal-Bank, u jagħmel dawn il-pagamenti b'mod li l-Bank kellu għax jaħseb li dawn kienu pagamenti normali awtorizzati mill-Ilmentatur.

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

Dan il-każ ma jinkwadrax mal-ilmenti li għalihom l-Arbitru ħareġ mudell dwar kif għandha tiġi allokata r-responsabbilità bejn l-Ilmentatur 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-responsabbilità 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' tlett ijiem u ma kienx hemm relazzjoni ta' kunfidenza bejn il-vittma u l-frodist.

Jekk l-Arbitru jsib li ma kienx hemm negliġenza grossolana min-naħa tal-Ilmentatur skont il-preamboli 71 u 72 ta' PSD 2 (Directive EU 2016/2366) (riprodotti hawn taħt), allura, l-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, jirriżulta lill-Arbitru li l-Ilmentatur wera negliġenza grossolana, allura, jieħu kundiserazzjoni wkoll tat-tieni punt.

Kunsiderazzjoni dwar jekk kienx hemm negliġenza grossolana mill-Ilmentatur

L-Ilmentatur ammetta żewġ affarijiet ta' ċertu importanza:

a. L-ewwel investiment ta' €499 għamlu minn jeddu u, fil-fatt, dan ma jiffurmax parti minn dan l-ilment. Iżda qal li dan xorta ma ġiex awtorizzat bit-3D Secure u, allura, xorta ma kienx kopert bi Strong Customer Authentication (SCA) skont artiku 97 tal-PSD 2, li jgħid:

'*Article 97*

Authentication

1. *Member States shall ensure that a payment service provider applies strong customer authentication where the payer:*

(a) accesses its payment account online;

(b) initiates an electronic payment transaction;

(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. *With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.*

3. *With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.*

   …

Artiklu 4(30) tal-istess direttiva jiddefenixxi SCA:

> *'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'.*

b. L-Ilmentatur jammetti li huwa min jeddu niżżel fil-mobile tiegħu l-App, 'TeamViewer', deskritta bħala '***remote access software designed to grant third parties direct control over his mobile device'.***[25]

   Fil-proċess ħareġ li l-Ilmentatur ma kienx ċert dwar l-isem tal-App,[26] iżda li jgħodd huwa li permezz ta' din l-App ta aċċess lill-frodist biex jippersonafikah u jagħmel tranżazzjonijiet f'ismu fuq il-kont daqslikieku kien hu stess.

Min-naħa tal-Bank, fix-xhieda ta' Sandra Stevens, ġie sostnut li l-pagamenti kollha kienu saru bit-3D Secure (inkluż l-ewwel pagament ta' €499) u, għalhekk, il-BOV kien konformi mar-regolament tal-PSD 2 rigward SCA. Qalet ukoll li għal kull pagament li sar inbaghat SMS fuq il-mobile reġistrat tal-Ilmentatur biex jinfurmah bil-pagament u jgħidlu jċempel numri tal-Bank apposta jekk dan mhux kif ġie awtorizzat minnu.[27]

Fix-xhieda tiegħu, l-Ilmenatatur baqa' jsostni li huwa ma rċeviex SMS u ma awtorizzax il-pagamenti bit-3D Secure. Iżda, filwaqt li ammetta li waqt li kienu għaddejjin dawn il-pagamenti frawdolenti, il-mobile beda jilgħab u ma setax

[25] P. 3
[26] P. 104
[27] P. 54; 166

jidħol bil-laptop,[28] kien biss wara li saru l-pagamenti ilmentati kollha filgħaxija tal-1 ta' Novembru 2023 li nduna bil-frodi u ċempel lill-Bank u filgħodu mar waqqaf il-card.[29]

L-Arbitru jsib li hemm ferm aktar probabbilità fil-verżjoni tal-BOV li l-pagamenti saru kollha bil-kunsens tal-Ilmententur anke jekk dan il-kunsens fir-rigward tal-pagamenti ilmentati (eskluż l-ewwel pagament ta' €499 li mhux parti minn dan l-ilment) kienu potenzjalment ivvizzjati mill-aċċess li l-Ilmentatur ta lill-frodist biex jagħmel tranżazzjonijiet f'ismu fuq il-kontijiet tiegħu mal-Bank.

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-Ilmentatur ta aċċess għall-kont tiegħu biex terzi frodisti jkunu jistgħu jippersonafikawh mal-Bank, allura, neħħa kull protezzjoni li joffri l-Bank permezz tal-SCA la l-frodist seta' huwa stess japprova n-notifiki ta' 3D Secure.

Huwa stramb ukoll li waqt li kien għaddej dan il-frodi, fi tlett ijiem bejn it-30 t'Ottubru u l-1 ta' Novembru, l-Ilmentatur ammetta li ma setax jaċċessa l-kont bil-laptop u beda jara l-mobile jilgħab u jara l-iscreen tal-mobile sejjer 'l hawn u 'l hemm,[30] iżda ma għamilx kuntatt mal-BOV biex jara x'kien qed jiġri. Jekk kien qed jistenna li dawn jirrifondulu l-ewwel pagament li għamel żgur li kellu jqajjem suspett li kien hemm xi ħaġa mhux soltu fil-kont tiegħu u kien jimmerita kuntatt mal-Bank.

Diffiċli l-Arbitru jaċċetta li huwa niżżel l-App Teamviewer biex ikun jista' jirċievi lura l-ewwel pagament li kien għamel meta l-Ilmentatur stess kien konsapevoli li biex tirċievi l-flus ma għandek bżonn l-ebda App.[31]

L-Arbitru jsib ukoll nuqqas ta' kredibilità fix-xhieda tal-Ilmentatur li biex fetħulu kont ma' Wise kien biss aċċetta li l-frodist jeħodlu ritratt u ma bagħatx kopja tal-

[28] P. 105
[29] P. 107
[30] P. 103; 105
[31] P. 103

ID card jew awtentikazzjoni oħra. Hemm evidenza ċara li l-kont ma' WISE kien f'ismu u mill-kont ta' WISE, il-flus marru f'xi kont ieħor f'ismu.[32]

M'huwiex konċepibbli li istituzzjoni bħal WISE tiftaħ kont f'isem xi ħadd bla ma jkollhom dokumenti ta' awtentikazzjoni bħal ID card jew passaport.

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

Obbligi tal-Bank dwar moniteraġġ ta' pagamenti

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

> '*Nota 4: PSP (inkluż banek) huma obbligati li jkollhom sistemi effettivi ta' sorveljanza ta' pagamenti biex jipproteġu 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.*[33]
>
> *Dan jipprovdi fl-artikolu 2(1) li:*
>
> > ***"Il-fornituri ta' servizzi ta' pagament għandu jkollhom fis-seħħ mekkaniżmi li jimmonitorjaw it-tranżazzjonijiet li jippermettulhom jaqbdu tranżazzjonijiet tal-pagament mhux awtorizzati jew frodulenti ... Dawn il-mekkaniżmi għandhom ikunu msejsa fuq l-analiżi tat-tranżazzjonijiet tal-pagament, filwaqt li jqisu elementi li huma tipiċi tal-utent ta' servizzi ta' 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-tranżazzjonijiet:*

[32] P. 76 - 83
[33] https://eur-lex.europa.eu/legal-content/EN-MT/TXT/?from=EN&uri=CELEX%3A32018R0389

a. *Listi ta' elementi tal-awtentikazzjoni kompromessi jew misruqa;*

b. *L-ammont ta' kull tranżazzjoni 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'ħin reali' u solitament isir 'wara' l-eżekuzzjoni tat-tranżazzjoni ta' pagament. Għadu ma ġiex definit kemm wara, imma ovvjament għal kwalunkwe valur reali ta' tali mekkaniżmi, d-differenza bejn il-ħin 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 jħallas."***

F'dan il-każ partikolari jirriżulta li:

- Il-pagamenti ilmentati saru fuq medda ta' tlett ijiem.

- Skont 'DOC A' anness mar-Risposta tal-BOV,[34] matul dawn it-tlett ijiem il-Bank waqqaf dawn il-pagamenti:

    a. 30.10.2023 @ 5:16:37 pm € 5000 Nevada Simplex – Reversed

    b. 01.11.2023 @ 10:47:48 am € 5,000 Revolut – SCA required

    c. 01.11.2023 @ 10:47:59 am € 5,000 Revolut – SCA required

    d. 01.11.2023 @ 10:52:23 am € 100.47 Wise – suspected fraud

    e. 01.11.2023 @ 11:19:41 am € 2,500 Nevada Simplex – Reversed

    f. 01.11.2023 @ 11:27:54 am € 2461.52 Wise – daily limit

    g. 01.11.2023 @ 11:27:55 am € 2461.52 Wise – daily limit

    h. 01.11.2023 @ 3:39:33 pm € 2100 Binance – daily limit.

- 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-Ilmentatur bit-telefon u qalulu anke biex iċempel lura iżda kien kollu għalxejn.[35]

In vista ta' dan, l-Arbitru jidhirlu li l-Bank għamel moniteraġġ ta' pagamenti effettiv li, fil-fatt, ipprevena milli l-Ilmentatur jinkorri telf akbar.

Deċiżjoni

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

Alfred Mifsud
Arbitru għas-Servizzi Finanzjarji

[34] P. 71 - 72
[35] P. 54; 168

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