

Quddiem l-Arbitru għas-Servizzi Finanzjarji

Każ ASF 157/2024

HJ

(‘l-Ilmentatriċi’)

vs

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

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

Seduta tal-31 ta’ Jannar 2025

L-Arbitru,

L-ilment

Ra l-Ilment¹ magħmul kontra l-BOV dwar ir-rifjut li jirrifondi ammont ta’ €2,170.79² rigward pagamenti li saru mill-kont li l-Ilmentatriċi għandha mal-Bank abbinat mas-sistema *PayPal* permezz tal-*Visa Card* li tispicċa bin-numri 5308. Dawn il-pagament kienu mferrxa fuq 16-il tranżazzjoni li seħħew nhar it-13 ta’ Lulju 2024 bejn il-ħin ta’ 13:11:03 u 21:27:52, f’affari ta’ madwar 8 sigħat.

Sitta minn dawn it-tranżazzjonijiet saru dirett lill-*Merchants scammers* għall-valur ta’ €936.79 filwaqt li l-10 l-oħra ġew trasferiti fil-kont tal-Ilmentatriċi ma *Revolut* għall-ammont ta’ €1,234, u minn hemm reġġhu ġew trasferiti lill-istess *Merchants scammers*. Il-medja ta’ dawn il-pagamenti kienet ta’ €135.67, bl-oġġla pagament ikun ta’ €280 lil *Merchant PAYBIS*, u l-inqas ta’ €11 lil *Revolut*.

L-Ilmentatriċi spjegat:

¹ Formola tal-Ilment minn paġna (p.) 1 - 6 b’dokumentazzjoni addizzjonali minn p. 7 - 64.

² Oriġinarjament l-ammont kien dikjarat bħala €2,711.94 issa saret korrezzjoni matul il-proċess.

'I, HJ, holder of ID card XXXXXX, hereby declare that I have been scammed. This happened when I received a fake link claiming to be sent from PayPal. On the 13/07/2023 I pressed this link www.PayPal.com which I had received from this number +1(719)416-0018, and was asked to input my details in order to supposedly link with PayPal, my bank card and bank account.

Subsequently, several transactions were effected and a total to €2,711.94 was withdrawn from my BOV account. These transactions only showed in my bank account on the 15/07/23. I declare that I had never carried out similar transactions with the same frequency before and that I blocked my card after I received a late notification by the bank but it was already too late because the scammers had already managed to carry out multiple transactions in a very short space of time. I believe that the bank's monitoring systems should have flagged the transactions as suspicious and taken timely action to protect me.

I have complained with the provider and held several exchanges in this regard. Unfortunately, however, the financial services provider rejected any liability and has been denying me an effective remedy for more than a year now. I once again reiterate my expectation that the bank should have called me or blocked the card when all of these transactions were going through.'

Bħala rimedju, hemm talba għar-rifużjoni sħiħa tat-telf f'ammont ta' €2,170.79.

Risposta

Ra r-risposta tal-BOV³ fejn qalu:

'Respectfully submits:

- 1. Whereas Ms. HJ ("the complainant") explains that she "received a fake link claiming to be sent from PayPal."⁴ She pressed on this link on the 13/07/2023 which she received from the number +1(719)416-0018 and where she was asked to input her details in order to link her card and bank account with PayPal. She says that "subsequently, several transactions were effected and a total of €2,711.94 was withdrawn from my BOV account."⁵*

³ P. 70 - 74 u dokumenti annessi p. 75 - 83

⁴ Fol. 003 of the complaint.

⁵ Fol. 003 of the complaint.

2. *Whereas on pages 15-16 of her complaint, Ms. HJ attached an extract of her account statement and highlighted the disputed transactions. According to the Bank's calculations, these transactions amount to €2,170.79 and not €2,711.94⁶ as stipulated by the complainant. Therefore, the Bank respectfully requests that Ms. HJ clarifies the disputed transactions, as well as the amount of "€2,7211"⁷ which she states she wants to receive from the Bank in the last part of her complaint, since this amount differs from the €2,711.94 she mentions earlier on in her complaint.*
3. *Whereas it is important to first clarify the method used to approve these transactions. The Bank offers the possibility to customers to enroll their BOV cards on the Apple Wallet or Google Pay. As will be explained further on, Ms. HJ has had her card enrolled on the Apple Wallet of 3 devices. This means that when Ms. HJ wants to make a transaction, she can use the digital card enrolled on her device, instead of presenting the physical card for an in-store payment or entering her card details for an online payment. The below extract was present on the Bank's website at the time Ms. HJ enrolled her card on the Apple Wallet and provides a concise overview of the functions of the service:*

"Bank of Valletta brings its customers Apple Pay

BOV Visa debit and credit card holders can enjoy all the benefits with Apple Pay on iPhone, Apple Watch, iPad, and Mac.

Using Apple Pay is simple, and it works with the devices you use every day. Your card information is secure because it isn't stored on your device or shared when you pay. You can use Apple Pay for any amount of purchase.

Bank of Valletta uses the most advanced payment technologies – EMV and tokenization to ensure the integrity of cardholder information. Security and privacy is at the core of Apple Pay.

When you use a credit or debit card with Apple Pay, the actual card numbers are not stored on the device, nor on Apple servers.

⁶ Fol. 003 of the complaint.

⁷ Fol. 003 of the complaint.

Instead, a unique Device Account Number is assigned, encrypted and securely stored in the Secure Element on your device.”

4. *Whereas with respect to the abovementioned transactions amounting to €2,170.79, the Bank’s records show that these were authorized using Ms. HJ’s token (Unique Device Account Number).*
5. *Whereas article 40(1) of Directive 1 of the Central Bank of Malta (which Directive is based on the PSD2) provides that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. As explained, the Bank received legitimate instructions from credentials associated with the complainant and therefore has no obligation to refund her.*
6. *Whereas the Bank implemented the necessary measures to ensure that its’ systems are secure and in line with the PSD 2 which provides the following on ‘strong customer authentication’:*

‘strong customer authentication’ means an authentication based on the use of two or more elements categorised as **knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is)** that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;⁸

7. *Whereas in this case, strong customer authentication was present because, as will be explained further on, the device used to authorize the transactions was Ms. HJ’s phone, therefore the physical element was present. However, simply having possession of the phone would not have led to the authorization of the transactions. In order for the transactions to be authorized, Ms. HJ needed to approve them using either her passcode (the element of knowledge) or her biometrics (facial recognition or fingerprint, which constitute the element of inherence). Without either of these elements, the transactions would not have been approved.*

⁸ Article 4(30) of PSD2.

8. *Whereas according to the Bank's records, the token used to approve the transactions in question had been registered on an iPhone entitled 'Fran's iPhone' since the 13th of January 2023 as per the attached document marked as 'DOC.A'.*
9. *Whereas in fact, every token registered on a particular device has a unique number associated with it. In fact, the number associated with the token which was used to approve the transactions in question is the same one associated with the token of the complainant which she has previously used to make other payments, which she is not contesting the legitimacy of. This can be seen from the documents attached and marked as 'DOC.B' and 'DOC.C' where 'DOC.B' shows the transactions in question along with the token used to approve them and 'DOC.C.' shows previous transactions, and the token used to approve them. As evidenced by these documents, the token used to approve both sets of transactions were the same.*
10. *Whereas a token number is unique to each device, and even if a customer has the same card registered on the digital wallet of different devices, the token number for each device would be different, even though it is the same customer using the same card. In fact, in this case, Ms. HJ also has her card registered on the digital wallet of her iPad and Apple Watch and the token numbers for these devices are different from each other, as well as from the one registered on her phone. This can be seen from the abovementioned 'DOC.A' where the first column shows the different token numbers for the devices indicated in the third column.*
11. *Therefore, the fact that Ms. HJ had "never carried out similar transactions with the same frequency before"⁹ and thus "the bank's monitoring systems should have flagged the transactions as suspicious and taken timely action to protect me"¹⁰ is an unfounded argument since the transactions were all duly authorized using a device registered in her name which she had previously used to affect transactions of similar amounts. Moreover, the elements of strong customer authentication were satisfied for each transaction.*

⁹ Fol. 003 of the complaint.

¹⁰ Fol. 003 of the complaint.

12. *Therefore, the Bank's system would not stop these transactions since there was nothing suspicious about them and the Bank cannot arbitrarily decide not to process transactions as this would cause great inconvenience to customers. The Bank's practice when such transactions are approved is to send an SMS to customers to inform them that the transactions were affected. In fact, the Bank sent Ms. HJ an SMS for each transaction as they occurred. This can be seen in the attached document marked as 'DOC.D'. Therefore, it is completely unfounded for the complainant to say that she "received a late notification by the bank"¹¹. Moreover, it was Ms. HJ who took delayed action since she called the Bank on the 14th of July at 05:47 to report the fraud.*
13. *Whereas respectfully the Bank submits that the only connection it has with this case is the fact that Ms. HJ used a BOV card to approve the transactions. The Bank has no affiliation with PayPal and does not control how their systems work. Moreover, the Bank is not privy to any communication Ms. HJ made with any third parties in this case. In fact, the number which Ms. HJ received the initial communication from was '+1(719)416-0018'. This number does not belong to BOV, nor does BOV use it to communicate with customers.*
14. *Whereas the Bank makes numerous educational campaigns to raise awareness about the secure use of its' systems. In fact, the Bank also sends direct communications to customers to inform them of fraudulent schemes which imitate its' communication channels (smishing or spoofing). However, it is not reasonably expected for the Bank to send such direct communication about every possible scam which may be circulating. The Bank respectfully submits that the customer certainly has rights and interests, however, they also have a duty to adhere to terms and conditions and need to be aware of the use they are making of the Bank's services.*
15. *Whereas Ms. HJ had the option to decide which merchants to effect payments to and now cannot expect the Bank to bear the responsibility for her actions. The Bank simply provided her with a service to process payments which she herself authorized.*

¹¹ Fol. 003 of the complaint.

16. *Whereas once Ms. HJ communicated with the Bank to report the alleged fraud, the Bank informed her that it would be instituting a chargeback claim for the disputed transactions, however, the transactions affected to Revolut accounts had to be challenged with Revolut directly, thus the Bank informed Ms. HJ of this.*
17. *Whereas the outcome of the Visa Chargeback made by the Bank was not successful since the transactions were authenticated and authorized by the cardholder. Moreover, the merchants stated that they had rendered a service to Ms. HJ and thus the funds could not be retrieved. Once the Bank had the final reply, it informed Ms. HJ and her representative accordingly.*

Conclusion

18. *Whereas in view of the above, the Bank respectfully submits that the Complainant's claims are unfounded in fact and in law.*
19. *Chapter 555 of the Laws of Malta vests the Honourable Arbiter with the authority to decide a case on the basis, inter alia, of the Complainant's legitimate expectations and what he deems fair and equitable in the circumstances of the case. The Bank very respectfully submits that such element of fairness and a customer's legitimate expectations are founded and pivot on a balance between rights and obligations whereby a customer most certainly has rights but also an inherent interest and obligation to faithfully abide with all terms, conditions as well as guidelines issued by the Bank, as these are ultimately intended to serve and protect the customer.*
20. *The Bank reserves the right to bring oral and documentary evidence in order to substantiate the defenses raised in this reply, as well as to make submissions both verbally and in writing pursuant to the provisions of Chapter 555 of the Laws of Malta.*
21. *The Bank reserves all rights/ actions pertaining to it at law, and respectfully requests the Arbiter to reject and dismiss the complaint's claims.*

*With expenses.*¹²

¹² P. 70 - 74

Seduti

Fis-seduta tal-4 ta' Novembru 2024, xehed ir-rappreżentant legali tal-Ilmentatriċi, Dr Mark Muscat fejn qal:

'Bazikament, dan il-każ mhuwiex kwistjoni tal-BOV as such. Però, l-argument huwa dan, illi l-fatti esposti fl-ilment tagħna u l-fatti esposti fir-risposta tal-bank mhuwiex qed jiġu dubitati; dawn kollha ġraw.

Li ġara huwa li hemm diverġenza fl-opinjoni ta' kif ġrat din l-iscam, jiġifieri, filwaqt li l-klijenta tiegħi qed tgħid li bagħtulha email bil-PayPal u mliet xi dettalji u b'xi mod ħadu over is-sistema biex setgħu jiscamjawha, il-bank qed jgħid li intuża device illi kienet awtorizzatu hi bilfors u, allura, hemmhekk, kif ġrat u ma ġratx it's a technical issue illi ma nafx kif wieħed jista' jibni ċertezza kif ġrat u ma ġratx.

Però, l-punt tal-klijenta tiegħi mhuwiex dak. Dak iva, għamlet żball meta tat id-dettalji, però, qed jiġu scammed ħafna nies u forsi m'hawnx daqshekk biżżejjed awareness fis-socjetà fuqhom dawn l-affarijiet. Però, żball min-naħa tagħha sar hemm.

Il-complaint tal-klijenta tiegħi huwa aktar fir-rigward tal-fatt li meta bdew jiġu dawn it-transactions waħda f'waħda, kemm il-klijenta tiegħi u kemm kulhadd jaf li l-bank għandu monitoring system illi kemm-il darba jiffriżawlek il-card u jċemplulek jew jgħidulek biex iċċemplilhom biex jibblokkjawhielek for your own security.

B'dawn l-ammont ta' transactions li ġraw, il-klijenta tiegħi kienet tippretendi li jiġri hekk bħalma jiġri ma' kulhadd u li jiġri spiss.

Ngħid li dan hu l-punt kollu ta' din il-kawża; jien ma rridx nikkumplikaha aktar. Bħala provi, l-aktar l-aktar, nistaqsi lir-rappreżentant tal-monitoring system biex jikkonferma li dan li qed ngħid jiġri għax il-bqija, il-fatti huma li huma. Hemm l-istatements, hemm it-transactions, anke l-bank mhux dak hu d-dubju. Il-punt hu r-responsabbiltà tal-bank li meta ra numru ta' transactions f'dak il-ħin qasir, seta' jibblokkja l-card u jikkonferma mal-klijenta li dawn vera għax kien hemm wisq f'dak il-ħin hekk qasir.

L-Arbitru jgħid li fl-ilment, l-ilmentatriċi qalet li rċeviet link fuq email u qed jitlob lil Dr Mark Muscat biex jipprezenta kopja ta' din l-email.

L-Arbitru jgħid li l-ilmentatriċi, f'paġna 3 tal-ilment tgħid:

'.. after I received a late notification by the bank ...' u jitlob kopja tan-notifications li rċeviet mill-bank partikolarment irid jara x'tip ta' notifications li normalment ikunu notifications li t-tranzazzjoni digà saret imma jixtieq jara l-ħin li rċeviethom peress li f'paġna 83 tal-proċess hemm skeda li turi li għal kull tranzazzjoni intbagħat SMS alert u hemm il-ħin ħdejh u, allura, jikkonferma li dak il-ħin li ntbagħat l-SMS huwa bejn wieħed u ieħor l-istess ħin li rċevietu l-klijenta.

Dr Mark Muscat jgħid li wara l-complaint hu ċċara mal-klijenta tiegħu u fil-fatt, huwa veru li l-SMSes daħlu f'dik id-data, fit-13 ta'Lulju, però, għal xi raġuni rathom l-għada u, allura, skont hi, kienu delayed.

***Ngħid li rċeviet dawn l-SMS alerts bejn wieħed u ieħor fil-ħinijiet li qed jgħid il-bank.'*¹³**

Fil-kontroezami li sar fit-3 ta' Diċembru 2024, l-Ilmentatriċi xehdet:

'Qed niġi mistoqsija x'inhu l-ammont eżatt li qed nikkontesta f'dan l-ilment għaliex fl-ilment issem mew żewġ ammonti u hemm ukoll xi transactions li huma highlighted (paġni 15 u 16 tal-proċess) u jekk tgħoddhom dawn it-transactions ma jammontawx għall-istess ammont li hemm imsemmi fil-bidu tal-ilment.

Qed jingħad li fl-ilment li ktibt lill-Arbitru għidt €2,711.94 u l-Bank of Valletta jgħid li l-ammont ta' dawk it-tranzazzjonijiet li għandhom x'jaqsmu miegħu huwa ta' €2,170.79.

Nikkonferma li l-ammont hu ta' €2,170.79 għax kont għoddejt bi żball tar-Revolut.

Qed jingħad li fl-ilment tiegħi semmejt li rċevejt xi SMS b'link u mistoqsija kellix l-intenzjoni li nillinkja l-kont tiegħi u l-card ma' PayPal, ngħid li qatt ma kelli PayPal u għidt, 'U iva'. Għalhekk blajtha.

¹³ P. 84 - 85

Mistoqsija kellix l-intenzjoni li nagħmilha jew just imxejt mal-passi tal-SMS, ngħid li imxejt mal-passi tal-SMS u, mbagħad, irċevejt l-emails u minn hemm bdiet l-iscam.

Mistoqsija niftakarx x'għamilt meta għafast fuq il-link, ngħid li ġejt directed to PayPal, dħalt fil-PayPal u għamilt l-account tiegħi normali and I connected my BOV credit card to PayPal.

Ngħid li iva, jien familjari ma' kif taħdem id-Digital Wallet tal-Apple Pay, għax nużah on a daily basis.

Ngħid li ġieli użajt u appovajt tranzazzjonijiet biha.

Mistoqsija x'nagħmel is-soltu biex napprova t- tranzazzjonijiet b'din is-sistema, ngħid li skont xi tkun; meta nixtri online, Apple Pay, they ask me for my password u daqshekk.

Ngħid li dakinhar tal-incident, fit-13 ta' Lulju 2023, m'użajthiex f'dan il-każ. Użajt għal xi affarijiet oħrajn u jekk hemm il-lista tat-transactions nista' ngħid liema huma li użajt dakinhar. Niftakar li kont mort il-Persona u kien hemm xi haġa oħra ta' Revolut, imma l-bqija, l-oħrajn le. Ngħid li my phone was hacked because it also happened on Revolut with the Face ID on Apple Wallet.

Mistoqsija s-soltu x'nuża jekk hux il-passcode jew il-Face ID biex napprova t-tranzazzjonijiet, ngħid li r-Revolut huwa bil-password imma l-Apple Pay tista' tużah bil-Face ID jew password.

Mistoqsija inix familjari mat-Terms and Conditions tal-card tiegħi, ngħid skont.

Mistoqsija ġielix qrajthom, ngħid li le, mhux kollha.

Mistoqsija jekk wara li ġara dan l-incident jien għamiltx rapport mal-Pulizija, ngħid li iva. Mistoqsija tawnix xi update, ngħid li jien kont ikkuntattajt il-bank mill-ewwel x'hin irċevejt il-messaġġi, kienu xi s-6.00 a.m., u kont tkellimt ma' Kimberly through emails. Qaltli biex nagħmel ir-rapport u mort nagħmel ir-rapport mill-ewwel. Kulma qaluli x'irrid nikteb fir-rapport. Ktibna kollox

flimkien, urejthom it-transactions u kitbuli r-rapport. U jien bgħatt ir-rapport lil xxx u daqshekk.¹⁴

Fl-istess seduta tat-3 ta' Diċembru 2024, il-Bank ressaq ix-xhieda ta' xxx xxx li qalet:

'Jiena nokkupa r-rwol ta' Manager taċ-Chargebacks Department. Ili nokkupa dan ir-rwol minn Lulju 2022 u ili nagħmel parti minn dan id-dipartiment għal tmintax-il sena.

Ngħid li jiena segwejt il-każ tal-ilmentatriċi u anke kif saru l-investigazzjonijiet rigward dawn it-tranzazzjonijiet.

Nibda billi ngħid li mill-investigazzjonijiet li għamilna mis-sistemi tal-bank, gie kkonfermat li l-ilmentatriċi kellha l-card tagħha enrolled fl-Apple Wallet fuq tliet devices differenti. Kellha l-card enrolled fuq l-iPhone tagħha u l-enrolment sar fit-13 ta' Jannar 2023. Kellha enrolment ieħor fuq l-Apple Watch li sar fl-istess ġurnata u kellha enrolment ieħor fuq iPad. Dan l-enrolment sar fl-20 ta' Marzu 2023.

Kull darba li jsir enrolment fuq device partikolari jiġi ġġenerat token number li huwa assoċjat ma' dak id-device biss. U din ipprezentajniha wkoll fir-risposta tal-bank. Għanda Dokument A fejn jidher li kull token li kien assoċjat mal-iPhone, mal-Apple Watch u mat-tablet, kull darba kien hemm token differenti, jiġifieri, għal ma' kull device kien hemm token differenti.

It-token assoċjat mal-iPhone, jispicċa 7177, u t-tranzazzjonijiet li huma relatati ma' dan il-każ kollha ġew awtorizzati mill-ilmentatriċi mill-iPhone tagħha u huma kollha abbinati ma' dan it-token number li jispicċa 7177.

Aħna pprezentajna wkoll Dokument B fejn juri li kull tranzazzjoni li saret, li għandha x'taqsam ma' dan il-każ, qed juri dan it-token number.

Ngħid li dawn it-tranzazzjonijiet ġew awtorizzati mill-ilmentatriċi u kien hemm l-iStrong Customer Authentication, jiġifieri kull tranzazzjoni ġiet approvata minnha mill-iPhone tagħha dejjem bil-mod li hija għażlet: jew kien passcode, jew kien Facial Recognition jew Fingerprint. Li kieku ma sarx dan it-tip ta'

¹⁴ P. 86 - 87

authorisation għal kull tranżazzjoni, ma kinux jiġu awtorizzati dawn it-tranżazzjonijiet kollha.

L-ilmentatriċi hija familjari ma' dan il-proċess għax ukoll ipprezentajna Dokument C fejn juri li għamlet diversi pagamenti bl-użu tal-iPhone u dawn kollha huma relatati mal-istess token number, jiġifieri dak li jispicċa 7177. Fosthom kien hemm tranżazzjonijiet li għamlet mar-Revolut.

Xi ħaġa oħra li nixtieq insemmi hija li l-bank baġhat SMS għal kull transaction li saret. Kien hemm diversi SMSes wara kull pagament li sar. Baġhatna wkoll Dokument D mar-risposta li juri l-ħinijiet kollha li ntbagħtu dawn it-transactions.

L-ilmentatriċi semmiet diversi tranżazzjonijiet meta fetħet il-claim mal-bank, fosthom, tranżazzjonijiet tar-Revolut li l-bank infurmaha li dawk trid titkellem hi mar-Revolut fuqhom, jiġifieri aħna mill-ewwel spjegajnilha li t-tranżazzjonijiet tar-Revolut trid tikkuntattja hi lir-Revolut biex tagħmel query fuqhom.

Ngħid li dawn it-tranżazzjonijiet kollha saru mid-device tagħha u ġew awtentikati kollha minnha.'¹⁵

Fil-kontroezami kompliet tixhed:

'Qed jingħad li jien semmejt li t-tranżazzjonijiet għamlithom kollha l-ilmentatriċi. Mistoqsija naqbilx li llum il-ġurnata anke l-bank hu familjari ma' scams li jirnexxilhom li jagħmlu hacking anke tal-passcodes, facial recognition, eċċ., li bihom jiġu awtorizzati t-tranżazzjonijiet; li b'xi mod jirreplikawhom u jużawhom.

Ngħid li però, dan mhuwiex il-każ. Hadd ma seta' jagħmel face recognition, pereżempju, fuq il-mobile jekk id-device hu tal-ilmentatriċi u kien qiegħed għandha, jiġifieri dawn it-tranżazzjonijiet ma sarux b'dan il-mod.

Mistoqsija neskludix li xi hadd seta' b'xi mod, pereżempju, identifika l-passcode u beda jużah hu, ngħid li f'dan il-każ ma setax jagħmel hekk għax ried jiġi awtentikat fuq l-istess device.

¹⁵ P. 88 - 89

Ngħid li kull każ li jiġi rridu ninvestigawh separatament, jiġifieri ma nistgħux ngħidu li jista' jkun li ġara xi ħaġa jekk ma tiġix investigata. Li nista' nikkonferma huwa x'ġara fil-każ tal-ilmentatriċi. Ma nistax inpoġġi perspettiva ta' xi ħaġa li mhix relatata mal-każ.

Mistoqsija naqbilx li jien la rajt lill-ilmentatriċi tawtorizzahom dawn u li m'għandi l-ebda evidenza min għamel dawn it-tranzazzjonijiet, ngħid li għandi l-evidenza li hi pprovduta mis-sistemi tal-bank li kollox hu dokumentat u nistgħu niċċekkjaw minnu.

Aħna li qed ngħidu hu li l-klijenta għamlet enrolment tal-card tagħha fl-Apple Wallet; u biex isiru t-tranzazzjonijiet fuq l-Apple Wallet iridu bilfors isiru ċertu affarijiet li l-klijenta biss tista' tagħmilhom. Ma jistax xi ħadd ikollu l-mobile tal-klijenta jekk il-klijenta għandha l-mobile f'idha.

Qed jingħad li jekk xi ħadd b'xi mod jagħmel hacking tal-mobile u jkun jaf il-passcode, ikun jista' jagħmilhom hu.

Ngħid li ma nistax ngħid iva jew le għax dan mhux il-każ. Li nista' nikkonferma hu dak li għandna fis-sistema tal-bank relatat mal-każ tal-ilmentatriċi.

Qed jingħad li l-ilmentatriċi iċċarat li dawk it-tranzazzjonijiet tar-Revolut eskludiethom mill-claim u mistoqsija jekk meta semmejt it-tranzazzjonijiet tar-Revolut kontx qed nirreferi għalihom, ngħid li l-claim tal-ilmentatriċi fil-bidunett qed issemmi madwar €2,000 u xi ħaġa. Ngħid li meta għamlet il-claim magħna semmiet ħafna modi ta' Revolut li allura aħna għidnilha mill-ewwel, jiġifieri, jekk innaqqsu dak l-ammont kollu, l-ammont jiġi ħafna inqas.

Qed jingħad li l-ammont ġie €2,170. Ngħid li, le. Jien qed insemmi t-transactions tar-Revolut li hi semmiet li huma parti mill-claim.

Qed jingħad li l-claim kien €2,711 u fil-verità, ġie €2,170. Ngħid li, le, ġew ħafna inqas; ġew xi €900 u xi ħaġa. U għidnilha mill-ewwel lill-ilmentatriċi.

L-Arbitru qed jitlob kjarifika fuq l-ammont tal-pagamenti li saru bil-card tal-Bank of Valletta.

Dr Mark Muscat jgħid li fis-seduta l-oħra gie stabbilit li fl-*istatement* tal-*Bank of Valletta* qegħdin *highlighted* bl-isfar it-*transactions* li għaddew mill-kont tal-*Bank of Valletta*.

L-Arbitru jirreferi għar-risposta tal-bank fejn hemm miktub li jekk tghoddhom, jiġu €2,170. U issa Ms XXX qed tghid li jekk tghoddhom jiġu ħafna inqas.

Ms XXX tghid li meta kitbu lill-ilmentatriċi qalulha li daww il-pagamenti li hi ħallset lir-*Revolut*, li huma *highlighted* fil-lista, daww riedet tkellem lir-*Revolut* dirett fuqhom.

Mistoqsija jekk dawn il-pagamenti saru mill-*Bank of Valletta* lejn ir-*Revolut*, Ms XXX tghid:

Hekk hu. Hekk awtorizzat l-ilmentatriċi.¹⁶

Xehed ukoll għan-naħa tal-Bank, XXX li qal:

‘Ngħid li jiena XXX u ili fir-rwol kurrenti tiegħi sena u nofs.

Jiena l-lead responsabbli għall-operat tal-bank fuq l-area tal-card payments, però, ili fl-area tal-card payments ferm qabel din is-sena w nofs, jiġifieri, kont involut anke direttament fl-implimentazzjoni tal-monitoring systems li għandna u ili madwar 29 sena fl-area tal-cards.

Ngħid li jien familjari mal-ilment tal-ilmentatriċi partikolarment dwar it-tranzazzjonijiet li qed tikkontesta.

Ngħid li bħala parti mill-kontrolli li għandu l-bank fuq frodi, għandna żewġ livelli ta’ transaction monitoring. Għandna livell li huwa statiku, jiġifieri ibbażat fuq parametri statiči bħalma jistgħu ikunu l-ammont tat-tranzazzjoni, l-industrija minn fejn hi ġejja u, abbażi ta’ dawn ir-regoli, nibgħatu, pereżempju, l-SMSes li klijent jirċievi meta jagħmel it-transaction dejjem skont ir-riskju fuq dik it-transaction skont ir-regoli li għandna fuq din is-sistema.

Apparti din is-sistema, għandna livell ieħor ta’ transaction monitoring li huwa aktar dinamiku u bbażat fuq machine learning, jiġifieri s-sistema tevolvi skont ċertu patterns ta’ frodi li jsiru kemm min-naħa tal-card holders u kemm min-

¹⁶ P. 89

naħa tal-merchants u tieħu feed ukoll mill-actual fraud, jiġifieri sistema li titgħallem kontinwament mill-patterns li jkunu qed isiru fuq is-suq.

Din is-sistema xtrajniha mingħand il-VISA, però, nixtieq nikkjarifika li mhijjex parti mill-membership tagħna tal-VISA. Għażilna s-sistema tal-VISA bħalma stajna għażilna sistemi ta' vendors oħrajn, però, rajna li tal-VISA hija l-aktar waħda sofistikata u l-aktar li għandha access għal data biex tibni risk score sofistikat u reliable.

Il-mod kif taħdem din is-sistema hi, kif għidt, li tieħu input mid-data li kollha li għandha vizibilità fuqha l-VISA, jiġifieri kemm min-naħa tal-card holder, kif ukoll min-naħa tal-merchant. U, ovvjament, il-VISA għandha vizibilità li tmur ħafna oltre minn dak li jista' jara l-bank, jiġifieri l-VISA għandha risk profile ta' kull merchant ibbażat fuq it-traffiku kollu tiegħu u mhux biss dak li jara l-Bank of Valletta. U, abbażi ta' din l-informazzjoni, l-VISA tabbina risk score għal kull tranzazzjoni li tgħaddi.

Is-sistema hija owned mill-bank u mhu qed nagħmlu l-ebda reliance fuq il-VISA. U r-risk appetite u l-parametri li nissettjaw fuq is-sistema, dawk huma kollha parametri li jiddeċiedi l-bank. F'dan il-każ, għandna regoli li 'l fuq minn ċertu score aħna nirrifjutaw it-transaction outright. Dik nimminizzawha kemm jista' jkun u aħna dejjem irridu nsibu bilanċ tajjeb illi ma nwaqqfux transactions illi jkunu legittimi kemm jista' jkun, jiġifieri, għandna monitoring kontinwu fuq il-false positives biex naraw li l-parametri tagħna mhumiex baxxi iżżejjed li naffettwaw tranzazzjonijiet legittimi.

Imbagħad, hemm bracket ta' scores ieħor li ma nwaqqfux it-transactions, però, jidhlu fi queues tagħna biex ninvestigawhom u jekk naraw li hemm bżonn nikkuntattjaw lill-klijent biex nivverifikaw li veru hu qed jagħmilhom.

Fil-każijiet tat-transactions ta' dan il-każ, ir-risk scores li l-VISA assigned kienu ferm inqas minn dawk il-parametri that we follow up on, jiġifieri jekk hemm indikazzjoni li t-transactions ġew, pereżempju, authenticated, dak jaffettwa r-risk score li jingħata u, aħna, l-focus tagħna hu allura fejn m'hemmx authentication, jew dik l-authentication hija suspettuża.

F'dan il-każ ma kienx hemm il-parametri li jqajjmu suspett fuq it-tranzazzjonijiet.¹⁷

Fil-kontroezami, XXX kompli jgħid:

'Mistoqsi naqbilx illi waħda mill-affarijiet li l-monitoring section tagħti kas u tistabbilixxi bħala parameter huwa the number of transactions li jsiru in a short space of time, ngħid li naqbel.

Mistoqsi kontx involut fil-monitoring ta' dan il-każ partikolari, ngħid li jien m'inix involut direttament. Għandna team ta' analysts li jaraw dawn il-queues li ddeskrivejt. Ngħid li l-velocity, il-frekwenza tat-transactions, dak huwa parti mill-parametri tas-sistema li minnu jibni dak ir-risk score li semmejt; huwa wieħed mill-ħafna parametri li jikkontribwixxu għal dak ir-risk score.

Qed jingħad li n-numru ta' tranzazzjonijiet li saru kien sostanzjalment kbir.

Qed niġi mistoqsi naqbilx li bank ġieli waqqaf tranzazzjonijiet li kienu ħafna anqas frekwenti fejn ġieli bblokkja l-card u staqsa lill-individwu jekk kienx hu li qed jagħmilhom.

Qed niġi mistoqsi jekk hix konkluzjoni tajba illi kien hemm parametru ieħor li milli qed nixhed jiena, jidher li kien il-fatt illi kien hemm authentication min-naħa tal-klijent, allura, l-parameters issettjajnihom għoljin ħafna u, għalhekk, ma nqabadx dan il-każ.

Ngħid li aħna żgur li qatt ma nwaqqafu transactions abbażi biss tal-frekwenza tagħhom. Kif spjegajt, l-iscore li jiġi assigned huwa fiss u d-deċiżjoni tagħna tidhol fejn indaħħlu dik il-linja fejn aħna nibdew inwaqqafu t-transactions. Jekk aħna nibdew inwaqqafu t-transactions minn score, pereżempju, ta' 85 'il fuq, dawn it-transactions qatt ma qabżu s-60, jiġifieri kieku aħna kellna nwaqqafu transactions li jidhlu bl-iscores ta' dawn it-transactions, nassigurakom li nkunu qed naffettwaw lil ħafna u nkunu qed inħarbtu s-suq.

Mistoqsi kemm saru transactions f'dan il-każ partikolari, u f'kemm spazju saru, ngħid li m'għandix dik l-informazzjoni fl-immedjat.

¹⁷ P. 90 - 92

Mistoqsi allura kif qed ngħid li l-iscore huwa aktar baxx, ngħid li għax għandi l-iscores ta' kull tranzazzjoni li saret.

Qed jingħad li l-bank qalu li f'dan il-każ partikolari intbagħtu diversi SMSes, wieħed f'wieħed, u mistoqsi jekk din is-sistema meta tara ħafna SMSes, eżempju, xi t-nax-il SMS qed jintbagħtu jkunx hemm a second level of protection, ngħid li t-t-nax-il SMS jikkorrelaw mat-transactions li saru; u t-transactions li saru qed jidhlu biex jinbena dak ir-risk score, jiġifieri, iva.

Mistoqsi meta s-sistema awtomatika ippikkjat il-bżonn li tibgħat SMSes, hemmx xi sistema oħra li mbagħad tiġi a second layer of protection, eżempju, a manual intervention, li tiġbed l-attenzjoni ta' xi ufficjal u jieħu xi deċiżjoni x'għandu jagħmel jew nieqfux b'din is-sistema biss, ngħid li din spjegajtha qabel: għandna score li minnu 'l fuq, we decline outright but it is rare for the bank to decline outright għaliex wieħed irid joqgħod attent li ma jtellifx attività legittima.

Ngħid li hemm bracket ta' scores li f'dik il-bracket aħna nimmoniterjaw manwalment and we follow up according to the case. Jekk ikun hemm bżonn, inċemplu lill-klijent biex niverifikaw. Jintbagħatx SMS jew le, it's not really relevant to us għaliex aħna nistgħu niddeċiedu, pereżempju, li għal kull ATM transaction nibgħatu SMS, but there is no risk. It is just information to the customer.

L-istess parametri li niddeċiedu nibgħatux SMS jidhlu wkoll fil-parametri l-oħrajn biex jinbena r-riskju.¹⁸

Wara kjarifiki mitluba mill-Arbitru, ġie stabbilit li l-ammont mitlub bħala rimedju jinkludi l-pagamenti li saru fil-kont ta' *Revolut* għax dawn ma kinux awtorizzati konxjenzjożament mill-Ilmentatriċi u, fil-fatt, mir-*Revolut* dawn mal-ewwel tħallsu lill-*Merchants scammers*. Ġie stabbilit ukoll li l-SMSes tal-Bank b'notifika tal-pagamenti intbagħtu fil-ħin indikat mill-Bank.¹⁹

¹⁸ P. 92 - 93

¹⁹ P. 79

Sottomissjonijiet finali

Fis-sottosmissjonijiet finali tal-Ilmentatriċi, ġew repetuti l-argumenti li l-Bank kien ħtija tat-telf għax ma kellux sistemi ta' moniteragg ta' pagamenti effettiva għax kieku kien iwaqqaf il-pagamenti u jevita jew inaqqas it-telf.

Ġie argumentat ukoll li, fil-fatt, il-Bank bagħat 34 SMSes b'notifika tat-tranzazzjoni meta fil-fatt kien hemm biss 16 u dan bla ma ngħatat ebda spjega dwar it-18-il pagament l-ieħor. L-SMSes dwar dawn it-18 ma humiex inklużi fl-iskeda tal-Bank u staqsiet għaliex.

Ġie kkonfermat ukoll li l-Ilmentatriċi damet ma ndunat b'dawn l-SMSes u ċomplet il-Bank biex tindaga fis-6:00 ta' fil-għodu tal-għada, jiġifieri 17 il-siegħa wara l-ewwel SMS u 8 sigħat wara l-aħħar wieħed.

Fis-sottomissjonijiet finali tal-Bank emfasizza dak li kien diġà qal fir-risposta u waqt is-seduti. Rigward l-argument ġdid li tqajjem dwar it-18-il SMSes li ma ġewx inklużi fl-iskeda tal-Bank ġie spjegat li dawn ma kinux jirrigwardaw tranzazzjonijiet ilmentati u issa kien tard wisq biex jitqajjmu argumenti godda li ma ġewx ittrattati waqt il-proċess.

Ġie emfasizzat li l-BOV kien għamel il-proċess ta' *chargeback* għall-pagamenti ilmentati iżda dan ma rnexxiex. U li waqt li kienu qed iseħħu t-tranzazzjonijiet ilmentati, l-Ilmentatriċi wettqet tranzazzjonijiet ġenwini bl-istess *device* li qalet li kien *hacked*.

Analizi u osservazzjonijiet

F'dan il-każ, l-Ilmentatriċi aċċettat li hija kellha parti mit-tort tat-telf li ġarrbet iżda l-*complaint* tagħha huwa

'... aktar fir-rigward tal-fatt li meta bdew jiġu dawn it-transactions waħda f'waħda ... il-bank għandu monitoring system li kemm-il darba jiffriżawlek il-card u jċemplulek jew jgħidulek biex iċċemplilhom biex jibblokkjawhielek for your own security'.²⁰

²⁰ P. 85

Min-naħa tal-Bank, ikkonferma li għandu sistemi ta' moniteragg ta' pagamenti iżda qal li l-pagamenti konċernati ma gġeneraw l-ebda xamma ta' frodi għax kienu fil-parametri normali tas-sistema.

Iżda s-sistema gġenerat SMS bħala notifika lill-klijenta għal kull pagament ilmentat u l-klijenta ma għamlet xejn dwarhom ħlief meta kien tard wisq.

L-Arbitru jifhem li l-pagamenti kienu f'ammonti relattivament żgħar li mhux normali li jibagħtu xi sinjal ta' allarm dwar frodi. Il-frekwenza tal-pagamenti kienet mhux solita iżda l-fatt li l-klijenta ma ħadet l-ebda azzjoni dwar l-SMSes li bdew jaslulha seta' jiġi interpretat mill-Bank li dawn il-pagamenti kienu kollha kkonfermati bil-kunsens tal-klijenta.

Allura, l-Arbitru ma jifhimx kif l-Ilmentatriċi tista' twaħħal it-telf li nkorriet fuq is-sistema ta' moniteragg ta' pagamenti tal-Bank meta hi stess ma kellha l-ebda moniteragg fuq l-SMSes li kienu qed jintbagħtulha dwar il-pagamenti.

Il-fatt li ntbagħtu 18-il-SMS aktar mis-16 li dwarhom fil-fatt sar pagament frawdolenti, iżid id-doża ta' nuqqas fuq il-klijenta li injorat aktar indizzji serji li messu giegħelha tagħmel kuntatt mal-Bank (kif kienu jitolbu l-SMSes) biex tifhem x'inhu jiġri. Kieku għamlet hekk, it-telf li nkorriet kien jonqos drastikament għax il-card kienet tiġi mbukklata mill-ewwel.

Fix-xhieda tagħha xejn ma kienet konsistenti dwar il-ħin li rċeviet l-SMSes mill-BOV,²¹ kif ukoll xejn ma kienet ċara dwar l-ammont ta' pagamenti ilmentati.²² Xejn ma kienet ċara x'wassalha biex taċċetta tabbina il-card tagħha ma' PayPal meta hi ma kellhiex kont ma' PayPal u, b'hekk, qatt ma kienet għamlet pagamenti permezz ta' PayPal. Dan inaqqas il-kredibbilità tax-xhieda tagħha.

²¹ P. 3 qalet, *'after I received a late notification by the bank'*. P. 85 intqal, *'Dr Mark Muscat jgħid li wara l-complaint hu ċċara mal-klijenta tiegħu u fil-fatt, huwa veru li l-SMSes daħlu f'dik id-data, fit-13 ta' Lulju, però, għal xi raġuni rathom l-għada u, allura, skont hi, kienu delayed.'* P.87 qalet, *'jien kont ikkuntattajt il-bank mill-ewwel x'ħin irċevejt il-messaġġi, kienu xi 6.0 a.m. ...'*. P. 94 qalet, *'Ngħid li rċevejt SMSes mill-bank mhux mill-ewwel. Ngħid li għandi l-iscreenshots kollha. Ngħid li rċevejthom xi nofs siegħa, siegħa wara'*. Fis-sottomossjonijiet finali, p. 113 intqal, *'Għal xi raġuni, minkejja li l-SMSes jidhru li ntbagħtu mill-Bank presso o poco fil-ħin li seħħew it-tranzazzjonijiet, l-Ilmentatriċi ndunat bihom biss l-għada fis-6.00 a.m. ta' filgħodu, u hija kkuntattjat lill-Bank minnufih ...'*

²² Fl-ilment oriġinali, qalet li dawn kienu jammontaw għal €2,711.94. Wara ġie ċċarat li l-ammont kien €2,170.79 li minnhom, fil-fatt, €1,234 marru fil-kont tagħha ta' *Revolut*.

Deciżjoni

Għar-raġunijiet hawn spjegati, l-Arbitru qed jiċċad dan l-ilment u jordna lil kull parti għorri l-ispejjeż tagħha.

Alfred Mifsud

Arbitru għas-Servizzi Finanzjarji

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.