VENDIM
Nr. 29, datë 1.6.2022

PËR MIRATIMIN E RREGULLORES "PËR AUTENTIFIKIMIN E THELLUAR TË KLIENTIT DHE STANDARDET E PËRBASHKËTA, TË HAPURA DHE TË SIGURTA TË KOMUNIKIMIT"

Në bazë dhe për zbatim të nenit 3, pika 3, nenit 12, shkronja "a" dhe nenit 43, shkronja "c", të ligjit nr. 8269, datë 23.12.1997, "Për Bankën e Shqipërisë", i ndryshuar; dhe të nenit 90 dhe nenit 91, të ligjit nr. 55/2020, datë 30.4.2020, "Për shërbimet e pagesave"; Këshilli Mbikëqyrës i Bankës së Shqipërisë, me propozimin e Departamentit të Mbikëqyrjes,

VENDOSI:

1. Të miratojë rregulloren "Për autentifikimin e thelluar të klientit dhe standardet e përbashkëta, të hapura dhe të sigurta të komunikimit", sipas tekstit bashkëlidhur këtij vendimi.
2. Ngarkohen ofruesit e shërbimeve të pagesave për zbatimin e këtij vendimi.
3. Ofruesit e shërbimeve të pagesave, deri në hyrjen në fuqi të rregullores "Për autentifikimin e thelluar të klientit dhe standardet e përbashkëta, të hapura dhe të sigurta të komunikimit", marrin masat dhe krijojnë kushtet e nevojshme për zbatimin e kërkesave të rregullores.
4. Ngarkohet Departamenti i Mbikëqyrjes së Bankës së Shqipërisë për ndjekjen e zbatimit të këtij vendimi.
5. Ngarkohen Kabineti i Guvernatorit dhe Departamenti i Kërkimeve me publikimin e këtij vendimi, përkatësisht në Fletoren Zyrtare të Republikës së Shqipërisë dhe në Buletinin Zyrtar të Bankës së Shqipërisë.

Ky vendim hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

KRYETAR
Gent Sejko

RREGULLORE
PËR AUTENTIFIKIMIN E THELLUAR TË KLIENTIT DHE STANDARDET E PËRBASHKËTA, TË HAPURA DHE TË SIGURTA TË KOMUNIKIMIT

KREU I
TË PËRGJITHSHME

Neni 1
Objekti

Objekti i kësaj rregulloreje është përcaktimi i kërkesave që duhet të plotësohen nga ofruesit e shërbimeve të pagesave, me qëllim zbatimin e masave të sigurisë për:

a) zbatimin e procedurës së autentifikimit të thelluar të klientit, në zbatim të nenit 90 të ligjit "Për shërbimet e pagesave";

b) përjashtimin nga zbatimi i kërkesave të sigurisë së autentifikimit të thelluar të klientit, bazuar në nivelin e rrezikut, shumën dhe përsëritjen e transaksionit të pagesës, si dhe të mënyrës (kanalit) të pagesës të përdorur për ekzekutimin e tij;

c) mbrojtjen e konfidencialitetit dhe integritetit të kredencialeve të personalizuara të sigurisë së përdoruesve të shërbimeve të pagesave;

d) vendosjen e standardeve të përbashkëta, të hapura dhe të sigurta të komunikimit ndërmjet ofruesve të shërbimit të pagesës për shërbimin e llogarisë, ofruesve të shërbimit të inicimit të pagesës, ofruesve të shërbimit të informimit të llogarisë, paguesve, përfituesve të pagesës dhe ofruesve të tjerë të shërbimeve të pagesave, në lidhje me ofrimin dhe përdorimin e shërbimeve të pagesave, në zbatim të titullit IV, të ligjit "Për shërbimet e pagesave".

Neni 2
Subjektet

Subjekte të kësaj rregulloreje janë ofruesit e shërbimeve të pagesave, siç përcaktohen në nenin 3, pika 2, të ligjit nr. 55/2020, datë 30.4.2020 "Për shërbimet e pagesave", i cili në këtë rregullore do të quhet ligji "Për shërbimet e pagesave".

Neni 3
Baza ligjore

Kjo rregullore nxirret në bazë dhe për zbatim të nenit 3, pika 3, nenit 12, shkronja "a" dhe nenit 43, shkronja "c" të ligjit nr. 8269, datë 23.12.1997, "Për Bankën e Shqipërisë", i ndryshuar; dhe të nenit 90 dhe nenit 91, të ligjit "Për shërbimet e pagesave".

Neni 4
Përkufizime

Termat e përdorur në këtë rregullore kanë të njëjtin kuptim me termat e përdorur në ligjin "Për shërbimet e pagesave", në ligjin nr. 9662, datë 18.12.2006 "Për bankat në Republikën e Shqipërisë", i ndryshuar (i cili për thjeshtësi në këtë rregullore do të quhet ligji "Për bankat") dhe në ligjin nr. 107/2015 "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar.

KREU II
KËRKESA TË PËRGJITHSHME PËR AUTENTIFIKIMIN

Neni 5
Kërkesa të përgjithshme për autentifikimin

1. Ofruesit e shërbimeve të pagesave disponojnë mekanizma të monitorimit të transaksioneve, që u mundësojnë atyre zbulimin (identifikimin) e transaksioneve të pagesave të paautorizuara ose me qëllime mashtrimi, për zbatimin e masave të sigurisë të parashikuara në shkronjat "a" dhe "b" të nenit 1 të kësaj rregulloreje, si dhe konfirmimin e origjinës dhe integritetin e të dhënave në formë elektronike. Këto mekanizma bazohen në analizën e transaksioneve të pagesave, duke marrë parasysh elementet që janë tipike për përdoruesit e

shërbimeve të pagesave në rrethanat e një përdorimi normal të kredencialeve të personalizuara të sigurisë.

2. Ofruesit e shërbimeve të pagesave sigurojnë që mekanizmat e monitorimit të transaksioneve marrin në konsideratë, të paktën, faktorët e mëposhtëm të bazuar në rrezik:

a) elementet e autentifikimit, të kompromentuara ose të vjedhura;

b) shumën e secilit transaksion pagese;

c) skenarët e njohur të mashtrimit në ofrimin e shërbimeve të pagesave;

d) shenjat e infektimit nga programe keqdashëse (*signs of malware infection*) në çdo sesion të procedurës së autentifikimit;

e) gjurmët (*log*) e përdorimit të pajisjes së aksesit ose programit (*software*) të ofruar përdoruesit të shërbimeve të pagesave dhe përdorimit jo normal të pajisjes së aksesit ose programit, në rastet kur pajisja e aksesit ose programi ofrohet (sigurohet) nga ofruesi i shërbimeve të pagesave.

Neni 6

Rishikimi i masave të sigurisë

1. Zbatimi i masave të sigurisë të parashikuara në nenin 1 të kësaj rregulloreje do të dokumentohet, testohet periodikisht, vlerësohet dhe kontrollohet në përputhje me kuadrin ligjor e rregullativ në fuqi për ofruesit e shërbimeve të pagesave, nga kontrolli i brendshëm ose auditorët e jashtëm, me ekspertizë në sigurinë e teknologjisë së informacionit dhe pagesa, të cilët janë të pavarur nga pikëpamja operacionale brenda ofruesit, ose nga ofruesi i shërbimeve të pagesave.

2. Periudha midis auditimeve të referuara në pikën 1 të këtij neni, do të përcaktohet sipas kërkesave të standardeve ndërkombëtare të auditimit të zbatueshme për ofruesit e shërbimeve të pagesave.

3. Në çdo rast, ofruesit e shërbimeve të pagesave që përfitojnë nga përjashtimi i parashikuar në nenin 22 të kësaj rregulloreje, do të jenë subjekt i auditimit, të paktën mbi baza vjetore, mbi metodologjinë, modelin dhe normat e mashtrimit të raportuara. Audituesi që kryen këtë auditim duhet të ketë ekspertizë në sigurinë e teknologjisë së informacionit dhe pagesa, si dhe të jetë i pavarur nga pikëpamja operacionale brenda ofruesit, ose nga ofruesi i shërbimeve të pagesave. Gjatë vitit të parë të përdorimit të përjashtimit sipas nenit 22 të kësaj rregulloreje dhe të paktën çdo 3 vjet pas kësaj periudhe, ose më shpesh nëse kërkohet nga Banka e Shqipërisë, ky auditim kryhet nga një auditues i jashtëm, i pavarur dhe i kualifikuar.

4. Auditimi i parashikuar në këtë nen paraqet një vlerësim dhe raport mbi përputhshmërinë e masave të sigurisë të ofruesit të shërbimeve të pagesave, me kërkesat e kësaj rregulloreje. Raporti i plotë, i vihet në dispozicion Bankës së Shqipërisë, me kërkesën e saj.

KREU III

MASAT E SIGURISË PËR ZBATIMIN E AUTENTIFIKIMIT TË THELLUAR TË KLIENTIT

Neni 7

Kodi i autentifikimit

1. Kur ofruesit e shërbimeve të pagesave zbatojnë autentifikim të thelluar të klientit, për rastet e parashikuara në pikën 1, të nenit 90, të ligjit "Për shërbimet e pagesave", autentifikimi bazohet në dy ose më shumë elemente të pavarura, që kategorizohen si njohuri, posedim dhe qenësi, dhe rezultojnë në gjenerimin e një kodi autentifikimi.

2. Kodi i autentifikimit i parashikuar në pikën 1 të këtij neni, pranohet vetëm një herë nga ofruesi i shërbimeve të pagesave, në rastet kur paguesi përdor kodin e autentifikimit për të aksesuar llogarinë e tij të pagesës *online*, për të iniciuar një transaksion elektronik pagese, ose për të kryer çdo veprim nëpërmjet një mënyre komunikimi në distancë, që mund të nënkuptojë një rrezik mashtrimi pagese ose abuzime të tjera.

3. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave zbatojnë masa sigurie, të cilat sigurojnë plotësimin e të gjitha kërkesave të mëposhtme:

a) asnjë informacion mbi elementet e parashikuara në pikën 1 të këtij neni, nuk mund të gjenerohet nga zbulimi (*disclosure*) i kodit të autentifikimit;

b) nuk është e mundur të gjenerohet një kod i ri autentifikimi, bazuar në njohurinë e ndonjë kodi tjetër autentifikimi të gjeneruar më parë;

c) kodi i autentifikimit nuk mund të falsifikohet.

4. Ofruesit e shërbimeve të pagesave sigurojnë që autentifikimi nëpërmjet krijimit të një kodi autentifikimi, përfshin të gjitha masat e mëposhtme:

a) kur autentifikimi për aksesin në distancë, pagesat elektronike në distancë dhe çdo veprim tjetër përmes një mënyre komunikimi në distancë, që mund të nënkuptojë një rrezik mashtrimi pagese ose abuzime të tjera, dështon të gjenerojë një kod autentifikimi për qëllimet e pikës 1 të këtij neni, nuk do të jetë e mundur të identifikohet se cili nga elementet e parashikuara në atë pikë, ishte i pasaktë;

b) numri i tentativave të dështuara të autentifikimit që mund të ndodhin njëra pas tjetrës, pas së cilave veprimet e parashikuara në pikën 1 të nenit 90 të ligjit "Për shërbimet e pagesave" do të bllokohen përkohësisht ose përgjithmonë, nuk duhet të jetë më shumë se pesë, brenda një periudhe të caktuar kohore;

c) seancat e komunikimit janë të mbrojtura ndaj kapjes së të dhënave të autentifikimit të transmetuara gjatë autentifikimit dhe ndaj manipulimit nga palë të paautorizuara, në përputhje me kërkesat e kreut VI të kësaj rregulloreje;

d) pasi paguesi të jetë autentifikuar për të aksesuar *online* llogarinë e tij të pagesës, koha maksimale pa aktivitet (pa veprime) nuk duhet të kalojë 5 minuta.

5. Në rastet kur bllokimi i parashikuar në shkronjën "b" të pikës 4 të këtij neni, është i përkohshëm, kohëzgjatja e bllokimit dhe numri i tentativave përcaktohet bazuar në karakteristikat e shërbimit të ofruar drejt paguesit dhe në të gjitha rreziqet përkatëse të përfshira, duke marrë parasysh, së paku, faktorët e përcaktuar në pikën 2 të nenit 5 të kësaj rregulloreje. Ofruesi i shërbimeve të pagesave njofton paguesin përpara se bllokimi të bëhet i përhershëm. Kur bllokimi është bërë i përhershëm, krijohet një procedurë e sigurt që lejon paguesin të rifitojë përdorimin e instrumenteve të bllokuara të pagesave elektronike.

Neni 8

Lidhjet dinamike

1. Në rastet kur ofruesit e shërbimeve të pagesave aplikojnë autentifikimin e thelluar të klientit në përputhje me pikën 2, të nenit 90, të ligjit "Për shërbimet e pagesave", përveç kërkesave të nenit 7 të kësaj rregulloreje, ata gjithashtu miratojnë masa sigurie që plotësojnë të gjitha kërkesat e mëposhtme:

a) paguesi është në dijeni të shumës së transaksionit të pagesës dhe të përfituesit;

b) kodi i gjeneruar i autentifikimit është specifik për shumën e transaksionit të pagesës dhe për përfituesin, për të cilët paguesi ka rënë dakord në momentin e inicimit të transaksionit;

c) kodi i autentifikimit i pranuar nga ofruesi i shërbimeve të pagesave korrespondon me shumën specifike origjinale të transaksionit të pagesës dhe me identitetin e përfituesit të dakorduar nga paguesi;

d) çdo ndryshim i shumës ose i përfituesit rezulton në pavlefshmëri të kodit të gjeneruar të autentifikimit.

2. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave zbatojnë masa sigurie, të cilat sigurojnë konfidencialitetin, autenticitetin dhe integritetin e elementeve të mëposhtme:

a) të shumës së transaksionit dhe përfituesit, gjatë të gjitha fazave të autentifikimit; dhe

b) të informacionit që i shfaqet paguesit gjatë të gjitha fazave të autentifikimit, përfshirë gjenerimin, transmetimin dhe përdorimin e kodit të autentifikimit.

3. Për qëllime të shkronjës "b", të pikës 1, të këtij neni dhe kur ofruesit e shërbimeve të pagesave aplikojnë autentifikim të thelluar të klientit në përputhje me pikën 2, të nenit 90, të ligjit "Për shërbimet e pagesave", për kodin e autentifikimit zbatohen kërkesat e mëposhtme:

a) për një transaksion pagese nëpërmjet kartës, për të cilin paguesi ka dhënë pëlqimin për shumën e saktë të fondeve që do të bllokohen në përputhje me nenin 68, të ligjit "Për shërbimet e pagesave", kodi i autentifikimit do të jetë specifik për shumën që paguesi ka dhënë pëlqimin për t'u bllokuar dhe që është rënë dakord nga paguesi në momentin e inicimit të transaksionit;

b) për transaksionet e pagesave, për të cilat paguesi ka dhënë pëlqimin për t'u ekzekutuar si grup transaksionesh të pagesave elektronike në distancë për një ose disa përfitues, kodi i autentifikimit do të jetë specifik për shumën totale të grupit të transaksioneve të pagesave dhe për përfituesit e përcaktuar (specifikuar).

Neni 9

Kërkesat për elementet e kategorizuara si "njohuri"

1. Ofruesit e shërbimeve të pagesave marrin masa për të reduktuar rrezikun që elementet e autentifikimit të thelluar të klientit të kategorizuara si "njohuri", të mund të zbulohen nga palët e paautorizuara ose t'u shpërndahen atyre.

2. Përdorimi i këtyre elementeve nga paguesi, do të jetë subjekt i masave zbutëse për të parandaluar shpërndarjen e tyre te palë të paautorizuara.

Neni 10

Kërkesat për elementet e kategorizuara si "posedim"

1. Ofruesit e shërbimeve të pagesave marrin masa për të reduktuar rrezikun që elementet e autentifikimit të thelluar të klientit të kategorizuara si "posedim", të përdoren nga palë të paautorizuara.

2. Përdorimi i këtyre elementeve nga paguesi, do të jetë subjekt i masave të hartuara për të parandaluar kopjimin (*replication*) e elementeve.

Neni 11

Kërkesat për pajisjet dhe programin (*software*), të lidhur me elemente të kategorizuara si "qenësi"

1. Ofruesit e shërbimeve të pagesave marrin masa për të reduktuar rrezikun që elementet e autentifikimit të kategorizuara si "qenësi" dhe të lexuara nga pajisjet e aksesit dhe programi, që i vihen në dispozicion paguesit, të zbulohen nga palë të paautorizuara. Ofruesit e shërbimeve të pagesave sigurojnë të paktën që pajisjet e aksesit dhe programi të kenë një probabilitet shumë të ulët që një palë e paautorizuar të autentifikohet si pagues.

2. Përdorimi i këtyre elementeve nga paguesi, do të jetë subjekt i masave që sigurojnë që pajisjet dhe programi të garantojnë rezistencë ndaj përdorimit të paautorizuar të elementeve nëpërmjet aksesit në pajisje dhe në program.

Neni 12

Pavarësia e elementeve

1. Ofruesit e shërbimeve të pagesave sigurojnë që përdorimi i elementeve të autentifikimit të thelluar të klientit, të parashikuara në nenet 9, 10 dhe 11 të kësaj rregulloreje, është subjekt i masave që sigurojnë që shkelja (thyerja) e njërit prej elementeve nuk kompromenton besueshmërinë e elementeve të tjera, në lidhje me teknologjinë, algoritmet dhe parametrat.

2. Ofruesit e shërbimeve të pagesave marrin masa sigurie, kur ndonjë nga elementet e autentifikimit të thelluar të klientit ose vetë kodi i autentifikimit përdoret nëpërmjet një pajisjeje shumëfunksionale, me qëllim që të reduktojnë rrezikun që mund të rezultojë nga kompromentimi i kësaj pajisjeje.

3. Për qëllime të pikës 2 të këtij neni, masat përfshijnë secilin nga elementet e mëposhtme:

a) përdorimin e mjediseve të ndara dhe të sigurta të ekzekutimit nëpërmjet programit të instaluar brenda pajisjes shumëfunksionale;

b) mekanizmat për të siguruar që programi kompjuterik ose pajisja nuk është modifikuar nga paguesi ose nga një palë e tretë;

c) mekanizmat për të zbutur pasojat, në rastet kur kanë ndodhur ndryshime apo modifikime.

KREU IV

PËRJASHTIMET NGA AUTENTIFIKIMI I THELLUAR I KLIENTIT

Neni 13

Aksesi në informacionin e llogarisë së pagesës në mënyrë direkte me ofruesin e shërbimit të pagesës për shërbimin e llogarisë

1. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësohen kërkesat e parashikuara në nenin 5 dhe me përjashtim të rasteve të parashikuara në pikën 2 të këtij neni, kur përdoruesi i shërbimeve të pagesave akseson *online* llogarinë e tij të pagesave në mënyrë direkte, me kusht që aksesi *online* është i kufizuar për të paktën njërin prej elementeve të mëposhtme, pa zbuluar të dhënat sensitive të pagesës:

a) gjendjen (balancën) e një ose më shumë llogarive të caktuara të pagesave;

b) transaksionet e pagesave të kryera në 90 ditët e fundit nëpërmjet një ose më shumë llogarive të caktuara të pagesave.

2. Përjashtimisht nga sa parashikohet në pikën 1 të këtij neni, ofruesit e shërbimeve të pagesave do të zbatojnë autentifikimin e thelluar të klientit, në rastet kur plotësohet njëri nga kushtet e mëposhtme:

a) përdoruesi i shërbimeve të pagesave akseson *online* për herë të parë, informacionin e parashikuar në pikën 1 të këtij neni;

b) kanë kaluar më shumë se 180 ditë që nga hera e fundit kur përdoruesi i shërbimeve të pagesave ka aksesuar *online* informacionin e përcaktuar në pikën 1 të këtij neni dhe kur është zbatuar autentifikimi i thelluar i klientit.

Neni 14

Aksesi në informacionin e llogarisë së pagesës nëpërmjet një ofruesi të shërbimit të informimit të llogarisë

1. Ofruesit e shërbimeve të pagesave nuk do të zbatojnë autentifikimin e thelluar të klientit, me përjashtim të rasteve të parashikuara në pikën 2 të këtij neni, kur përdoruesi i shërbimeve të pagesave akseson *online* llogarinë e tij të pagesave nëpërmjet një ofruesi të shërbimit të informimit të llogarisë, me kusht që aksesi *online* është i kufizuar për të paktën njërin prej elementeve të mëposhtme, pa zbuluar të dhënat sensitive të pagesës:

a) gjendjen (balancën) e një ose më shumë llogarive të caktuara të pagesave;

b) transaksionet e pagesave të kryera në 90 ditët e fundit nëpërmjet një ose më shumë llogarive të caktuara të pagesave.

2. Përjashtimisht nga sa parashikohet në pikën 1 të këtij neni, ofruesit e shërbimeve të pagesave do të zbatojnë autentifikimin e thelluar të klientit, në rastet kur plotësohet njëri nga kushtet e mëposhtme:

a) përdoruesi i shërbimeve të pagesave akseson *online* për herë të parë, informacionin e parashikuar në pikën 1 të këtij neni, nëpërmjet ofruesit të shërbimit të informimit të llogarisë;

b) kanë kaluar më shumë se 180 ditë që nga hera e fundit kur përdoruesi i shërbimeve të pagesave ka aksesuar *online* informacionin e përcaktuar në pikën 1 të këtij neni, nëpërmjet ofruesit të shërbimit të informimit të llogarisë dhe kur është zbatuar autentifikimi i thelluar i klientit.

3. Përjashtimisht nga sa parashikohet në pikën 1 të këtij neni, ofruesit e shërbimeve të pagesave do të zbatojnë autentifikimin e thelluar të klientit, kur një përdorues i shërbimeve të pagesave po akseson *online* llogarinë e tij të pagesave nëpërmjet një ofruesi të shërbimit të informimit të llogarisë dhe kur ofruesi i shërbimeve të pagesave justifikon në mënyrë objektive dhe evidenton qartë, arsye të lidhura me hyrje të paautorizuara ose me qëllim mashtrimi në llogarinë e pagesës. Në këtë rast, ofruesi i shërbimeve të pagesave dokumenton dhe justifikon në mënyrë të qartë për Bankën e Shqipërisë, me kërkesën e kësaj të fundit, arsyet për zbatimin e autentifikimit të thelluar të klientit.

4. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë që ofrojnë një ndërfaqe të dedikuar siç parashikohet në nenin 35 të kësaj rregulloreje, nuk zbatojnë përjashtimin e parashikuar në pikën 1 të këtij neni, për qëllime të mekanizmit të emergjencës të parashikuar në nenin 37, pika 4 të kësaj rregulloreje, kur ata nuk zbatojnë përjashtimin e parashikuar në nenin 13 të kësaj rregulloreje, në ndërfaqen e drejtpërdrejtë të përdorur për autentifikimin dhe komunikimin me përdoruesit e tyre të shërbimeve të pagesave.

Neni 15

Pagesat pa kontakt në pikën e shitjes

1. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësojnë kërkesat e parashikuara në nenin 5 të kësaj rregulloreje, kur paguesi inicion një transaksion pagese elektronike pa kontakt (*contactless*), nëse plotësohen kushtet e mëposhtme:

a) shuma individuale e transaksionit të pagesës elektronike pa kontakt nuk tejkalon vlerën ekuivalente në lekë të shumës 50 euro; dhe

b) shuma kumulative e transaksioneve të mëparshme të pagesave elektronike pa kontakt të iniciuara me anë të një instrumenti pagese me një funksionalitet pa kontakt, nga data e zbatimit të fundit të autentifikimit të thelluar të klientit nuk tejkalon vlerën ekuivalente në lekë të shumës 150 euro; ose

c) numri i transaksioneve të njëpasnjëshme të pagesave elektronike pa kontakt të iniciuara nëpërmjet instrumentit të pagesës që ofron një funksionalitet pa kontakt, që nga zbatimi i fundit i autentifikimit të thelluar të klientit, nuk është më i lartë se pesë.

Neni 16

Terminalet e pambikëqyrura për pagesat e transportit dhe tarifat e parkimit

Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësojnë kërkesat e parashikuara në nenin 5 të kësaj rregulloreje, kur paguesi inicion një transaksion pagese elektronike në një terminal pagese të pambikëqyrur (*unattended*), për qëllime të pagimit të një pagese/bilete transporti ose një tarife parkimi.

Neni 17

Përfituesit e besuar

1. Ofruesit e shërbimeve të pagesave do të zbatojnë autentifikimin e thelluar të klientit, kur një pagues krijon ose ndryshon një listë të përfituesve të besuar, nëpërmjet ofruesit të shërbimit të pagesës për shërbimin e llogarisë së paguesit.

2. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësojnë kërkesat e përgjithshme të autentifikimit, në rastet kur paguesi inicion një transaksion pagese dhe përfituesi përfshihet në një listë të përfituesve të besuar të krijuar më parë nga paguesi.

Neni 18

Transaksionet e përsëritura

1. Ofruesit e shërbimeve të pagesave zbatojnë autentifikimin e thelluar të klientit, kur një pagues krijon, ndryshon ose inicion për herë të parë, një seri transaksionesh të përsëritura, me të njëjtën shumë dhe me të njëjtin përfitues.

2. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësojnë kërkesat e përgjithshme të autentifikimit, për inicimin e të gjitha transaksioneve të pagesave pasuese, të përfshira në serinë e transaksioneve të pagesave të referuara në pikën 1 të këtij neni.

Neni 19

Transfertat e kreditit ndërmjet llogarive të mbajtura nga i njëjti person fizik ose juridik

Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, nëse plotësojnë kërkesat e parashikuara në nenin 5, kur paguesi inicion një transfertë krediti në kushtet kur paguesi dhe përfituesi janë i njëjti person fizik ose juridik dhe të dyja llogaritë e pagesave mbahen nga i njëjti ofrues i shërbimit të pagesës për shërbimin e llogarisë.

Neni 20
Transaksionet me vlerë të ulët

1. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, kur paguesi inicion një transaksion pagese elektronike në distancë, nëse plotësohen kushtet e mëposhtme:

a) shuma e transaksionit të pagesës elektronike në distancë nuk tejkalon vlerën ekuivalente në lekë të shumës 30 euro; dhe

b) shuma kumulative e transaksioneve të mëparshme të pagesave elektronike në distancë të iniciuara nga paguesi, që nga zbatimi i fundit i autentifikimit të thelluar të klientit, nuk tejkalon vlerën ekuivalente në lekë të shumës 100 euro; ose

c) numri i transaksioneve të mëparshme të pagesave elektronike në distancë, të iniciuara nga paguesi, që nga zbatimi i fundit i autentifikimit të thelluar të klientit, nuk i kalon pesë transaksione individuale të njëpasnjëshme të pagesave elektronike në distancë (*remote*).

Neni 21
Proceset dhe protokollet e sigurta të pagesave të kompanive

Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit për personat juridikë që iniciojnë transaksione pagese elektronike nëpërmjet përdorimit të proceseve të dedikuara të pagesave ose protokolleve, që u vihen në dispozicion vetëm paguesve që nuk janë konsumatorë, në rastin kur Banka e Shqipërisë vlerëson që ato procese ose protokolle garantojnë të paktën nivele ekuivalente të sigurisë me ato të parashikuara në ligjin "Për shërbimet e pagesave".

Neni 22
Analiza e rrezikut të transaksionit

1. Ofruesit e shërbimeve të pagesave mund të mos zbatojnë autentifikimin e thelluar të klientit, në rastet kur paguesi inicion një transaksion të pagesave elektronike në distancë, të kategorizuar nga ofruesi i shërbimeve të pagesave si një transaksion me nivel të ulët rreziku, sipas mekanizmave të monitorimit të transaksioneve të parashikuara në nenin 5 dhe në shkronjën "c", të pikës 2, të këtij neni.

2. Një transaksion pagese elektronike në distancë i referuar në pikën 1, të këtij neni, do të konsiderohet se paraqet një nivel të ulët rreziku, kur plotësohen të gjitha kushtet e mëposhtme:

a) norma e mashtrimit për atë lloj transaksioni, e raportuar nga ofruesi i shërbimeve të pagesave dhe e llogaritur në përputhje me nenin 23 të kësaj rregulloreje, është e njëjtë me,

ose më e ulët se, normat referencë të mashtrimit të parashikuara në aneksin 1 të kësaj rregulloreje për "pagesat elektronike me kartë në distancë" dhe "transfertat elektronike të kreditit në distancë";

b) shuma e transaksionit nuk tejkalon vlerën përkatëse të kufirit të përjashtimit ("VKP") të parashikuar në aneksin 1 të kësaj rregulloreje;

c) ofruesit e shërbimeve të pagesave, si rezultat i kryerjes së një analize të rrezikut në kohë reale, nuk kanë identifikuar ndonjë nga elementet e mëposhtme:

i. shpenzime jonormale apo model (mënyrë) sjellje jo të zakonshme të paguesit;

ii. informacion të pazakontë në lidhje me pajisjen e aksesit ose programin e paguesit;

iii. shenja të infektimit nga programe keqdashëse (*signs of malware infection*) në ndonjë sesion të procedurës së autentifikimit;

iv. skenar të njohur mashtrimi (*fraud*) në ofrimin e shërbimeve të pagesave,

v. vendndodhje jonormale të paguesit,

vi. vendndodhje me rrezik të lartë të përfituesit.

3. Ofruesit e shërbimeve të pagesave që synojnë të përjashtojnë transaksionet e pagesave elektronike në distancë nga autentifikimi i thelluar i klientit, me arsyetimin se ato paraqesin një rrezik të ulët, marrin parasysh të paktën faktorët e mëposhtëm të bazuar në rrezik:

a) modelet e mëparshme të shpenzimeve të përdoruesit individual të shërbimeve të pagesave;

b) historikun e transaksioneve të pagesave të secilit prej përdoruesve të shërbimeve të pagesave të ofruesit të shërbimeve të pagesave;

c) vendndodhjen e paguesit dhe të përfituesit në kohën e transaksionit të pagesës, në rastet kur pajisja e aksesit ose programi ofrohet (sigurohet) nga ofruesi i shërbimeve të pagesave;

d) identifikimin e modeleve jonormale të pagesave të përdoruesit të shërbimeve të pagesave, në lidhje me historikun e transaksioneve të pagesave të përdoruesit.

4. Ofruesi i shërbimeve të pagesave kombinon të gjithë faktorët e bazuar në rrezik, të parashikuar në pikën 3 të këtij neni, në një vlerësim të agreguar të rrezikut për çdo transaksion individual, për të përcaktuar nëse duhet të lejohet të kryhet një pagesë specifike pa zbatuar autentifikimin e thelluar të klientit.

Neni 23

Llogaritja e normave të mashtrimit

1. Ofruesi i shërbimeve të pagesave sigurohet që, për secilin lloj të transaksioneve të parashikuara në aneksin 1 të kësaj rregulloreje, normat e përgjithshme të mashtrimit që mbulojnë të dy transaksionet e pagesave të autentifikuara nëpërmjet autentifikimit të thelluar të klientit dhe ato të ekzekutuara sipas çdo përjashtimi të parashikuar në nenet 17 deri në 22 të kësaj rregulloreje, janë të njëjta me, ose më të ulëta se, normat referencë të mashtrimit për të njëjtin lloj transaksioni pagese të parashikuar në aneksin 1 të kësaj rregulloreje.

2. Norma e përgjithshme e mashtrimit për secilin lloj të transaksioneve llogaritet si vlera totale e transaksioneve elektronike në distancë (*remote*), të paautorizuara ose me qëllim mashtrimi, pavarësisht nëse fondet janë rikuperuar ose jo, pjesëtuar me vlerën totale të të gjitha transaksioneve në distancë për të njëjtin lloj transaksionesh, pavarësisht nëse janë të autentifikuara nëpërmjet zbatimit të autentifikimit të thelluar të klientit ose të ekzekutuara në përputhje me përjashtimet e parashikuara në nenet 17 deri në 22 të kësaj rregulloreje, mbi baza rrëshqitëse (*rolling*) tremujore (90 ditë).

3. Llogaritja e normave të mashtrimit dhe rezultatet e marra, vlerësohen nga rishikimi i auditit, siç përcaktohet në pikën 3 të nenit 6 të kësaj rregulloreje, i cili siguron që ato të jenë të plota dhe të sakta.

4. Metodologjia dhe çdo model i përdorur nga ofruesi i shërbimeve të pagesave për të llogaritur normat e mashtrimit, si dhe vetë normat e mashtrimit, dokumentohen në mënyrë të përshtatshme dhe vihen në dispozicion të Bankës së Shqipërisë, me kërkesë të saj.

Neni 24

Ndërprerja e përjashtimeve bazuar në analizën e rrezikut të transaksionit

1. Ofruesit e shërbimeve të pagesave që përdorin përjashtimin e parashikuar në nenin 22 të kësaj rregulloreje, raportojnë menjëherë në Bankën e Shqipërisë në rastet kur një nga normat e tyre të mashtrimit të monitoruara, për çdo lloj transaksioni pagese të parashikuar në aneksin 1 të kësaj rregulloreje, tejkalon normën referencë të mashtrimit të zbatueshme dhe i paraqesin Bankës së Shqipërisë, një përshkrim të masave që synojnë të marrin për të rivendosur përputhshmërinë e normës të monitoruar të mashtrimit me normën referencë të mashtrimit të zbatueshme.

2. Ofruesit e shërbimeve të pagesave ndërpresin menjëherë përdorimin e përjashtimit të parashikuar në nenin 22 të kësaj rregulloreje për çdo lloj transaksioni pagese të parashikuar në aneksin 1 të kësaj rregulloreje, sipas intervaleve përkatëse të përjashtimit, në rastet kur niveli i normave të mashtrimit të monitoruara tejkalon për dy tremujorë radhazi normën referencë të mashtrimit, të zbatueshme për atë instrument pagese ose për atë lloj transaksioni të pagesës, sipas intervaleve përkatëse të përjashtimit.

3. Pas ndërprerjes së përdorimit të përjashtimit të parashikuar në nenin 22 të kësaj rregulloreje, në përputhje me pikën 2 të këtij neni, ofruesit e shërbimeve të pagesave nuk e përdorin atë përjashtim, derisa norma e llogaritur e mashtrimit të jetë e barabartë ose më e ulët se normat referencë të mashtrimit, të zbatueshme për atë lloj transaksioni pagese sipas intervaleve përkatëse të përjashtimit, për një tremujor.

4. Në rastet kur ofruesit e shërbimeve të pagesave synojnë të përdorin përsëri përjashtimin e parashikuar në nenin 22 të kësaj rregulloreje, përpara se të përdorin përsëri përjashtimin, ata njoftojnë Bankën e Shqipërisë brenda një afati të arsyeshëm kohor dhe i paraqesin dëshmi të përputhshmërisë së normës së monitoruar të mashtrimit me normën referencë të mashtrimit, të zbatueshme sipas intervaleve përkatëse të përjashtimit, në përputhje me pikën 3 të këtij neni.

Neni 25

Monitorimi

1. Ofruesit e shërbimeve të pagesave, për të përdorur përjashtimet e përcaktuara në nenet 13 deri 22 të kësaj rregulloreje, regjistrojnë dhe monitorojnë të dhënat e mëposhtme për secilin lloj të transaksioneve të pagesave, duke evidentuar në mënyrë të veçantë transaksionet e pagesave në distancë dhe jo në distancë, të paktën në baza tremujore:

a) vlerën totale të transaksioneve të pagesave të paautorizuara ose me qëllim mashtrimi, në përputhje me pikën 4, të nenit 57, të ligjit "Për shërbimet e pagesave", vlerën totale të të gjitha transaksioneve të pagesave dhe normën e mashtrimit që rezulton, duke përfshirë edhe ndarjen e transaksioneve të pagesave, të iniciuara nëpërmjet autentifikimit të thelluar të klientit dhe sipas secilit nga përjashtimet;

b) vlerën mesatare të transaksionit, duke përfshirë edhe ndarjen e transaksioneve të pagesave të iniciuara nëpërmjet autentifikimit të thelluar të klientit dhe sipas secilit nga përjashtimet;

c) numrin e transaksioneve të pagesave ku është zbatuar secili prej përjashtimeve dhe përqindjen e tyre në lidhje me numrin total të transaksioneve të pagesave.

2. Ofruesit e shërbimeve të pagesave vënë në dispozicion të Bankës së Shqipërisë, me kërkesë të saj, rezultatet e monitorimit sipas parashikimeve në pikën 1 të këtij neni.

KREU V
KONFIDENCIALITETI DHE INTEGRITETI I KREDENCIALEVE TË PERSONALIZUARA TË SIGURISË TË PËRDORUESVE TË SHËRBIMEVE TË PAGESAVE

Neni 26
Kërkesa të përgjithshme

1. Ofruesit e shërbimeve të pagesave sigurojnë konfidencialitetin dhe integritetin e kredencialeve (të dhënave) të personalizuara të sigurisë të përdoruesit të shërbimeve të pagesave, përfshirë kodet e autentifikimit përgjatë të gjitha fazave të autentifikimit.

2. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave sigurojnë plotësimin e kërkesave të mëposhtme:

a) kredencialet e personalizuara të sigurisë shfaqen të maskuara dhe nuk janë të lexueshme në mënyrë të plotë kur vendosen (*input*) nga përdoruesi i shërbimeve të pagesave gjatë autentifikimit;

b) kredencialet e personalizuara të sigurisë në format të dhënash, si dhe materialet kriptografike që lidhen me enkriptimin e kredencialeve të personalizuara të sigurisë, nuk ruhen në tekst të thjeshtë;

c) materiali sekret kriptografik mbrohet nga zbulimi i paautorizuar.

3. Ofruesit e shërbimeve të pagesave dokumentojnë plotësisht procesin e administrimit të materialit kriptografik, të përdorur për të enkriptuar ose për t'i bërë të palexueshme kredencialet e personalizuara të sigurisë.

4. Ofruesit e shërbimeve të pagesave sigurojnë që përpunimi dhe transmetimi (*routing*) i kredencialeve të personalizuara të sigurisë dhe i kodeve të autentifikimit të gjeneruara në përputhje me kreun III të kësaj rregulloreje, zhvillohen në mjedise të sigurta në përputhje me standardet e thelluara dhe të njohura gjerësisht.

Neni 27
Krijimi dhe dorëzimi i kredencialeve të personalizuara të sigurisë

1. Ofruesit e shërbimeve të pagesave sigurojnë që krijimi i kredencialeve të personalizuara të sigurisë të kryhet në një mjedis të sigurt.

2. Ofruesit e shërbimeve të pagesave marrin masat e duhura për të reduktuar rreziqet e përdorimit të paautorizuar të kredencialeve të personalizuara të sigurisë dhe të pajisjeve apo programeve të autentifikimit, pas humbjes, vjedhjes ose kopjimit të tyre dhe para dërgimit të tyre te paguesi.

Neni 28

Lidhja me përdoruesin e shërbimeve të pagesave

1. Ofruesit e shërbimeve të pagesave sigurojnë që vetëm përdoruesi i shërbimeve të pagesave të jetë i lidhur, në një mënyrë të sigurt, me kredencialet e personalizuara të sigurisë, pajisjet dhe programin e autentifikimit.

2. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave sigurojnë plotësimin e kërkesave të mëposhtme:

a) lidhja e identitetit të përdoruesit të shërbimeve të pagesave me kredencialet e personalizuara të sigurisë, pajisjet dhe programin e autentifikimit, kryhet në mjedise të sigurta, nën përgjegjësinë e ofruesit të shërbimeve të pagesave, që përfshin të paktën mjediset e ofruesit të shërbimeve të pagesave, mjedisin e internetit të siguruar (ofruar) nga ofruesi i shërbimeve të pagesave ose faqe interneti të tjera të ngjashme të sigurta, të përdorura nga ofruesi i shërbimeve të pagesave dhe shërbimet e tij të ATM-së, si dhe duke marrë parasysh rreziqet që lidhen me pajisjet dhe komponentët bazë të përdorur gjatë procesit të lidhjes, që nuk janë nën përgjegjësinë e ofruesit të shërbimeve të pagesave;

b) lidhja me anë të një mënyre komunikimi në distancë, e identitetit të përdoruesit të shërbimeve të pagesave me kredencialet e personalizuara të sigurisë dhe me pajisje ose programin e autentifikimit, kryhet duke përdorur autentifikim të thelluar të klientit.

Neni 29

Dërgimi i kredencialeve, pajisjeve dhe programit të autentifikimit

1. Ofruesit e shërbimeve të pagesave sigurojnë që dërgimi i kredencialeve të personalizuara të sigurisë, pajisjeve dhe programit të autentifikimit te përdoruesit e shërbimeve të pagesave, të kryhet në një mënyrë të sigurt, të krijuar për të adresuar rreziqet në lidhje me përdorimin e paautorizuar të tyre për shkak të humbjes, vjedhjes ose kopjimit.

2. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave zbatojnë të paktën, masat e mëposhtme:

a) mekanizma efektivë dhe të sigurt të dërgimit, duke siguruar që kredencialet e personalizuara të sigurisë, pajisjet dhe programi i autentifikimit, t'i dorëzohen përdoruesit legjitim të shërbimeve të pagesave;

b) mekanizma që lejojnë ofruesin e shërbimeve të pagesave, të verifikojë vërtetësinë e programit të autentifikimit të dërguar te përdoruesi i shërbimeve të pagesave, me anë të internetit;

c) marrëveshje që sigurojnë se, kur dërgimi i kredencialeve të personalizuara të sigurisë ekzekutohet jashtë mjediseve të ofruesit të shërbimeve të pagesave ose nëpërmjet një mënyre komunikimi në distancë:

i. asnjë palë e paautorizuar nuk mund të marrë më shumë se një atribut të kredencialeve të personalizuara të sigurisë, pajisjeve të autentifikimit ose programeve, kur dërgohen nëpërmjet të njëjtit kanal,

ii. kredencialet e personalizuara të sigurisë të dërguara, pajisjet ose programi i autentifikimit, kërkojnë aktivizim përpara përdorimit;

d) marrëveshje që sigurojnë se, në rastet kur kredencialet e personalizuara të sigurisë, pajisjet ose programi (*software*) i autentifikimit duhet të aktivizohen para përdorimit të tyre të parë, aktivizimi do të zhvillohet në një mjedis të sigurt në përputhje me procedurat e lidhjes të parashikuara në nenin 28 të kësaj rregulloreje.

3. Ofruesi i shërbimeve të pagesave është i detyruar të informojë përdoruesin legjitim të shërbimeve të pagesave, në lidhje me rëndësinë e ruajtjes së fshehtësisë së kredencialeve të personalizuara të sigurisë nga persona të tretë.

Neni 30
Rinovimi i kredencialeve të personalizuara të sigurisë

Ofruesit e shërbimeve të pagesave sigurojnë që rinovimi ose riaktivizimi i kredencialeve të personalizuara të sigurisë është në përputhje me procedurat për krijimin, lidhjen dhe dërgimin e kredencialeve dhe pajisjeve të autentifikimit, siç parashikohet në nenet 27, 28 dhe 29 të kësaj rregulloreje.

Neni 31
Shkatërrimi, çaktivizimi dhe revokimi

Ofruesit e shërbimeve të pagesave sigurojnë procese efektive, me qëllim që të zbatojnë secilën nga masat e mëposhtme të sigurisë:

a) shkatërrimin, çaktivizimin ose revokimin e sigurt të kredencialeve të personalizuara të sigurisë, pajisjeve dhe programit të autentifikimit;

b) kur ofruesi i shërbimeve të pagesave shpërndan pajisje dhe programe të autentifikimit të ripërdorshme, ripërdorimi i sigurt i pajisjes ose programit kryhet, dokumentohet dhe zbatohet, përpara vendosjes në dispozicion të një përdoruesi tjetër të shërbimeve të pagesave;

c) çaktivizimi ose revokimi i informacionit në lidhje me kredencialet e personalizuara të sigurisë, të ruajtura në sistemet dhe bazat e të dhënave të ofruesit të shërbimeve të pagesave dhe, kur është e përshtatshme, në sistemet publike të ruajtjes së informacionit (*public repositories*).

KREU VI
STANDARDET E PËRBASHKËTA, TË HAPURA DHE TË SIGURTA TË KOMUNIKIMIT

NËNKREU I
KËRKESA TË PËRGJITHSHME PËR KOMUNIKIMIN

Neni 32
Kërkesat për procedurat e identifikimit elektronik të sigurt

1. Ofruesit e shërbimeve të pagesave sigurojnë identifikim elektronik të sigurt, sipas përcaktimeve në legjislacionin për identifikimin elektronik dhe shërbimet e besuara, gjatë komunikimit midis pajisjes së paguesit dhe pajisjeve të pranimit të përfituesit për pagesat elektronike, duke përfshirë, por pa u kufizuar në terminalet e pagesave.

2. Ofruesit e shërbimeve të pagesave sigurojnë që rreziqet e keqorientimit të komunikimit për palët e paautorizuara në aplikacionet *mobile* dhe ndërfaqet e përdoruesve të tjerë të shërbimeve të pagesave, që ofrojnë shërbime të pagesave elektronike, të zbuten në mënyrë efektive.

Neni 33
Gjurmueshmëria

1. Ofruesit e shërbimeve të pagesave krijojnë procese të caktuara që sigurojnë që të gjitha transaksionet e pagesave dhe ndërveprimet e tjera me përdoruesin e shërbimeve të pagesave, me ofruesit e tjerë të shërbimeve të pagesave dhe me subjekte të tjera, përfshirë edhe tregtarët, në kontekstin e ofrimit të shërbimit të pagesave, janë të gjurmueshme, duke siguruar njohuri *ex post* për të gjitha ngjarjet që lidhen me transaksionin elektronik, në të gjitha fazat e ndryshme.

2. Për qëllime të pikës 1 të këtij neni, ofruesit e shërbimeve të pagesave sigurojnë që çdo seancë komunikimi e realizuar me përdoruesin e shërbimeve të pagesave, me ofruesit e tjerë të shërbimeve të pagesave dhe me subjekte të tjera, përfshirë edhe tregtarët, mbështetet në secilin nga elementet e mëposhtme:

a) një kod unik identifikimi të seancës;

b) mekanizmat e sigurisë për gjurmimin (*logging*) e hollësishëm të transaksionit, përfshirë numrin e transaksionit, vulën kohore (*timestamp*) të kryerjes së tij dhe të gjitha të dhënat përkatëse të transaksionit;

c) vulën kohore të kualifikuar (*timestamp*), sipas përcaktimeve në legjislacionin për identifikimin elektronik dhe shërbimet e besuara, e cila bazohet në një sistem të unifikuar të referencës kohore dhe sinkronizohet sipas një sinjali zyrtar kohor.

NËNKREU II
KËRKESA SPECIFIKE PËR STANDARDE TË PËRBASHKËTA, TË HAPURA DHE TË SIGURTA TË KOMUNIKIMIT

Neni 34
Detyrimet e përgjithshme për ndërfaqet e aksesit

1. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë që i ofrojnë një paguesi një llogari pagese të aksesueshme *online*, duhet të kenë të paktën një ndërfaqe, që plotëson secilën nga kërkesat e mëposhtme:

a) ofruesit e shërbimit të informimit të llogarisë, ofruesit e shërbimit të inicimit të pagesës dhe ofruesit e shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta, janë në gjendje të identifikojnë veten e tyre kundrejt ofruesit të shërbimit të pagesës për shërbimin e llogarisë;

b) ofruesit e shërbimit të informimit të llogarisë janë në gjendje të komunikojnë në mënyrë të sigurt, për të kërkuar dhe për të marrë informacion mbi një ose më shumë llogari të përcaktuara pagese, si dhe mbi transaksionet e pagesave që lidhen me këto llogari;

c) ofruesit e shërbimit të inicimit të pagesës janë në gjendje të komunikojnë në mënyrë të sigurt për të iniciuar një urdhërpagesë nga llogaria e pagesës së paguesit dhe për të marrë të gjithë informacionin mbi inicimin e transaksionit të pagesës dhe të gjithë informacionin e aksesueshëm për ofruesit e shërbimit të pagesës për shërbimin e llogarisë në lidhje me ekzekutimin e transaksionit të pagesës.

2. Për qëllime të autentifikimit të përdoruesit të shërbimeve të pagesave, ndërfaqja e parashikuar në pikën 1, të këtij neni, i lejon ofruesit të shërbimit të informimit të llogarisë dhe ofruesit të shërbimit të inicimit të pagesës, të mbështetet në të gjitha procedurat e

autentifikimit të ofruara nga ofruesi i shërbimit të pagesës për shërbimin e llogarisë te përdoruesi i shërbimeve të pagesave.

3. Ndërfaqja e parashikuar në pikën 1, të këtij neni, duhet të plotësojë të paktën kërkesat e mëposhtme:

a) një ofrues i shërbimit të inicimit të pagesës ose një ofrues i shërbimit të informimit të llogarisë të jetë në gjendje të udhëzojë ofruesin e shërbimit të pagesës për shërbimin e llogarisë, të fillojë autentifikimin bazuar në pëlqimin e përdoruesit të shërbimeve të pagesave;

b) seancat e komunikimit ndërmjet ofruesit të shërbimit të pagesës për shërbimin e llogarisë, ofruesit të shërbimit të informimit të llogarisë, ofruesit të shërbimit të inicimit të pagesës dhe çdo përdoruesi të shërbimeve të pagesave në fjalë, krijohen dhe mirëmbahen gjatë gjithë autentifikimit;

c) sigurohet integriteti dhe konfidencialiteti i kredencialeve të personalizuara të sigurisë dhe i kodeve të autentifikimit të transmetuara nga ose nëpërmjet ofruesit të shërbimit të inicimit të pagesës ose ofruesit të shërbimit të informimit të llogarisë.

4. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë sigurojnë që ndërfaqet e tyre të ndjekin standardet e komunikimit të aplikueshme në Bashkimin Evropian.

5. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë gjithashtu sigurojnë që specifikimi teknik i secilës ndërfaqe, dokumentohet duke specifikuar një sërë protokollesh dhe mjetesh që nevojiten nga ofruesit e shërbimit të inicimit të pagesës, ofruesit e shërbimit të informimit të llogarisë dhe ofruesit e shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta, për të lejuar programet dhe aplikacionet e tyre të ndërveprojnë me sistemet e ofruesve të shërbimit të pagesës për shërbimin e llogarisë.

6. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë, të paktën 6 muaj para datës së synuar të prezantimit në treg të ndërfaqes së aksesit, vënë në dispozicion pa pagesë dokumentacionin, me kërkesë të ofruesve të shërbimit të inicimit të pagesës, ofruesve të shërbimit të informimit të llogarisë dhe ofruesve të shërbimeve të pagesave që emetojnë instrumente pagesash të bazuara në karta, të licencuar ose të regjistruar, ose ofruesve të shërbimeve të pagesave që kanë aplikuar në Bankën e Shqipërisë për licencën apo regjistrimin përkatës, si dhe publikojnë një përmbledhje të dokumentacionit në faqen e tyre të internetit.

7. Përveç sa parashikohet në pikat 4–6 të këtij neni, ofruesit e shërbimit të pagesës për shërbimin e llogarisë sigurojnë që, përveç se në rastet e situatave emergjente që vijnë nga fatkeqësitë natyrore, gabimi njerëzor apo ndërhyrjet e qëllimshme, çdo ndryshim në specifikimin teknik të ndërfaqes së tyre, vihet paraprakisht në dispozicion të ofruesve të shërbimit të inicimit të pagesës, ofruesve të shërbimit të informimit të llogarisë dhe ofruesve të shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta, të licencuar ose të regjistruar, ose të ofruesve të shërbimeve të pagesave që kanë aplikuar në Bankën e Shqipërisë për licencën apo regjistrimin përkatës, sa më parë të jetë e mundur dhe jo më pak se 3 muaj para se të zbatohet ky ndryshim.

8. Ofruesit e shërbimeve të pagesave dokumentojnë situatat emergjente ku janë zbatuar ndryshime dhe vendosin dokumentacionin në dispozicion të Bankës së Shqipërisë, sipas kërkesës së kësaj të fundit.

9. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë vënë në dispozicion një strukturë testimi, përfshirë suportin për lidhjen dhe testimin funksional, që t'u mundësojnë ofruesve të shërbimit të inicimit të pagesës, ofruesve të shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta dhe ofruesve të shërbimit të informimit të llogarisë, të licencuar ose të regjistruar, ose ofruesve të shërbimeve të pagesave që kanë aplikuar në

Bankën e Shqipërisë për licencën apo regjistrimin përkatës, testimin e programeve dhe aplikacioneve të tyre të përdorura për ofrimin e një shërbimi pagese për përdoruesit. Kjo strukturë testimi vihet në dispozicion të paktën 6 muaj para datës së synuar të prezantimit në treg të ndërfaqes së aksesit. Në çdo rast, asnjë informacion sensitiv nuk do të shpërndahet nëpërmjet strukturës së testimit.

10. Banka e Shqipërisë monitoron ofruesit e shërbimit të pagesës për shërbimin e llogarisë që të jenë në përputhje në çdo kohë me detyrimet e përfshira në këto standarde në lidhje me ndërfaqen/et që ata vendosin. Në rast se një ofrues i shërbimit të pagesës për shërbimin e llogarisë nuk i plotëson kërkesat për ndërfaqet e përcaktuara në këto standarde, Banka e Shqipërisë monitoron që sigurimi i shërbimit të inicimit të pagesës dhe shërbimit të informimit të llogarisë të mos pengohet ose të ndërpritet, në masën që ofruesit e shërbimeve të tilla të jenë në përputhje me kushtet e përcaktuara në pikën 5, të nenit 37, të kësaj rregulloreje.

Neni 35

Opsionet e aksesit në ndërfaqe

Ofruesit e shërbimit të pagesës për shërbimin e llogarisë krijojnë ndërfaqen/et e referuara në nenin 34, të kësaj rregulloreje, nëpërmjet një ndërfaqeje të dedikuar ose nëpërmjet lejimit të përdorimit nga ofruesit e shërbimeve të pagesave të referuar në pikën 1, të nenit 34, të kësaj rregulloreje, të ndërfaqeve të përdorura për autentifikimin dhe komunikimin me përdoruesit e shërbimeve të pagesave të ofruesve të shërbimit të pagesës për shërbimin e llogarisë.

Neni 36

Detyrimi për një ndërfaqe të dedikuar

1. Në përputhje me nenet 34 dhe 35, të kësaj rregulloreje, ofruesit e shërbimit të pagesës për shërbimin e llogarisë që kanë krijuar (vendosur) një ndërfaqe të dedikuar, sigurohen që ndërfaqja e dedikuar ofron në çdo kohë të njëjtin nivel të disponueshmërisë dhe performancës, duke përfshirë suportin, si ndërfaqet e vëna në dispozicion të përdoruesit të shërbimeve të pagesave për të aksesuar direkt llogarinë e tij të pagesës *online*.

2. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë që kanë krijuar (vendosur) një ndërfaqe të dedikuar, përcaktojnë në mënyrë transparente treguesit kryesorë të performancës dhe objektivat e nivelit të shërbimit, të cilët janë të paktën po aq striktë sa ata të vendosur për ndërfaqen e përdorur nga përdoruesit e tyre të shërbimeve të pagesave, për sa i përket disponueshmërisë dhe të dhënave të siguruara në përputhje me nenin 40 të kësaj rregulloreje. Këto ndërfaqe, tregues dhe objektiva monitorohen nga Banka e Shqipërisë dhe testohen nga ofruesit e shërbimit të pagesës për shërbimin e llogarisë nëpërmjet "*stress-test*-eve".

3. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë që kanë krijuar (vendosur) një ndërfaqe të dedikuar, sigurojnë që kjo ndërfaqe të mos krijojë pengesa për ofrimin e shërbimeve të inicimit të pagesës dhe të informimit të llogarisë. Pengesa të tilla mund të përfshijnë, pengimin e përdorimit nga ofruesit e shërbimeve të pagesave, të përcaktuar në pikën 1, të nenit 34, të kësaj rregulloreje, të kredencialeve të lëshuara nga ofruesit e shërbimit të pagesës për shërbimin e llogarisë për klientët e tyre, imponimin e riorientimit drejt autentifikimit ose funksioneve të tjera të ofruesit të shërbimit të pagesës për shërbimin e llogarisë, që kërkojnë licencim dhe regjistrim shtesë përveç atyre të parashikuara në nenet 13

dhe 16, të ligjit "Për shërbimet e pagesave", ose që kërkojnë kontrolle shtesë të pëlqimit të dhënë nga përdoruesit e shërbimeve të pagesave për ofruesit e shërbimit të inicimit të pagesës dhe të informimit të llogarisë.

4. Për qëllime të pikave 1 dhe 2 të këtij neni, ofruesit e shërbimit të pagesës për shërbimin e llogarisë monitorojnë disponueshmërinë dhe performancën e ndërfaqes së dedikuar. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë publikojnë në faqen e tyre të internetit, statistikat tremujore mbi disponueshmërinë dhe performancën e ndërfaqes së dedikuar dhe të ndërfaqes së përdorur nga përdoruesit e shërbimeve të tyre të pagesave.

Neni 37

Masat për ngjarje të paparashikuara (masat e emergjencës) për një ndërfaqe të dedikuar

1. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë përfshijnë në krijimin e ndërfaqes së dedikuar, një strategji dhe plane për masat e emergjencës, në rastet kur ndërfaqja nuk funksionon në përputhje me nenin 36 të kësaj rregulloreje, në rastet kur ka një mosfunksionim të paplanifikuar të ndërfaqes ose në rastet kur ekziston një rënie e sistemeve. Mosfunksionimi i paplanifikuar ose rënia e sistemeve supozohet se ka ndodhur, kur pas pesë kërkesave radhazi për akses në informacion për ofrimin e shërbimeve të inicimit të pagesës ose të informimit të llogarisë, nuk ka një përgjigje brenda 30 sekondave.

2. Masat e emergjencës përfshijnë plane komunikimi për të informuar ofruesit e shërbimeve të pagesave që përdorin ndërfaqen e dedikuar, mbi masat për të rikthyer sistemin në gjendje normale dhe një përshkrim të opsioneve alternative që ofruesit e shërbimeve të pagesave mund të kenë të disponueshme gjatë kësaj kohe.

3. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë, si dhe ofruesit e shërbimit të pagesës të parashikuar në pikën 1, të nenit 34, të kësaj rregulloreje, raportojnë menjëherë në Bankën e Shqipërisë, problemet me ndërfaqet e dedikuara të parashikuara në pikën 1 të këtij neni.

4. Ofruesit e shërbimeve të pagesave të parashikuar në pikën 1 të nenit 34 të kësaj rregulloreje, si pjesë të një mekanizmi të emergjencës (*contingency mechanism*), lejohen të përdorin ndërfaqet e vëna në dispozicion të përdoruesve të shërbimeve të pagesave për autentifikimin dhe komunikimin me ofruesin e tyre të shërbimit të pagesës për shërbimin e llogarisë, deri sa ndërfaqja e dedikuar të rikthehet në nivelin e disponueshmërisë dhe performancës së parashikuar në nenin 36, të kësaj rregulloreje.

5. Referuar mekanizmit të përshkruar në pikën 4, të këtij neni, ofruesit e shërbimit të pagesës për shërbimin e llogarisë sigurojnë që ofruesit e shërbimeve të pagesave të parashikuar në pikën 1, të nenit 34, të kësaj rregulloreje, mund të identifikohen dhe të mbështeten në procedurat e autentifikimit të ofruara nga ofruesi i shërbimit të pagesës për shërbimin e llogarisë, për përdoruesit e shërbimeve të pagesave. Në rastet kur ofruesit e shërbimeve të pagesave të parashikuar në pikën 1, të nenit 34, të kësaj rregulloreje, përdorin ndërfaqen e parashikuar në pikën 4, të këtij neni, ata:

a) marrin masat e nevojshme për të siguruar që të mos aksesojnë, ruajnë ose përpunojnë të dhënat, për qëllime të tjera përveç ofrimit të shërbimit siç kërkohet nga përdoruesi i shërbimeve të pagesave;

b) vazhdojnë të respektojnë detyrimet përkatëse në zbatim të kërkesave të pikës 3 të nenit 59 dhe pikës 2, të nenit 60, të ligjit "Për shërbimet e pagesave";

c) gjurmojnë (*log*) të dhënat që janë aksesuar nëpërmjet ndërfaqes së operuar nga ofruesi i shërbimit të pagesës për shërbimin e llogarisë për përdoruesit e tij të shërbimeve të pagesave dhe vënë në dispozicion të Bankës së Shqipërisë, me kërkesë të kësaj të fundit dhe pa vonesa të panevojshme, skedarët e gjurmëve (*log files*);

d) i paraqesin Bankës së Shqipërisë, me kërkesë të kësaj të fundit dhe pa vonesa të panevojshme, arsyet mbi përdorimin e ndërfaqes së vënë në dispozicion të përdoruesve të shërbimeve të pagesave për të aksesuar drejtpërdrejt llogarinë e pagesave *online*;

e) informojnë ofruesin përkatës të shërbimit të pagesës për shërbimin e llogarisë.

6. Banka e Shqipërisë mund të përjashtojë ofruesit e shërbimit të pagesës për shërbimin e llogarisë, që kanë zgjedhur një ndërfaqe të dedikuar, nga detyrimi për të krijuar mekanizmat e përshkruar në pikën 4, të këtij neni, nëse ndërfaqja e dedikuar plotëson të gjitha kushtet e mëposhtme:

a) plotëson të gjitha detyrimet për ndërfaqet e dedikuara, siç përcaktohet në nenin 36 të kësaj rregulloreje;

b) është krijuar dhe testuar në përputhje me pikën 9 të nenit 34 të kësaj rregulloreje, për përmbushjen e kërkesave të ofruesve të shërbimeve të pagesave, të parashikuar në atë pikë;

c) është përdorur gjerësisht për të paktën 3 muaj nga ofruesit e shërbimeve të pagesave për të ofruar shërbimin e informimit të llogarisë, shërbimin e inicimit të pagesës dhe për të siguruar konfirmimin e disponueshmërisë së fondeve për pagesat e bazuara në karta;

d) çdo problem në lidhje me ndërfaqen e dedikuar është zgjidhur pa vonesa të panevojshme.

7. Banka e Shqipërisë anulon përjashtimin e parashikuar në pikën 6 të këtij neni, kur kushtet e parashikuara në shkronjat "a" dhe "d" nuk plotësohen nga ofruesit e shërbimit të pagesës për shërbimin e llogarisë, për më shumë se 2 javë kalendarike, rresht. Banka e Shqipërisë sigurohet që ofruesit e shërbimit të pagesës për shërbimin e llogarisë vendosin brenda kohës më të shkurtër të mundshme dhe maksimalisht brenda 2 muajve, mekanizmat e emergjencës të parashikuar në pikën 4 të këtij neni.

Neni 38

Certifikatat e kualifikuara elektronike

1. Për qëllime të identifikimit elektronik të sigurt, siç referohet në shkronjën "a" të pikës 1 të nenit 34 të kësaj rregulloreje, ofruesit e shërbimeve të pagesave do të mbështeten në certifikatat e kualifikuara për vulat elektronike ose në certifikatat e kualifikuara për autentifikimin e faqeve të internetit, sipas përcaktimeve në legjislacionin për identifikimin elektronik dhe shërbimet e besuara.

2. Për qëllime të kësaj rregulloreje, numri unik i identifikimit ose numri i regjistrimit, siç është regjistruar në të dhënat zyrtare, që parashikohet në legjislacionin për identifikimin elektronik dhe shërbimet e besuara, do të jetë numri i licencës ose i vendimit të ofruesit të shërbimit të pagesës që emeton instrumente pagese të bazuara në karta, ofruesit të shërbimit të informimit të llogarisë, ofruesit të shërbimit të inicimit të pagesës, përfshirë edhe ofruesit e shërbimit të pagesës për shërbimin e llogarisë që ofrojnë këto shërbime, të regjistruar në regjistrin publik të Bankës së Shqipërisë, në përputhje me nenin 16, të ligjit "Për shërbimet e pagesave" dhe me nenin 128, të ligjit "Për bankat".

3. Për qëllime të kësaj rregulloreje, certifikatat e kualifikuara për vulat elektronike ose për autentifikimin e faqeve të internetit, të referuara në pikën 1 të këtij neni, duhet të plotësojnë kërkesat e përcaktuara në legjislacionin për identifikimin elektronik dhe shërbimet e besuara,

si dhe duhet të përfshijnë në një gjuhë të zakonshme e të përdorshme, në financat ndërkombëtare, të dhëna specifike shtesë në lidhje me elementet e mëposhtme:

a) rolin e ofruesit të shërbimeve të pagesave, i cili mund të përfshijë një ose disa nga të mëposhtmit:

i. shërbimin e llogarisë,

ii. inicimin e pagesës,

iii. informimin e llogarisë,

iv. emetimin e instrumenteve të pagesave të bazuara në karta;

b) Bankën e Shqipërisë, si autoriteti që ka regjistruar ofruesin e shërbimeve të pagesave.

4. Të dhënat e parashikuara në pikën 3 të këtij neni nuk ndikojnë ndërveprueshmërinë dhe njohjen e certifikatave të kualifikuara për vulat elektronike ose certifikatave të kualifikuara për autentifikimin e faqeve të internetit.

Neni 39

Siguria e seancës së komunikimit

1. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë, ofruesit e shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta, ofruesit e shërbimit të informimit të llogarisë dhe ofruesit e shërbimit të inicimit të pagesës, sigurojnë që, kur shkëmbejnë të dhëna nëpërmjet internetit, të zbatohet një enkriptim i sigurt midis palëve komunikuese, përgjatë të gjithë seancës përkatëse të komunikimit, në mënyrë që të ruhet konfidencialiteti dhe integriteti i të dhënave, duke përdorur teknika të thelluara dhe të njohura gjerësisht të enkriptimit.

2. Ofruesit e shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta, ofruesit e shërbimit të informimit të llogarisë dhe ofruesit e shërbimit të inicimit të pagesës i mbajnë seancat e aksesit të ofruara nga ofruesit e shërbimit të pagesës për shërbimin e llogarisë, sa më të shkurtra të jetë e mundur dhe përfundojnë në mënyrë aktive çdo seancë të tillë, sapo veprimi i kërkuar të jetë përfunduar.

3. Kur mbahen seanca të rrjeteve paralele me ofruesin e shërbimit të pagesës për shërbimin e llogarisë, ofruesit e shërbimit të informimit të llogarisë dhe ofruesit e shërbimit të inicimit të pagesës, duhet të sigurohen që këto seanca të jenë të lidhura në mënyrë të sigurt me seancat përkatëse të krijuara me përdoruesin (përdoruesit) e shërbimeve të pagesave, për të parandaluar mundësinë që çdo mesazh ose informacion i komunikuar ndërmjet tyre të mund të transmetohet në drejtimin e gabuar (*misrouted*).

4. Ofruesit e shërbimit të informimit të llogarisë, ofruesit e shërbimit të inicimit të pagesës dhe ofruesit e shërbimeve të pagesave që emetojnë instrumente pagese të bazuara në karta me ofruesin e shërbimit të pagesës për shërbimin e llogarisë duhet të përmbajnë referenca të qarta për secilën nga pikat e mëposhtme:

a) përdoruesit e shërbimeve të pagesave dhe seancën përkatëse të komunikimit, për të dalluar kërkesa të ndryshme nga i njëjti përdorues i shërbimeve të pagesave;

b) për shërbimin e inicimit të pagesës, transaksionin e iniciuar të pagesës të identifikueshëm në mënyrë unike;

c) për konfirmimin mbi disponueshmërinë e fondeve, kërkesën e identifikuar në mënyrë unike lidhur me shumën e nevojshme për ekzekutimin e transaksioneve të pagesave me kartë.

5. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë, ofruesit e shërbimit të informimit të llogarisë, ofruesit e shërbimit të inicimit të pagesës dhe ofruesit e shërbimeve

të pagesave që emetojnë instrumente pagese të bazuara në karta, duhet të sigurojnë që kur komunikojnë kredencialet e personalizuara të sigurisë dhe kodet e autentifikimit, ato të mos jenë të lexueshme, drejtpërdrejt ose në mënyrë të tërthortë, nga çdo punonjës, në çdo kohë.

6. Në rast të humbjes (cenimit) të konfidencialitetit të kredencialeve të personalizuara të sigurisë nën kompetencën (përgjegjësinë) e tyre, ofruesit e parashikuar në pikën 5 të këtij neni, informojnë menjëherë përdoruesin e shërbimeve të pagesave të lidhur me ta, si dhe emetuesin e kredencialeve të personalizuara të sigurisë.

Neni 40

Shkëmbimi i të dhënave

1. Ofruesit e shërbimit të pagesës për shërbimin e llogarisë plotësojnë kërkesat e mëposhtme:

a) u sigurojnë ofruesve të shërbimit të informimit të llogarisë, të njëjtin informacion mbi llogaritë e përcaktuara të pagesave dhe transaksionet e lidhura të pagesave, të vënë në dispozicion të përdoruesit të shërbimeve të pagesave, kur ky i fundit kërkon drejtpërdrejt akses në informacionin e llogarisë, me kusht që ky informacion të mos përfshijë të dhëna sensitive të pagesës;

b) u sigurojnë ofruesve të shërbimit të inicimit të pagesës, menjëherë pas marrjes së urdhërpagesës, të njëjtin informacion mbi inicimin dhe ekzekutimin e transaksionit të pagesës, të siguruar ose të vënë në dispozicion të përdoruesit të shërbimeve të pagesave kur transaksioni iniciohet drejtpërdrejt nga ky i fundit;

c) u sigurojnë ofruesve të shërbimeve të pagesave, menjëherë pas marrjes së kërkesës, një konfirmim në një format të thjeshtë "po" ose "jo", nëse shuma e nevojshme për ekzekutimin e një transaksioni pagese është e disponueshme në llogarinë e pagesës së paguesit.

2. Në rast të një gabimi të papritur ose incidenti kibernetik që ndodh gjatë procesit të identifikimit elektronik, autentifikimit ose shkëmbimit të elementeve të të dhënave, ofruesi i shërbimit të pagesës për shërbimin e llogarisë i dërgon një mesazh njoftimi ofruesit të shërbimit të inicimit të pagesës ose ofruesit të shërbimit të informimit të llogarisë dhe ofruesit të shërbimit të pagesës që emeton instrumente pagese të bazuara në karta, ku shpjegon arsyen e gabimit të papritur ose incidentit kibernetik.

3. Në rastet kur ofruesi i shërbimit të pagesës për shërbimin e llogarisë ofron një ndërfaqe të dedikuar në përputhje me nenin 36 të kësaj rregulloreje, ndërfaqja duhet të parashikojë edhe mesazhe njoftimi në lidhje me gabime të papritura ose incidente kibernetike që do të komunikohen nga çdo ofrues i shërbimeve të pagesave që zbulon gabimin ose incidentin, tek ofruesit e tjerë të shërbimeve të pagesave që marrin pjesë në seancën e komunikimit.

4. Ofruesit e shërbimit të informimit të llogarisë krijojnë mekanizma të përshtatshëm dhe efektivë për parandalimin e aksesit në informacione të ndryshme nga informacionet mbi llogaritë e përcaktuara të pagesave dhe transaksionet e pagesave të lidhura me to, sipas pëlqimit të qartë të dhënë nga përdoruesi.

5. Ofruesit e shërbimit të inicimit të pagesës u sigurojnë ofruesve të shërbimit të pagesës për shërbimin e llogarisë, të njëjtin informacion, siç kërkohet nga përdoruesi i shërbimeve të pagesave, kur inicion direkt transaksionin e pagesës.

6. Ofruesit e shërbimit të informimit të llogarisë do të jenë në gjendje të përdorin informacionin nga llogaritë e përcaktuara të pagesave dhe transaksionet e pagesave të lidhura

me to, të mbajtur nga ofruesit e shërbimit të pagesës për shërbimin e llogarisë, për qëllimet e kryerjes së shërbimit të informimit të llogarisë në secilën prej rrethanave të mëposhtme:

a) sa herë që përdoruesi i shërbimeve të pagesave kërkon në mënyrë aktive një informacion të tillë;

b) kur përdoruesi i shërbimeve të pagesave nuk kërkon në mënyrë aktive një informacion të tillë, jo më shumë se katër herë brenda një periudhe 24-orëshe, përveç rastit kur është rënë dakord për një frekuencë më të lartë, nëpërmjet një marrëveshjeje midis ofruesit të shërbimit të informimit të llogarisë dhe ofruesit të shërbimit të pagesës për shërbimin e llogarisë, me pëlqimin e përdoruesit të shërbimeve të pagesave.

KREU VII
KËRKESA MBIKËQYRËSE

Neni 41
Masat mbikëqyrëse

Banka e Shqipërisë, në rast mosplotësimi të kërkesave të kësaj rregulloreje, zbaton masat mbikëqyrëse dhe/ose ndëshkimore të parashikuara në nenin 25 dhe në kreun I, të titullit V, të ligjit "Për shërbimet e pagesave".

Neni 42
Hyrja në fuqi

Kjo rregullore hyn në fuqi në datë 1 janar 2024.

KRYETAR I KËSHILLIT MBIKËQYRËS
Gent Sejko

ANEKS 1

Vlera e kufirit të përjashtimit (VKP)	NORMA REFERENCË E MASHTRIMIT (NË %)	
	Për pagesat elektronike me kartë në distancë	**Për transfertat elektronike të kreditit në distancë**
Vlera ekuivalente në lekë e shumës 500 euro	0.01	0.005
Vlera ekuivalente në lekë e shumës 250 euro	0.06	0.01
Vlera ekuivalente në lekë e shumës 100 euro	0.13	0.015