REGULAMENTUL DELEGAT (UE) 2018/389 AL COMISIEI

din 27 noiembrie 2017

de completare a Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea strictă a clienților și standardele deschise, comune și sigure de comunicare

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010 și de abrogare a Directivei 2007/64/CE ([1]), în special articolul 98 alineatul (4),

întrucât:

(1) Serviciile de plată oferite electronic ar trebui să se desfășoare în condiții de siguranță, adoptând tehnologii capabile să garanteze o autentificare în siguranță a utilizatorului și să reducă, în cea mai mare măsură cu putință, riscul de fraudă. Procedura de autentificare ar trebui să includă, în general, mecanisme de monitorizare a operațiunilor pentru a detecta încercările de a utiliza elementele de securitate personalizate ale unui utilizator de servicii de plată care au fost pierdute, furate sau deturnate și ar trebui, de asemenea, să garanteze că utilizatorul serviciilor de plată este utilizatorul legitim și, prin urmare, își dă acordul pentru transferarea de fonduri și accesul la informațiile privind contul său, prin utilizarea normală a elementelor de securitate personalizate. În plus, este necesar să se precizeze cerințele privind autentificarea strictă a clienților care ar trebui să se aplice de fiecare dată când un plătitor își accesează contul de plăți online, inițiază o operațiune electronică de plată sau întreprinde o acțiune printr-un canal la distanță care poate implica un risc de fraudare a plății sau alte abuzuri, solicitând generarea unui cod de autentificare care ar trebui să fie rezistent la riscul de a fi falsificat în totalitate sau prin prezentarea elementelor pe baza cărora a fost generat codul respectiv.

(2) Deoarece metodele de fraudare sunt în permanentă schimbare, cerințele privind autentificarea strictă a clienților ar trebui să permită inovarea în ceea ce privește soluțiile tehnice care abordează apariția unor noi amenințări la adresa securității plăților electronice. Pentru a se asigura că cerințele stabilite sunt puse în aplicare în mod continuu și eficace, este, de asemenea, oportun să se solicite ca măsurile de securitate pentru aplicarea autentificării stricte a clienților și excepțările de la acestea, măsurile în vederea protejării confidențialității și a integrității elementelor de securitate personalizate, precum și măsurile de stabilire a standardelor deschise, comune și sigure de comunicare să fie documentate, testate periodic, evaluate și auditate de către auditori cu experiență în domeniul securității informatice și al plăților și independenți din punct de vedere operațional. Pentru ca autoritățile competente să fie în măsură să monitorizeze calitatea reexaminării acestor măsuri, astfel de reexaminări ar trebui să fie puse la dispoziția acestora, la cerere.

(3) Întrucât operațiunile electronice de plată la distanță sunt supuse unui risc mai ridicat de fraudă, este necesar să se introducă cerințe suplimentare pentru autentificarea strictă a clienților în cazul acestor operațiuni, asigurându-se că elementele asigură o legătură dinamică între operațiunea în cauză, o sumă și un beneficiar specificat de către plătitor în momentul inițierii operațiunii.

(4) Corelarea dinamică este posibilă prin generarea de coduri de autentificare care face obiectul unui set de cerințe stricte de securitate. Pentru punerea în aplicare a codurilor de autentificare nu ar trebui să fie solicitată o anumită tehnologie, astfel încât aceasta să rămână neutră în sine. Prin urmare, codurile de autentificare ar trebui să se bazeze pe soluții precum generarea și validarea de parole unice, semnături digitale sau alte afirmații de validitate care utilizează chei criptografice sau materiale criptografice stocate în elementele de autentificare, atât timp cât sunt îndeplinite cerințele de securitate.

([1]) JO L 337, 23.12.2015, p. 35.

(5) Este necesar să se stabilească cerințe specifice pentru situația în care cuantumul final nu este cunoscut la momentul în care plătitorul inițiază o operațiune electronică de plată la distanță, în scopul de a garanta că autentificarea strictă a clienților este specifică pentru cuantumul maxim pentru care plătitorul și-a exprimat consimțământul, astfel cum se menționează în Directiva (UE) 2015/2366.

(6) În scopul de a garanta aplicarea autentificării stricte a clienților, este, de asemenea, necesar să se impună caracteristici de securitate adecvate pentru elementele de autentificare strictă a clienților clasificate drept cunoștințe (ceva ce doar utilizatorul cunoaște), cum ar fi lungimea sau complexitatea, pentru elementele clasificate drept posesie (ceva ce doar utilizatorul posedă), cum ar fi specificațiile algoritmilor, lungimea cheii și entropia informațională, precum și pentru dispozitivele și programele informatice care citesc elemente calificate drept inerență (ceva ce utilizatorul este), cum ar fi specificațiile algoritmilor, caracteristicile senzorilor biometrici și de protecție a modelelor, în special pentru a atenua riscul ca aceste elemente să fie citite, divulgate sau utilizate de persoane neautorizate. Este necesar, de asemenea, să se stabilească cerințe pentru a se asigura că aceste elemente sunt independente, astfel încât nerespectarea uneia să nu compromită fiabilitatea celorlalte, în special când oricare dintre aceste elemente este utilizat prin intermediul unui dispozitiv cu scopuri multiple, și anume un dispozitiv precum o tabletă sau un telefon mobil care poate fi folosit atât pentru a oferi instrucțiuni de efectuare a plății, cât și în procesul de autentificare.

(7) Cerințele privind autentificarea strictă a clienților se aplică plăților inițiate de către plătitor, indiferent dacă plătitorul este o persoană fizică sau o entitate juridică.

(8) Prin însăși natura lor, plățile efectuate prin utilizarea instrumentelor de plată anonime nu sunt supuse obligației de autentificare strictă a clienților. În cazul în care anonimatul acestor instrumente este îndepărtat din motive contractuale sau legislative, plățile se supun cerințelor de securitate care rezultă din Directiva (UE) 2015/2366 și din prezentul standard tehnic de reglementare.

(9) În conformitate cu Directiva (UE) 2015/2366, derogările de la principiul autentificării stricte a clienților au fost definite în funcție de nivelul de risc, valoarea, recurența și canalul de plată utilizat pentru executarea operațiunii de plată.

(10) Acțiunile care implică accesul la sold și la operațiunile recente ale unui cont de plăți fără divulgarea de date sensibile privind plățile, plățile recurente către aceiași beneficiari care au fost deja instituite sau confirmate de către plătitor prin utilizarea autentificării stricte a clienților, precum și privind plățile către și de la aceeași persoană fizică sau juridică cu conturi la același prestator de servicii de plată prezintă un nivel scăzut de risc, permițând, astfel, prestatorilor de servicii de plată să nu aplice autentificarea strictă a clienților. Se lasă deoparte faptul că, în conformitate cu articolele 65, 66 și 67 din Directiva (UE) 2015/2366, prestatorii de servicii de inițiere a plății, prestatorii de servicii de plată care emit instrumente de plată pe bază de card și prestatorii de servicii de informare cu privire la conturi ar trebui să solicite și să obțină informațiile necesare și esențiale exclusiv de la prestatorul de servicii de plată care oferă servicii de administrare cont pentru prestarea unui anumit serviciu de plată cu consimțământul utilizatorului serviciilor de plată. Acest consimțământ poate fi acordat în mod individual pentru fiecare cerere de informații sau pentru fiecare plată care urmează să fie inițiată ori, pentru prestatorii de servicii de informare cu privire la conturi, ca un mandat pentru conturile de plată desemnate și operațiunile de plată aferente, astfel cum a fost stabilit în acordul contractual cu utilizatorul serviciilor de plată.

(11) Derogările pentru plățile contactless cu valoare scăzută, efectuate la punctele de vânzare, care iau în considerare și un număr maxim de operațiuni consecutive sau o anumită valoare maximă fixă a operațiunilor consecutive fără aplicarea autentificării stricte a clienților, permit dezvoltarea unor servicii de plată ușor de utilizat și cu un nivel scăzut de risc și, prin urmare, ar trebui prevăzute. Este de asemenea oportun să se stabilească o derogare pentru cazul în care operațiunile electronice de plată inițiate la terminale neasistate unde utilizarea autentificării stricte a clienților nu poate fi întotdeauna ușor de aplicat din cauza unor motive operaționale (de exemplu, pentru a evita cozile și accidentele potențiale la barierele automate sau pentru alte riscuri de siguranță sau securitate).

(12) Similar cu derogarea pentru plățile contactless cu valoare scăzută efectuate la punctul de vânzare, trebuie să se ajungă la un echilibru adecvat între interesul unei securități sporite în cazul plăților la distanță și necesitățile legate de ușurința utilizării și accesibilitatea plăților în domeniul comerțului electronic. În conformitate cu aceste principii, ar trebui stabilite într-o manieră prudentă praguri sub care nu este necesar să se aplice autentificarea strictă a clienților și care să acopere numai achizițiile online cu valoare scăzută. Pragurile pentru achizițiile online ar trebui stabilite cu mai multă prudență, luând în considerare faptul că, întrucât persoana nu este prezentă fizic atunci când se efectuează achiziția, riscul de securitate implicat este ușor mai ridicat.

(13) Cerințele privind autentificarea strictă a clienților se aplică plăților inițiate de către plătitor, indiferent dacă plătitorul este o persoană fizică sau o entitate juridică. Multe plăți ale întreprinderilor sunt inițiate prin intermediul unor procese sau protocoale specifice care garantează un nivel ridicat de securitate în materie de plăți pe care Directiva (UE) 2015/2366 vizează să îl atingă prin intermediul autentificării stricte a clienților. În cazul în care autoritățile competente constată că procesele și protocoalele de plată respective care sunt puse doar la dispoziția plătitorilor care nu sunt consumatori îndeplinesc obiectivele Directivei (UE) 2015/2366 în materie de securitate, prestatorii de servicii de plată pot, în ceea ce privește procesele sau protocoalele în cauză, să fie scutiți de cerințele privind autentificarea strictă a clienților.

(14) În cazul unei analize a riscurilor aferente operațiunilor în timp real care clasifică o operațiune de plată cu risc redus, este, de asemenea, oportun să se introducă o derogare pentru prestatorii de servicii de plată care intenționează să nu aplice autentificarea strictă a clienților și să adopte în schimb cerințe eficace și bazate pe riscuri care să garanteze siguranța fondurilor și a datelor cu caracter personal ale utilizatorului serviciilor de plată. Aceste cerințe bazate pe risc ar trebui să combine punctajele din analiza de risc, care să confirme absența unor cheltuieli anormale sau a unui model anormal de comportament al plătitorului, luând în considerare alți factori de risc, printre care informațiile privind poziția geografică a plătitorului și a beneficiarului plății, cu praguri monetare bazate pe ratele de fraudă calculate pentru plățile la distanță. În cazul în care, pe baza analizei de risc a operațiunilor în timp real, o plată nu poate fi considerată ca prezentând un nivel scăzut de risc, prestatorul de servicii de plată ar trebui să revină la autentificarea strictă a clienților. Valoarea maximă a unei astfel de derogări bazate pe risc ar trebui stabilită astfel încât să asigure o rată aferentă foarte scăzută de fraudă și prin comparație cu ratele de fraudă ale tuturor operațiunilor de plată efectuate de prestatorul de servicii de plată, inclusiv cele autentificate prin autentificarea strictă a clienților, într-o anumită perioadă de timp și în mod constant.

(15) Pentru asigurarea unei aplicări eficiente, prestatorii de servicii de plată care doresc să beneficieze de derogări de la autentificarea strictă a clienților ar trebui să monitorizeze în mod regulat și să pună la dispoziția autorităților competente și a Autorității Bancare Europene (ABE), la cererea acestora, pentru fiecare tip de operațiune de plată, valoarea operațiunilor de plată frauduloase sau neautorizate, precum și ratele de fraudă înregistrate pentru toate operațiunile de plată efectuate, indiferent dacă acestea sunt autentificate prin intermediul autentificării stricte a clienților sau executate în temeiul unei derogări corespunzătoare.

(16) Colectarea acestor noi dovezi istorice privind ratele de fraudă ale operațiunilor electronice de plată va contribui, de asemenea, la o reexaminare eficientă de către ABE a pragurilor de derogare de la autentificarea strictă a clienților, pe baza unei analize de risc a operațiunilor în timp real. ABE ar trebui să revizuiască și să prezinte Comisiei un proiect de actualizare a acestor standarde tehnice de reglementare, dacă este cazul, propunând noi proiecte de praguri și de rate corespunzătoare de fraudă, cu scopul de a consolida securitatea plăților electronice la distanță, în conformitate cu articolul 98 alineatul (5) din Directiva (UE) 2015/2366 și cu articolul 10 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([1]).

(17) Prestatorilor de servicii de plată care recurg la oricare dintre derogările care urmează să fie prevăzute ar trebui să li se permită, în orice moment, să aleagă să aplice autentificarea strictă a clienților pentru acțiunile și operațiunile de plată menționate în dispozițiile respective.

(18) Măsurile care protejează confidențialitatea și integritatea elementelor de securitate personalizate, precum și dispozitivele și programele informatice de autentificare ar trebui să limiteze riscurile legate de fraudele săvârșite prin utilizarea neautorizată sau frauduloasă a instrumentelor de plată și accesul neautorizat la conturile de plăți. În acest scop, este necesar să se introducă cerințe privind crearea și transmiterea în siguranță a elementelor de securitate personalizate și privind asocierea acestora cu utilizatorul serviciilor de plată și să se prevadă condițiile pentru reînnoirea și dezactivarea elementelor respective.

(19) Pentru a asigura comunicarea eficace și sigură între actorii relevanți în contextul serviciilor de informare cu privire la conturi, al serviciilor de inițiere a plăților și al confirmării disponibilității fondurilor, este necesar să se precizeze cerințele din standardele deschise, comune și sigure de comunicare care trebuie respectate de către toți prestatorii de servicii de plată relevanți. Directiva (UE) 2015/2366 prevede accesul la informațiile privind contul de plăți și utilizarea acestor informații de către prestatorii de servicii de informare cu privire la conturi. Prin urmare, prezentul regulament nu modifică normele de acces la alte conturi decât cele de plăți.

([1]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12).

(20) Fiecare prestator de servicii de plată care oferă servicii de administrare cont cu conturi de plăți care sunt accesibile online ar trebui să ofere cel puțin o interfață de acces care să permită o comunicare sigură cu prestatorii de servicii de informare cu privire la conturi, cu prestatorii de servicii de inițiere a plății și cu prestatorii de servicii de plată care emit instrumente de plată pe bază de card. Interfața ar trebui să le permită prestatorilor de servicii de informare cu privire la conturi, prestatorilor de servicii de inițiere a plății și prestatorilor de servicii de plată care emit instrumente de plată pe bază de card să se identifice prestatorului de servicii de plată care oferă servicii de administrare cont. De asemenea, interfața ar trebui să le permită prestatorilor de servicii de informare cu privire la conturi și prestatorilor de servicii de inițiere a plății să se bazeze pe procedurile de autentificare furnizate de prestatorul de servicii de plată care oferă servicii de administrare cont utilizatorului serviciilor de plată. Pentru a asigura neutralitatea modelelor tehnologice și de afaceri, prestatorii de servicii de plată care oferă servicii de administrare cont ar trebui să fie liberi să decidă dacă să ofere o interfață care să fie dedicată comunicării cu prestatorii de servicii de informare cu privire la conturi, cu prestatorii de servicii de inițiere a plății și cu prestatorii de servicii de plată care emit instrumente de plată pe bază de card sau să permită, pentru respectiva comunicare, utilizarea interfeței de identificare și comunicare cu utilizatorii serviciilor de plată ai prestatorilor de servicii de plată care oferă servicii de administrare cont.

(21) Pentru ca prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății și prestatorii de servicii de plată care emit instrumente de plată pe bază de card să poată să își dezvolte soluțiile tehnice, specificațiile tehnice ale interfeței ar trebui să fie documentate în mod corespunzător și puse la dispoziția publicului. Mai mult, prestatorul de servicii de plată care oferă servicii de administrare cont ar trebui să ofere un mecanism care să le permită prestatorilor de servicii de plată să testeze soluțiile tehnice cu cel puțin șase luni înainte de data punerii în aplicare a prezentelor standarde de reglementare sau, în cazul în care lansarea are loc după data aplicării prezentelor standarde, înainte de data la care interfața va fi lansată pe piață. Pentru a asigura interoperabilitatea diferitelor soluții tehnologice de comunicare, interfața ar trebui să utilizeze standarde de comunicare elaborate de organizații de standardizare internaționale sau europene.

(22) Calitatea serviciilor oferite de prestatorii de servicii de informare cu privire la conturi și de prestatorii de servicii de inițiere a plății va depinde de funcționarea corectă a interfețelor instituite sau adaptate de către prestatorii de servicii de plată care oferă servicii de administrare cont. Prin urmare, este important ca, în cazul nerespectării de către aceste interfețe a dispozițiilor cuprinse în prezentele standarde, să fie luate măsuri pentru garantarea continuității activității în beneficiul utilizatorilor acestor servicii. Este responsabilitatea autorităților naționale competente să se asigure că prestatorii de servicii de informare cu privire la conturi și prestatorii de servicii de inițiere a plății nu sunt blocați sau obstrucționați în momentul prestării serviciilor lor.

(23) În cazul în care accesul la conturile de plăți este oferit prin intermediul unei interfețe specifice, pentru a garanta dreptul utilizatorilor serviciilor de plată de a face uz de serviciile de inițiere a plății și de serviciile care permit accesul la informații privind contul, astfel cum se prevede în Directiva (UE) 2015/2366, este necesar să se solicite ca interfețele specifice să aibă același nivel de disponibilitate și de performanță ca interfața pusă la dispoziția utilizatorului serviciilor de plată. Prestatorii de servicii de plată care oferă servicii de administrare cont ar trebui, de asemenea, să definească indicatori-cheie de performanță și obiective transparente privind nivelul serviciilor pentru gradul de disponibilitate și de performanță al interfețelor specifice care să fie cel puțin la fel de stricte precum cele pentru interfața folosită pentru propriii utilizatori ai serviciilor de plată. Interfețele respective ar trebui testate de către prestatorii de servicii de plată care urmează să le utilizeze și ar trebui să fie supuse unui test de rezistență și monitorizate de către autoritățile competente.

(24) Pentru a se asigura că prestatorii de servicii de plată care se bazează pe interfața specifică pot continua să își ofere serviciile în cazul unor probleme de disponibilitate sau al unei funcționări inadecvate, este necesar să se prevadă, în condiții stricte, un mecanism de rezervă care va permite acestor prestatori să utilizeze interfața pe care prestatorul de servicii de plată care oferă servicii de administrare cont o menține pentru identificarea propriilor utilizatori ai serviciilor de plată și pentru comunicarea cu aceștia. Anumiți prestatori de servicii de plată care oferă servicii de administrare cont vor fi scutiți de obligația de a furniza un astfel de mecanism de rezervă prin intermediul interfețelor lor cu clienții în cazul în care autoritățile lor competente stabilesc că interfețele specifice respectă anumite condiții care asigură o concurență fără îngrădire. În cazul în care interfețele specifice care fac obiectul derogării nu respectă condițiile necesare, derogările acordate sunt revocate de către autoritățile competente relevante.

(25) Pentru ca autoritățile competente să poată supraveghea și monitoriza în mod eficace punerea în aplicare și gestionarea interfețelor de comunicare, prestatorii de servicii de plată care oferă servicii de administrare cont ar trebui să pună la dispoziția publicului, pe site-ul lor internet, un rezumat al documentației relevante și să furnizeze, la cerere, autorităților competente documentele referitoare la soluțiile în caz de urgență. Prestatorii de servicii de plată care oferă servicii de administrare cont ar trebui, de asemenea, să pună la dispoziția publicului statistici cu privire la disponibilitatea și performanța respectivei interfețe.

(26) În scopul de a proteja confidențialitatea și integritatea datelor, trebuie să se asigure securitatea sesiunilor de comunicare dintre prestatorii de servicii de plată care oferă servicii de administrare cont, prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății și prestatorii de servicii de plată care emit

instrumente de plată pe bază de card. În special, este necesar să se solicite aplicarea criptării securizate între prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății, prestatorii de servicii de plată care emit instrumente de plată pe bază de card și prestatorii de servicii de plată care oferă servicii de administrare cont, atunci când fac schimb de date.

(27) Pentru a îmbunătăți încrederea utilizatorilor și a asigura o autentificare strictă a clienților, utilizarea mijloacelor de identificare electronică și a serviciilor de încredere, astfel cum se prevede în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([1]), ar trebui să fie luată în considerare, în special în ceea ce privește sistemele de identificare electronică notificate.

(28) Pentru a asigura alinierea datelor de aplicare, prezentul regulament ar trebui să se aplice de la aceeași dată de la care statele membre trebuie să asigure aplicarea măsurilor de securitate menționate la articolele 65, 66, 67 și 97 din Directiva (UE) 2015/2366.

(29) Prezentul regulament se bazează pe proiectul de standarde tehnice de reglementare transmis Comisiei de către Autoritatea Bancară Europeană (ABE).

(30) ABE a efectuat consultări publice deschise și transparente cu privire la proiectul de standarde tehnice de reglementare pe care se bazează prezentul regulament, a analizat costurile și beneficiile potențiale aferente și a solicitat punctul de vedere al Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1093/2010,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect

Prezentul regulament stabilește cerințele care trebuie respectate de prestatorii de servicii de plată în scopul punerii în aplicare a măsurilor de securitate care le permit următoarele:

(a) să aplice procedura de autentificare strictă a clienților, în conformitate cu articolul 97 din Directiva (UE) 2015/2366;

(b) să fie exceptați de la aplicarea cerințelor de securitate privind autentificarea strictă a clienților, sub rezerva unor condiții specifice și limitate în funcție de nivelul de risc, valoarea și frecvența operațiunii de plată și de canalul de plată utilizat pentru executarea acesteia;

(c) să protejeze confidențialitatea și integritatea elementelor de securitate personalizate ale utilizatorului serviciilor de plată;

(d) să stabilească standarde deschise, comune și sigure de comunicare între prestatorii de servicii de plată care oferă servicii de administrare cont, prestatorii de servicii de inițiere a plății, prestatorii de servicii de informare cu privire la conturi, plătitori, beneficiarii plății și alți prestatori de servicii de plată în ceea ce privește furnizarea și utilizarea serviciilor de plată în conformitate cu titlul IV din Directiva (UE) 2015/2366.

Articolul 2

Cerințe generale de autentificare

(1) Prestatorii de servicii de plată instituie mecanisme de monitorizare a operațiunilor care să le permită să identifice operațiunile de plată neautorizate sau frauduloase în scopul punerii în aplicare a măsurilor de securitate menționate la articolul 1 literele (a) și (b).

([1]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 53).

Mecanismele respective se bazează pe analiza operațiunilor de plată, ținând seama de elemente specifice ale utilizatorului serviciilor de plată în condiții de utilizare normală a elementelor de securitate personalizate.

(2) Prestatorii de servicii de plată se asigură că mecanismele de monitorizare a operațiunilor iau în considerare, ca o condiție minimă, fiecare dintre următorii factori bazați pe riscuri:

(a) listele de elemente de autentificare compromise sau furate;

(b) valoarea fiecărei operațiuni de plată;

(c) scenariile de fraudă cunoscute în ceea ce privește furnizarea de servicii de plată;

(d) semne de infectare cu programe malware în oricare sesiune din procedura de autentificare;

(e) în cazul în care dispozitivul de acces sau programul informatic este furnizat de prestatorul de servicii de plată, un registru de utilizare a dispozitivului de acces sau a programului informatic furnizat utilizatorului serviciilor de plată și utilizarea anormală a dispozitivului de acces sau a programului informatic.

Articolul 3

Revizuirea măsurilor de securitate

(1) Punerea în aplicare a măsurilor de securitate prevăzute la articolul 1 este documentată, testată periodic, evaluată și auditată în conformitate cu dispozițiile cadrului juridic aplicabil al prestatorului serviciilor de plată de către auditori cu experiență în domeniul securității informatice și al plăților și independenți din punct de vedere operațional de prestatorul de servicii de plată.

(2) Perioada dintre auditurile menționate la alineatul (1) se stabilește ținând seama de cadrul de contabilitate și de audit statutar relevant aplicabil prestatorului de servicii de plată.

Cu toate acestea, prestatorii de servicii de plată care recurg la derogarea prevăzută la articolul 18 fac obiectul unui audit, cel puțin o dată pe an, cu privire la metodologia, modelul și ratele de fraudă raportate. Auditorul care efectuează acest audit are competențe în domeniul securității informatice și al plăților și este independent din punct de vedere operațional de prestatorul de servicii de plată. În cursul primului an în care se aplică derogarea prevăzută la articolul 18 și, ulterior, cel puțin o dată la trei ani sau mai frecvent, la cererea autorității competente, acest audit este efectuat de către un auditor extern independent și calificat.

(3) Acest audit prezintă o evaluare și un raport privind conformitatea măsurilor de securitate ale prestatorului de servicii de plată cu cerințele prevăzute în prezentul regulament.

Întregul raport este pus la dispoziția autorităților competente, la cererea acestora.

CAPITOLUL II

MĂSURI DE SECURITATE PENTRU APLICAREA AUTENTIFICĂRII STRICTE A CLIENȚILOR

Articolul 4

Codul de autentificare

(1) În cazul în care prestatorii de servicii de plată aplică autentificarea strictă a clienților în conformitate cu articolul 97 alineatul (1) din Directiva (UE) 2015/2366, autentificarea se bazează pe două sau mai multe elemente care sunt incluse în categoria cunoștințelor, a posesiei și a inerenței și are ca rezultat generarea unui cod de autentificare.

Codul de autentificare este acceptat numai o singură dată de către prestatorul de servicii de plată atunci când plătitorul utilizează codul de autentificare pentru a-și accesa contul de plăți online, pentru a iniția o operațiune electronică de plată sau pentru a întreprinde orice acțiune, printr-un canal la distanță, care poate implica un risc de fraudare a plății sau alte abuzuri.

(2) În sensul alineatului (1), prestatorii de servicii de plată adoptă măsuri de securitate, asigurându-se că este îndeplinită fiecare dintre următoarele cerințe:

(a) nicio informație cu privire la oricare dintre elementele menționate la alineatul (1) nu poate fi derivată din divulgarea codului de autentificare;

(b) nu este posibilă generarea unui nou cod de autentificare bazat pe cunoașterea oricărui alt cod de autentificare generat anterior;

(c) codul de autentificare nu poate fi falsificat.

(3) Prestatorii de servicii de plată se asigură că autentificarea prin generarea unui cod de autentificare include fiecare dintre următoarele măsuri:

(a) în cazul în care autentificarea pentru accesul de la distanță, pentru plățile electronice la distanță și pentru orice alte acțiuni printr-un canal la distanță care pot implica un risc de fraudare a plății sau alte abuzuri nu a reușit să genereze un cod de autentificare în sensul alineatului (1), nu este posibil să se identifice care dintre elementele menționate la alineatul respectiv a fost incorect;

(b) numărul de încercări de autentificare eșuate care pot avea loc consecutiv, după care acțiunile menționate la articolul 97 alineatul (1) din Directiva (UE) 2015/2366 sunt blocate temporar sau permanent, nu trebuie să depășească cinci într-o anumită perioadă de timp;

(c) sesiunile de comunicare sunt protejate împotriva capturării datelor de autentificare transmise în cursul autentificării și împotriva manipulării de către părți neautorizate, în conformitate cu cerințele prevăzute în capitolul V;

(d) durata maximă de timp fără activitate desfășurată de plătitor după ce s-a autentificat pentru accesarea contului său online nu depășește cinci minute.

(4) În cazul în care blocarea menționată la alineatul (3) litera (b) este temporară, durata blocării și numărul de reîncercări se stabilesc pe baza caracteristicilor serviciului furnizat plătitorului și a tuturor riscurilor relevante implicate, ținând seama cel puțin de factorii menționați la articolul 2 alineatul (2).

Plătitorul este informat înainte ca blocarea să devină permanentă.

În cazul în care blocarea a devenit permanentă, se stabilește o procedură securizată care îi permite plătitorului să redobândească accesul la instrumentele electronice de plată.

Articolul 5

Corelarea dinamică

(1) În cazul în care prestatorii de servicii de plată aplică autentificarea strictă a clienților în conformitate cu articolul 97 alineatul (2) din Directiva (UE) 2015/2366, în plus față de cerințele prevăzute la articolul 4 din prezentul regulament, aceștia adoptă și măsuri de securitate care îndeplinesc fiecare dintre cerințele următoare:

(a) plătitorul este informat cu privire la valoarea operațiunii de plată și cu privire la beneficiarul plății;

(b) codul de autentificare generat este specific valorii operațiunii de plată și beneficiarului plății asupra cărora plătitorul a convenit în momentul inițierii operațiunii;

(c) codul de autentificare acceptat de către prestatorul de servicii de plată corespunde valorii specifice inițiale a operațiunii de plată și identității beneficiarului plății asupra cărora a convenit plătitorul;

(d) orice modificare a valorii sau a beneficiarului plății duce la invalidarea codului de autentificare generat.

(2) În sensul alineatului (1), prestatorii de servicii de plată adoptă măsuri de securitate care să asigure confidențialitatea, autenticitatea și integritatea fiecăruia dintre următoarele elemente:

(a) valoarea operațiunii de plată și beneficiarul plății în toate fazele procesului de autentificare;

(b) informațiile afișate plătitorului pe parcursul tuturor fazelor procesului de autentificare, inclusiv generarea, transmiterea și utilizarea codului de autentificare.

(3) În sensul alineatului (1) litera (b) și în cazul în care prestatorii de servicii de plată aplică autentificarea strictă a clienților în conformitate cu articolul 97 alineatul (2) din Directiva (UE) 2015/2366, se aplică următoarele cerințe pentru codul de autentificare:

(a) în legătură cu o operațiune de plată pe bază de card pentru care plătitorul și-a dat consimțământul în legătură cu cuantumul exact al fondurilor care urmează să fie blocate în temeiul articolului 75 alineatul (1) din directiva respectivă, codul de autentificare este specific cuantumului pentru blocarea căruia plătitorul și-a exprimat consimțământul și care a fost convenit de plătitor în momentul inițierii operațiunii;

(b) în legătură cu operațiunile de plată pentru care plătitorul și-a exprimat consimțământul referitor la executarea unui lot de operațiuni electronice de plată la distanță către unul sau mai mulți beneficiari, codul de autentificare este specific cuantumului total al lotului de operațiuni de plată și beneficiarilor specificați ai plății.

Articolul 6

Cerințele privind elementele clasificate drept cunoștințe

(1) Prestatorii de servicii de plată adoptă măsuri pentru a atenua riscul ca elementele privind autentificarea strictă a clienților clasificate drept cunoștințe să fie citite de părți neautorizate sau divulgate acestora.

(2) Utilizarea de către plătitor a acestor elemente face obiectul unor măsuri de atenuare pentru a preveni divulgarea lor către părți neautorizate.

Articolul 7

Cerințele privind elementele clasificate drept posesie

(1) Prestatorii de servicii de plată adoptă măsuri pentru a atenua riscul ca elementele privind autentificarea strictă a clienților clasificate drept posesie să fie utilizate de părți neautorizate.

(2) Utilizarea de către plătitor a acestor elemente face obiectul unor măsuri menite să prevină replicarea elementelor.

Articolul 8

Cerințele privind dispozitivele și programele informatice legate de elementele clasificate drept inerență

(1) Prestatorii de servicii de plată adoptă măsuri pentru a atenua riscul ca elementele de autentificare calificate drept inerență și citite de dispozitivele de acces și de programele informatice furnizate plătitorului să fie citite de părți neautorizate. Ca o condiție minimă, prestatorii de servicii de plată se asigură că dispozitivele de acces și programele informatice respective au o probabilitate foarte redusă ca o parte neautorizată să fie autentificată în calitate de plătitor.

(2) Utilizarea de către plătitor a acestor elemente face obiectul unor măsuri care să asigure că aceste dispozitive și programe informatice rezistă împotriva utilizării neautorizate a elementelor prin accesul la dispozitivele și programele informatice respective.

Articolul 9

Independența elementelor

(1) Prestatorii de servicii de plată se asigură că utilizarea elementelor de autentificare strictă a clienților menționate la articolele 6, 7 și 8 face obiectul unor măsuri care să garanteze că, în ceea ce privește tehnologia, algoritmii și parametrii, încălcarea unuia dintre elemente nu compromite fiabilitatea celorlalte elemente.

(2) Prestatorii de servicii de plată adoptă măsuri de securitate, în cazul în care oricare dintre elementele de autentificare strictă a clienților sau codul de autentificare însuși sunt utilizate printr-un dispozitiv universal, pentru a atenua riscul care ar rezulta din compromiterea acestui dispozitiv universal.

(3) În sensul alineatului (2), măsurile de atenuare includ fiecare dintre următoarele:

(a) utilizarea unor medii de executare sigure, separate cu ajutorul programelor informatice instalate pe dispozitivul universal;

(b) mecanisme prin care să se asigure că programele informatice sau dispozitivul nu au fost modificate de către plătitor sau de către un terț;

(c) în cazul în care au avut loc modificări, mecanisme pentru a atenua consecințele acestora.

CAPITOLUL III

DEROGĂRI DE LA AUTENTIFICAREA STRICTĂ A CLIENȚILOR

Articolul 10

Informații privind contul de plăți

(1) Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la articolul 2 și la prezentul articol alineatul (2), în cazul în care accesul unui utilizator de servicii de plată este limitat, în lipsa divulgării de date sensibile privind plățile, exclusiv la unul dintre următoarele două articole online sau exclusiv la acestea două:

(a) soldul unuia sau mai multor conturi de plată desemnate;

(b) operațiunile de plată executate în ultimele 90 de zile prin intermediul unuia sau mai multor conturi de plată desemnate.

(2) În sensul alineatului (1), prestatorii de servicii de plată nu sunt scutiți de la aplicarea autentificării stricte a clienților în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) utilizatorul serviciilor de plată accesează online, pentru prima dată, informațiile specificate la alineatul (1);

(b) s-au scurs mai mult de 90 de zile de când utilizatorul serviciilor de plată a accesat online ultima dată informațiile menționate la alineatul (1) litera (b) și de când a fost aplicată autentificarea strictă a clienților.

Articolul 11

Plățile contactless efectuate la punctul de vânzare

Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la articolul 2, în cazul în care plătitorul inițiază o operațiune electronică de plată contactless, cu condiția ca următoarele condiții să fie îndeplinite:

(a) valoarea individuală a operațiunii electronice de plată contactless nu depășește 50 EUR și

(b) valoarea cumulată a operațiunilor electronice de plată contactless anterioare inițiate de la data ultimei aplicări a autentificării stricte a clienților prin intermediul unui instrument de plată cu o funcționalitate contactless nu depășește 150 EUR sau

(c) numărul operațiunilor electronice de plată contactless consecutive inițiate de la data ultimei aplicări a autentificării stricte a clienților prin intermediul unui instrument de plată cu o funcționalitate contactless nu este mai mare de cinci.

Articolul 12

Terminale neasistate pentru bilete de transport și taxe de parcare

Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la articolul 2, în cazul în care plătitorul inițiază o operațiune electronică de plată la un terminal de plată neasistat, cu scopul de a plăti un bilet de transport sau o taxă de parcare.

Articolul 13

Beneficiarii agreați

(1) Prestatorii de servicii de plată aplică autentificarea strictă a clienților atunci când plătitorul creează sau modifică o listă a beneficiarilor agreați prin intermediul prestatorului de servicii de plată care administrează contul plătitorului.

(2) Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor generale în materie de autentificare, în cazul în care plătitorul inițiază o operațiune de plată și beneficiarul plății se află pe o listă a beneficiarilor agreați creată anterior de către plătitor.

Articolul 14

Operațiuni recurente

(1) Prestatorii de servicii de plată aplică autentificarea strictă a clienților atunci când un plătitor creează, modifică sau inițiază pentru prima dată o serie de operațiuni recurente cu aceeași valoare și cu același beneficiar al plății.

(2) Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor generale în materie de autentificare, pentru inițierea tuturor operațiunilor de plată ulterioare incluse în seria operațiunilor de plată menționate la alineatul (1).

Articolul 15

Operațiunile de transfer de credit între conturile deținute de aceeași persoană fizică sau juridică

Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților, sub rezerva respectării cerințelor prevăzute la articolul 2, în cazul în care plătitorul inițiază o operațiune de transfer de credit în cadrul căreia plătitorul și beneficiarul plății sunt una și aceeași persoană fizică sau juridică, iar ambele conturi de plăți sunt deținute de același prestator de servicii de plată care administrează contul.

Articolul 16

Operațiuni cu valoare scăzută

Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților în cazul în care plătitorul inițiază o operațiune electronică de plată la distanță, cu condiția ca următoarele condiții să fie îndeplinite:

(a) valoarea operațiunii electronice de plată la distanță nu depășește 30 EUR și

(b) valoarea cumulată a operațiunilor electronice de plată la distanță anterioare inițiate de plătitor de la ultima aplicare a autentificării stricte a clienților nu depășește 100 EUR sau

(c) numărul operațiunilor electronice de plată la distanță anterioare inițiate de plătitor de la ultima aplicare a autentificării stricte a clienților nu depășește 5 astfel de operațiuni individuale consecutive.

Articolul 17

Procese și protocoale de plată sigure în mediul întreprinderilor

Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților în ceea ce privește persoanele juridice care inițiază operațiuni electronice de plată prin utilizarea unor procese sau protocoale de plată specifice care sunt puse doar la dispoziția plătitorilor ce nu sunt consumatori, în cazul în care autoritățile competente consideră că aceste procese sau protocoale garantează niveluri de securitate cel puțin echivalente cu cele prevăzute în Directiva (UE) 2015/2366.

Articolul 18

Analiza de risc a operațiunilor

(1) Prestatorii de servicii de plată au dreptul să nu aplice autentificarea strictă a clienților în cazul în care plătitorul inițiază o operațiune electronică de plată la distanță care este identificată de către prestatorul de servicii de plată ca prezentând un nivel scăzut de risc în conformitate cu mecanismele de monitorizare a operațiunilor menționate la articolul 2 și la prezentul articol alineatul (2) litera (c).

(2) Se consideră că operațiunile electronice de plată menționate la alineatul (1) prezintă un nivel scăzut de risc în cazul în care sunt îndeplinite toate condițiile următoare:

(a) rata de fraudă pentru acest tip de operațiuni, raportată de către prestatorul de servicii de plată și calculată în conformitate cu articolul 19, este egală sau mai mică decât rata de referință a fraudelor specificată în tabelul prevăzut în anexă pentru „plățile electronice la distanță pe bază de card” și, respectiv, pentru „operațiunile electronice la distanță de transfer de credit”;

(b) valoarea operațiunii nu depășește valoarea relevantă a pragului de derogare menționată în tabelul din anexă;

(c) prestatorii de servicii de plată, în urma realizării unei analize de risc în timp real, nu au identificat niciunul dintre următoarele elemente:

(i) cheltuieli anormale sau un model anormal de comportament al plătitorului;

(ii) informații neobișnuite cu privire la accesul plătitorului la dispozitiv/programul informatic;

(iii) infectarea cu programe malware în oricare sesiune din procedura de autentificare;

(iv) scenarii de fraudă cunoscute în ceea ce privește furnizarea de servicii de plată;

(v) poziția geografică anormală a plătitorului;

(vi) poziția geografică cu risc ridicat a beneficiarului plății.

(3) Prestatorii de servicii de plată care intenționează să scutească operațiunile electronice de plată la distanță de la autentificarea strictă a clienților pe motivul că acestea prezintă un risc redus iau în considerare cel puțin următorii factorii bazați pe riscuri:

(a) modelul cheltuielilor anterioare al fiecărui utilizator al serviciilor de plată;

(b) istoricul operațiunilor de plată pentru fiecare utilizator de servicii de plată al prestatorilor de servicii de plată;

(c) poziția geografică a plătitorului și a beneficiarului plății în momentul operațiunii de plată, în cazul în care dispozitivul de acces sau programul informatic este furnizat de prestatorul de servicii de plată;

(d) identificarea unui model anormal de plată al utilizatorului serviciilor de plată în raport cu istoricul operațiunilor de plată ale utilizatorului.

Evaluarea efectuată de către un prestator de servicii de plată combină toți acești factori bazați pe riscuri într-un singur sistem de notare a riscurilor pentru fiecare operațiune individuală, pentru a stabili dacă o anumită plată ar trebui permisă fără autentificarea strictă a clienților.

Articolul 19

Calcularea ratelor fraudelor

(1) Pentru fiecare tip de operațiune menționată în tabelul din anexă, prestatorul serviciilor de plată se asigură că ratele globale ale fraudelor care acoperă atât operațiunile de plată autentificate prin autentificarea strictă a clienților, cât și pe cele executate în temeiul oricăreia dintre derogările menționate la articolele 13-18 sunt echivalente sau inferioare ratelor de referință ale fraudelor pentru același tip de operațiune de plată indicată în tabelul din anexă.

Rata globală a fraudelor pentru fiecare tip de operațiune se calculează ca fiind valoarea totală a operațiunilor la distanță neautorizate sau frauduloase, indiferent dacă fondurile au fost recuperate sau nu, împărțită la valoarea totală a tuturor operațiunilor la distanță pentru același tip de operațiune, indiferent dacă sunt autentificate cu aplicarea autentificării stricte a clienților sau executate în temeiul oricăreia dintre derogările menționate la articolele 13-18, pe o bază periodică trimestrială (90 de zile).

(2) Procesul de calcul al ratelor fraudelor și valorile rezultate se evaluează prin auditul întreprins în cadrul procesului de revizuire menționat la articolul 3 alineatul (2), care se asigură că rezultatele sunt complete și corecte.

(3) Metodologia și modelele utilizate de prestatorul de servicii de plată pentru a calcula ratele fraudelor, precum și ratele fraudelor propriu-zise sunt documentate în mod corespunzător și puse integral la dispoziția autorităților competente și ABE, cu notificarea prealabilă a autorității (autorităților) competente relevante, la cererea acestora.

Articolul 20

Încetarea derogărilor pe baza analizei de risc a operațiunilor

(1) Prestatorii de servicii de plată care utilizează derogarea menționată la articolul 18 informează imediat autoritățile competente în cazul în care una dintre ratele fraudelor monitorizate de aceștia, pentru orice tip de operațiune de plată indicată în tabelul din anexă, este mai mare decât rata de referință a fraudelor aplicabilă și furnizează autorităților competente o descriere a măsurilor pe care intenționează să le adopte pentru a restabili conformitatea ratelor lor de fraudă monitorizate cu ratele de referință ale fraudelor aplicabile.

(2) Prestatorii de servicii de plată încetează imediat să utilizeze derogarea menționată la articolul 18 pentru orice tip de operațiune de plată indicată în tabelul din anexă și aflată în intervalul specific al pragului de derogare, în cazul în care rata fraudelor monitorizată de aceștia depășește timp de două trimestre consecutive rata de referință a fraudelor aplicabilă pentru respectivul instrument de plată sau tipul de operațiune de plată din respectivul interval al pragului de derogare.

(3) După încetarea derogării menționate la articolul 18 în conformitate cu prezentul articol alineatul (2), prestatorii de servicii de plată nu mai utilizează respectiva derogare până când rata fraudelor calculată pentru un trimestru nu este egală sau mai mică decât ratele de referință ale fraudelor aplicabile pentru acel tip de operațiune de plată în respectivul interval al pragului de derogare.

(4) În cazul în care intenționează să utilizeze din nou derogarea menționată la articolul 18, prestatorii de servicii de plată informează autoritățile competente în acest sens într-un termen rezonabil și furnizează dovezi, înainte de a utiliza din nou derogarea, cu privire la restabilirea conformității ratei fraudelor monitorizate de aceștia cu rata de referință a fraudelor aplicabilă pentru respectivul interval al pragului de derogare în conformitate cu prezentul articol alineatul (3).

Articolul 21

Monitorizare

(1) Pentru a face uz de derogările prevăzute la articolele 10-18, prestatorii de servicii de plată înregistrează și monitorizează datele de mai jos, pentru fiecare tip de operațiune de plată, cu o defalcare atât pentru operațiunile de plată efectuate la distanță, cât și pentru cele neefectuate la distanță, cel puțin o dată pe trimestru:

(a) valoarea totală a operațiunilor de plată neautorizate sau frauduloase în conformitate cu articolul 64 alineatul (2) din Directiva (UE) 2015/2366, valoarea totală a tuturor operațiunilor de plată și rata de fraudă aferentă, inclusiv o defalcare a operațiunilor de plată inițiate prin autentificarea strictă a clienților și a celor efectuate în temeiul fiecărei derogări;

(b) valoarea medie a operațiunii, inclusiv o defalcare a operațiunilor de plată inițiate prin autentificarea strictă a clienților și a celor efectuate în temeiul fiecărei derogări;

(c) numărul de operațiuni de plată pentru care a fost aplicată fiecare dintre derogări și proporția acestora în raport cu numărul total al operațiunilor de plată.

(2) Prestatorii de servicii de plată pun rezultatele monitorizării efectuate în conformitate cu alineatul (1) la dispoziția autorităților competente și ABE, cu notificarea prealabilă a autorității (autorităților) competente relevante, la cererea acestora.

CAPITOLUL IV

CONFIDENȚIALITATEA ȘI INTEGRITATEA ELEMENTELOR DE SECURITATE PERSONALIZATE ALE UTILIZATORILOR SERVICIILOR DE PLATĂ

Articolul 22

Cerințe generale

(1) Prestatorii de servicii de plată asigură confidențialitatea și integritatea elementelor de securitate personalizate ale utilizatorilor serviciilor de plată, inclusiv a codurilor de autentificare, în toate fazele autentificării.

(2) În sensul alineatului (1), prestatorii de servicii de plată se asigură că este îndeplinită fiecare dintre următoarele cerințe:

(a) elementele de securitate personalizate sunt mascate atunci când sunt afișate și nu pot fi citite în integralitatea lor atunci când sunt introduse de către utilizatorul serviciilor de plată în cursul autentificării;

(b) nici elementele de securitate personalizate în formatul datelor și nici materialele criptografice legate de criptarea elementelor de securitate personalizate nu sunt stocate în text simplu;

(c) materialele criptografice secrete sunt protejate împotriva divulgării neautorizate.

(3) Prestatorii de servicii de plată documentează pe deplin procesul legat de gestionarea materialelor criptografice utilizate pentru a cripta sau a face ilizibile într-un alt mod elementele de securitate personalizate.

(4) Prestatorii de servicii de plată se asigură că prelucrarea și transmiterea elementelor de securitate personalizate și a codurilor de autentificare generate în conformitate cu capitolul II au loc în medii sigure, în conformitate cu standarde profesionale solide și recunoscute pe scară largă.

Articolul 23

Crearea și transmiterea elementelor de securitate

Prestatorii de servicii de plată se asigură că elementele de securitate personalizate sunt create într-un mediu sigur.

Aceștia atenuează riscurile utilizării neautorizate a elementelor de securitate personalizate și a dispozitivelor și programelor informatice de autentificare în urma pierderii, furtului sau copierii, înainte de a le transmite plătitorului.

Articolul 24

Asocierea cu utilizatorul serviciilor de plată

(1) Prestatorii de servicii de plată se asigură că numai utilizatorul serviciilor de plată este asociat, în condiții de siguranță, cu elemente de securitate personalizate și cu dispozitivele și programele informatice de autentificare.

(2) În sensul alineatului (1), prestatorii de servicii de plată se asigură că este îndeplinită fiecare dintre următoarele cerințe:

(a) asocierea identității utilizatorului serviciilor de plată cu elementele de securitate personalizate și cu dispozitivele și programele informatice de autentificare se desfășoară în medii sigure, sub responsabilitatea prestatorului de servicii de plată; este vorba, cel puțin, de sediul prestatorului de servicii de plată, de mediul internet furnizat de prestatorul de servicii de plată sau de alte site-uri web securizate similare utilizate de prestatorul de servicii de plată, precum și de serviciile de bancomate ale acestuia; trebuie avute în vedere riscurile asociate dispozitivelor și componentelor acestora care sunt utilizate în timpul procesului de asociere și care nu se află sub responsabilitatea prestatorului de servicii de plată;

(b) asocierea printr-un canal la distanță a identității utilizatorului serviciilor de plată cu elementele de securitate personalizate și cu dispozitivele sau programele informatice de autentificare se efectuează prin intermediul autentificării stricte a clienților.

Articolul 25

Transmiterea elementelor de securitate și a dispozitivelor și programelor informatice de autentificare

(1) Prestatorii de servicii de plată se asigură că transmiterea elementelor de securitate personalizate și a dispozitivelor și programelor informatice de autentificare către utilizatorul serviciilor de plată se desfășoară în condiții de siguranță menite să combată riscurile legate de utilizarea neautorizată a acestora în urma pierderii, furtului sau copierii lor.

(2) În sensul alineatului (1), prestatorii de servicii de plată pun în aplicare, ca o cerință minimă, fiecare dintre următoarele măsuri:

(a) mecanisme de transmitere eficace și sigure, care să garanteze că elementele de securitate personalizate și dispozitivele și programele informatice de autentificare sunt transmise utilizatorului legitim al serviciilor de plată;

(b) mecanisme care permit prestatorului de servicii de plată să verifice autenticitatea programelor informatice de autentificare transmise utilizatorului de servicii de plată prin intermediul internetului;

(c) dispoziții care să garanteze că, în cazul în care transmiterea elementelor de securitate personalizate este executată în afara sediilor prestatorului de servicii de plată sau printr-un canal la distanță:

(i) nicio parte neautorizată nu poate obține mai mult de o singură componentă a elementelor de securitate personalizate sau a dispozitivelor ori programelor informatice de autentificare, atunci când acestea sunt transmise prin intermediul aceluiași canal;

(ii) elementele de securitate personalizate sau dispozitivele ori programele informatice de autentificare transmise trebuie activate înainte de utilizare;

(d) dispoziții care să garanteze că, în cazul în care elementele de securitate personalizate sau dispozitivele ori programele informatice de autentificare trebuie activate înainte de prima utilizare, activarea are loc într-un mediu sigur, în conformitate cu procedurile de asociere menționate la articolul 24.

Articolul 26

Reînnoirea elementelor de securitate personalizate

Prestatorii de servicii de plată se asigură că reînnoirea sau reactivarea elementelor de securitate personalizate respectă procedurile pentru crearea, asocierea și transmiterea elementelor de securitate și a dispozitivelor de autentificare în conformitate cu articolele 23, 24 și 25.

Articolul 27

Distrugerea, dezactivarea și revocarea

Prestatorii de servicii de plată se asigură că dispun de proceduri eficace pentru a aplica fiecare dintre următoarele măsuri de securitate:

(a) distrugerea, dezactivarea sau revocarea în condiții de siguranță a elementelor de securitate personalizate și a dispozitivelor și programelor informatice de autentificare;

(b) în cazul în care prestatorul de servicii de plată distribuie dispozitive și programe informatice de autentificare reutilizabile, reutilizarea în condiții de siguranță a unui dispozitiv sau a unui program informatic este stabilită, documentată și pusă în aplicare înainte ca acesta să fie pus la dispoziția unui alt utilizator al serviciilor de plată;

(c) dezactivarea sau revocarea informațiilor legate de elementele de securitate personalizate stocate în sistemele și bazele de date ale prestatorului de servicii de plată și, dacă este relevant, în registrele publice.

CAPITOLUL V

STANDARDE DESCHISE, COMUNE ȘI SIGURE DE COMUNICARE

Secțiunea 1

Cerințe generale privind comunicarea

Articolul 28

Cerințe privind identificarea

(1) Prestatorii de servicii de plată se asigură că au fost create condiții sigure de identificare pentru comunicarea dintre dispozitivul plătitorului și dispozitivele beneficiarului plății prin care se acceptă plățile electronice, inclusiv, dar nu numai, în cazul terminalelor de plată.

(2) Prestatorii de servicii de plată se asigură că riscurile de direcționare greșită a comunicării către persoane neautorizate în cazul aplicațiilor mobile și al altor interfețe – ale utilizatorilor serviciilor de plată – care oferă servicii electronice de plată sunt atenuate în mod eficace.

Articolul 29

Trasabilitatea

(1) Prestatorii de servicii de plată instituie proceduri prin care să se asigure că toate operațiunile de plată și alte interacțiuni – realizate în contextul prestării de servicii de plată – cu utilizatorul serviciilor de plată, cu alți prestatori de servicii de plată și cu alte entități, inclusiv comercianți, pot fi urmărite, asigurând existența unor informații *ex post* cu privire la toate evenimentele relevante pentru operațiunea electronică, în orice etapă.

(2) În sensul alineatului (1), prestatorii de servicii de plată se asigură că orice sesiune de comunicare realizată cu utilizatorul serviciilor de plată, cu alți prestatori de servicii de plată și cu alte entități, inclusiv comercianți, se bazează pe fiecare dintre următoarele elemente:

(a) un identificator unic al sesiunii;

(b) mecanisme de securitate pentru înregistrarea detaliată a operațiunii, inclusiv numărul operațiunii, mărcile temporale și toate datele relevante privind operațiunea;

(c) mărci temporale care se bazează pe un sistem temporal de referință unic și care sunt sincronizate în conformitate cu un semnal temporal oficial.

Secțiunea 2

Cerințe specifice privind standardele deschise, comune și sigure de comunicare

Articolul 30

Obligații generale pentru interfețele de acces

(1) Prestatorii de servicii de plată care oferă servicii de administrare cont și care oferă unui plătitor un cont de plăți accesibil online trebuie să dispună de cel puțin o interfață care îndeplinește fiecare dintre cerințele următoare:

(a) prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății și prestatorii de servicii de plată care emit instrumente de plată pe bază de card sunt în măsură să se identifice față de prestatorul de servicii de plată care oferă servicii de administrare cont;

(b) prestatorii de servicii de informare cu privire la conturi sunt în măsură să comunice în condiții de siguranță pentru a solicita și a primi informații cu privire la unul sau mai multe conturi de plată desemnate și la operațiunile de plată aferente;

(c) prestatorii de servicii de inițiere a plății sunt în măsură să comunice în condiții de siguranță pentru a iniția un ordin de plată din contul de plăți al plătitorului și a primi toate informațiile privind inițierea operațiunii de plată și toate informațiile la care au acces prestatorii de servicii de plată care oferă servicii de administrare cont cu privire la executarea operațiunii de plată.

(2) În scopul autentificării utilizatorului serviciului de plată, interfața menționată la alineatul (1) le permite prestatorilor de servicii de informare cu privire la conturi și prestatorilor de servicii de inițiere a plății să se bazeze pe toate procedurile de autentificare furnizate de prestatorul de servicii de plată care oferă servicii de administrare cont utilizatorului serviciilor de plată.

Interfața îndeplinește cel puțin următoarele cerințe:

(a) un prestator de servicii de inițiere a plății sau un prestator de servicii de informare cu privire la conturi trebuie să fie în măsură să ceară prestatorului de servicii de plată care oferă servicii de administrare cont să înceapă autentificarea pe baza consimțământului utilizatorului serviciilor de plată;

(b) sesiunile de comunicare dintre prestatorul de servicii de plată care oferă servicii de administrare cont, prestatorul de servicii de informare cu privire la conturi, prestatorul de servicii de inițiere a plății și orice utilizator al serviciilor de plată în cauză trebuie stabilite și menținute pe întreaga durată a autentificării;

(c) integritatea și confidențialitatea elementelor de securitate personalizate și a codurilor de autentificare transmise de către sau prin intermediul prestatorului de servicii de inițiere a plății sau al prestatorului de servicii de informare cu privire la conturi trebuie garantate.

(3) Prestatorii de servicii de plată care oferă servicii de administrare cont se asigură că interfețele lor respectă standardele de comunicare emise de organizații de standardizare internaționale sau europene.

Prestatorii de servicii de plată care oferă servicii de administrare cont se asigură, de asemenea, că specificațiile tehnice ale oricărei interfețe sunt documentate cu informații care precizează care sunt procesele de rutină, protocoalele și instrumentele de care au nevoie prestatorii de servicii de inițiere a plății, prestatorii de servicii de informare cu privire la conturi și prestatorii de servicii de plată care emit instrumente de plată pe bază de card pentru a permite programelor informatice și aplicațiilor lor să fie interoperabile cu sistemele prestatorilor de servicii de plată care oferă servicii de administrare cont.

Ca o condiție minimă și cel târziu cu șase luni înainte de data aplicării menționată la articolul 38 alineatul (2) sau înainte de data prevăzută pentru lansarea pe piață a interfeței de acces, atunci când lansarea are loc după data menționată la articolul 38 alineatul (2), prestatorii de servicii de plată care oferă servicii de administrare cont pun la dispoziție documentația, în mod gratuit, la cererea prestatorilor de servicii de inițiere a plății autorizați, a prestatorilor de servicii de informare cu privire la conturi autorizați și a prestatorilor de servicii de plată care emit instrumente de plată pe bază de card autorizați sau a prestatorilor de servicii de plată care au depus o cerere la autoritățile lor competente pentru autorizația relevantă și pun rezumatul documentației la dispoziția publicului pe site-ul lor web.

(4) În plus față de alineatul (3), prestatorii de servicii de plată care oferă servicii de administrare cont se asigură că, exceptând situațiile de urgență, orice modificare adusă specificațiilor tehnice ale interfeței lor este pusă la dispoziția prestatorilor de servicii de inițiere a plății autorizați, a prestatorilor de servicii de informare cu privire la conturi autorizați și a prestatorilor de servicii de plată care emit instrumente de plată pe bază de card autorizați sau a prestatorilor de servicii de plată care au depus o cerere la autoritățile lor competente pentru autorizația relevantă, în prealabil, cât mai curând posibil și cel puțin cu 3 luni înainte de implementarea modificării.

Prestatorii de servicii de plată documentează situațiile de urgență în care au fost operate modificări și pun documentația la dispoziția autorităților competente, la cerere.

(5) Prestatorii de servicii de plată care oferă servicii de administrare cont pun la dispoziție o platformă de testare, inclusiv cu sprijinul aferent, în vederea conectării și a testării funcționale, pentru a le permite prestatorilor de servicii de inițiere a plății autorizați, prestatorilor de servicii de informare cu privire la conturi autorizați și prestatorilor de servicii de plată care emit instrumente de plată pe bază de card autorizați sau prestatorilor de servicii de plată care au depus o cerere la autoritățile lor competente pentru autorizația relevantă să testeze programele informatice și aplicațiile utilizate pentru a oferi un serviciu de plată utilizatorilor. Această platformă de testare trebuie pusă la dispoziție cel târziu cu șase luni înainte de data aplicării menționată la articolul 38 alineatul (2) sau înainte de data prevăzută pentru lansarea pe piață a interfeței de acces, atunci când lansarea are loc după data menționată la articolul 38 alineatul (2).

Cu toate acestea, nicio informație sensibilă nu este pusă la dispoziție prin platforma de testare.

(6) Autoritățile competente se asigură că prestatorii de servicii de plată care oferă servicii de administrare cont respectă în orice moment obligațiile incluse în aceste standarde în ceea ce privește interfața (interfețele) pe care au instituit-o (le-au instituit). În cazul în care un prestator de servicii de plată care oferă servicii de administrare cont nu respectă cerințele privind interfețele prevăzute în aceste standarde, autoritățile competente se asigură că furnizarea de servicii de inițiere a plății și de servicii de informare cu privire la conturi nu este împiedicată sau perturbată, în măsura în care respectivii prestatori de astfel de servicii respectă condițiile stabilite la articolul 33 alineatul (5).

Articolul 31

Opțiuni privind interfețele de acces

Prestatorii de servicii de plată care oferă servicii de administrare cont instituie interfața menționată (interfețele menționate) la articolul 30 prin intermediul unei interfețe specifice sau acordându-le prestatorilor de servicii de plată menționați la articolul 30 alineatul (1) dreptul de a folosi interfețele utilizate pentru autentificare și pentru comunicarea cu utilizatorii serviciilor de plată ai prestatorului de servicii de plată care oferă servicii de administrare cont.

Articolul 32

Obligații privind interfața specifică

(1) Sub rezerva respectării articolelor 30 și 31, prestatorii de servicii de plată care oferă servicii de administrare cont și care au instituit o interfață specifică se asigură că interfața specifică oferă în orice moment același nivel de disponibilitate și performanță, inclusiv sprijin, ca și interfețele puse la dispoziția utilizatorului serviciilor de plată pentru accesarea directă a contului său de plăți online.

(2) Prestatorii de servicii de plată care oferă servicii de administrare cont și care au instituit o interfață specifică definesc indicatori-cheie de performanță și obiective transparente privind nivelul serviciilor care să fie cel puțin la fel de stricte precum cele stabilite pentru interfața folosită de către utilizatorii lor de servicii de plată, atât în ceea ce privește disponibilitatea, cât și datele furnizate în conformitate cu articolul 36. Interfețele, indicatorii și obiectivele în cauză sunt monitorizate de către autoritățile competente și supuse unui test de rezistență.

(3) Prestatorii de servicii de plată care oferă servicii de administrare cont și care au instituit o interfață specifică se asigură că această interfață nu creează obstacole în calea furnizării serviciilor de inițiere a plății și a serviciilor de informare cu privire la conturi. Aceste obstacole includ, printre altele, împiedicarea utilizării de către prestatorii de servicii de plată menționați la articolul 30 alineatul (1) a elementelor de securitate emise de prestatorii de servicii de plată care oferă servicii de administrare cont clienților lor, impunerea redirecționării către serviciul de autentificare al prestatorului de servicii de plată care oferă servicii de administrare cont sau către alte funcții ale acestuia, solicitarea unor autorizații și înregistrări suplimentare, în plus față de cele prevăzute la articolele 11, 14 și 15 din Directiva (UE) 2015/2366 sau solicitarea unor controale suplimentare ale consimțământului dat de către utilizatorii serviciilor de plată prestatorilor serviciilor de inițiere a plății și ai serviciilor de informare cu privire la conturi.

(4) În sensul alineatelor (1) și (2), prestatorii de servicii de plată care oferă servicii de administrare cont monitorizează disponibilitatea și performanța interfeței specifice. Prestatorii de servicii de plată care oferă servicii de administrare cont publică pe siteul lor web statistici trimestriale privind disponibilitatea și performanța interfeței specifice și a interfeței utilizate de utilizatorii serviciilor lor de plată.

Articolul 33

Măsuri de urgență pentru interfața specifică

(1) Prestatorii de servicii de plată care oferă servicii de administrare cont prevăd, atunci când proiectează interfața specifică, strategia și planurile privind măsurile de urgență pentru situațiile în care interfața nu funcționează în conformitate cu articolul 32 sau se confruntă cu o indisponibilitate neprevăzută ori pentru cazul în care sistemul încetează să funcționeze. Se poate considera că a apărut o situație de indisponibilitate neprevăzută sau de încetare a funcționării sistemului atunci când cinci cereri consecutive de acces la informații pentru furnizarea de servicii de inițiere a plății sau de informare cu privire la conturi nu primesc răspuns în 30 de secunde.

(2) Măsurile de urgență includ planuri de comunicare pentru a le oferi prestatorilor de servicii de plată care utilizează interfața specifică informații cu privire la măsurile de restabilire a sistemului și o descriere a opțiunilor alternative disponibile imediat pe care prestatorii de servicii de plată le au între timp.

(3) Atât prestatorul de servicii de plată care oferă servicii de administrare cont, cât și prestatorii de servicii de plată menționați la articolul 30 alineatul (1) transmit fără întârziere rapoarte autorităților lor naționale competente privind problemele legate de interfețele specifice descrise la alineatul (1).

(4) Ca parte a unui mecanism de urgență, prestatorii de servicii de plată menționați la articolul 30 alineatul (1) au dreptul să utilizeze, până când interfața specifică revine la nivelul de disponibilitate și performanță prevăzut la articolul 32, interfețele puse la dispoziția utilizatorilor serviciilor de plată pentru autentificarea și comunicarea cu prestatorul lor de servicii de plată care oferă servicii de administrare cont.

(5) În acest scop, prestatorii de servicii de plată care oferă servicii de administrare cont se asigură că prestatorii de servicii de plată menționați la articolul 30 alineatul (1) pot fi identificați și se pot baza pe procedurile de autentificare furnizate de prestatorul de servicii de plată care oferă servicii de administrare cont utilizatorilor serviciilor de plată. În cazul în care utilizează interfața menționată la alineatul (4), prestatorii de servicii de plată menționați la articolul 30 alineatu (1):

(a) iau măsurile necesare pentru a se asigura că nu accesează, stochează sau prelucrează date în alte scopuri decât pentru furnizarea serviciului solicitat de utilizatorul serviciilor de plată;

(b) continuă să respecte obligațiile care decurg din articolul 66 alineatul (3) și din articolul 67 alineatul (2) din Directiva (UE) 2015/2366;

(c) înregistrează datele care sunt accesate prin intermediul interfeței operate de către prestatorul de servicii de plată care oferă servicii de administrare cont utilizatorilor serviciilor sale de plată și furnizează datele înregistrate autorității lor naționale competente, la cerere și fără întârzieri nejustificate;

(d) justifică în mod corespunzător autorității lor naționale competente, la cerere și fără întârzieri nejustificate, utilizarea interfeței puse la dispoziția utilizatorilor serviciilor de plată în scopul accesării directe a contului lor de plăți online;

(e) informează în acest sens prestatorul de servicii de plată care oferă servicii de administrare cont.

(6) Autoritățile competente, după consultarea ABE în vederea asigurării unei aplicări consecvente a următoarelor condiții, scutesc prestatorii de servicii de plată care oferă servicii de administrare cont și care au optat pentru o interfață specifică de obligația de a crea mecanismul de urgență descris la alineatul (4), în cazul în care interfața specifică îndeplinește toate condițiile următoare:

(a) respectă toate obligațiile privind interfețele specifice prevăzute la articolul 32;

(b) a fost proiectată și testată în conformitate cu articolul 30 alineatul (5) într-un mod pe care prestatorul serviciilor de plată menționat la articolul respectiv îl consideră satisfăcător;

(c) a fost utilizată la scară largă timp de cel puțin trei luni de către prestatorii de servicii de plată în vederea furnizării de servicii de informare cu privire la conturi și de servicii de inițiere a plății și în vederea confirmării disponibilității fondurilor pentru plățile pe bază de card;

(d) orice problemă legată de interfața specifică a fost rezolvată fără întârzieri nejustificate.

(7) Autoritățile competente revocă derogarea menționată la alineatul (6) în cazul în care condițiile de la literele (a) și (d) nu sunt îndeplinite de prestatorii de servicii de plată care oferă servicii de administrare cont timp de peste două săptămâni calendaristice consecutive. Autoritățile competente informează ABE cu privire la această revocare și se asigură că prestatorul de servicii de plată care oferă servicii de administrare cont instituie – în cel mai scurt timp posibil și în termen de cel mult două luni – mecanismul de urgență menționat la alineatul (4).

Articolul 34

Certificate

(1) În scopul identificării prevăzute la articolul 30 alineatul (1) litera (a), prestatorii de servicii de plată se bazează pe certificatele calificate pentru sigiliile electronice definite la articolul 3 punctul 30 din Regulamentul (UE) nr. 910/2014 sau pentru autentificarea unui site internet definită la articolul 3 punctul 39 din regulamentul respectiv.

(2) În sensul prezentului regulament, numărul de înregistrare menționat în registrele oficiale, care este prevăzut la litera (c) din anexa III sau la litera (c) din anexa IV la Regulamentul (UE) nr. 910/2014, este numărul autorizației prestatorilor de servicii de plată care emit instrumente de plată pe bază de card, a prestatorilor de servicii de informare cu privire la conturi și a prestatorilor de servicii de inițiere a plății, inclusiv a prestatorilor de servicii de plată care oferă servicii de administrare cont și care furnizează astfel de servicii, număr care este disponibil în registrul public din statul membru de origine în temeiul articolului 14 din Directiva (UE) 2015/2366 sau care rezultă din notificările fiecărei autorizații acordate în temeiul articolului 8 din Directiva 2013/36/UE a Parlamentului European și a Consiliului [1] în conformitate cu articolul 20 din directiva respectivă.

(3) În sensul prezentului regulament, certificatele calificate pentru sigiliile electronice sau pentru autentificarea site-urilor internet menționate la alineatul (1) includ, într-o limbă utilizată în mod obișnuit în domeniul finanțelor internaționale, atribute specifice suplimentare în legătură cu fiecare dintre următoarele elemente:

(a) rolul prestatorului de servicii de plată, care poate fi unul sau mai multe dintre următoarele:

(i) furnizarea de servicii de administrare cont;

(ii) furnizarea de servicii de inițiere a plății;

(iii) furnizarea de servicii de informare cu privire la conturi;

(iv) emiterea de instrumente de plată pe bază de card;

(b) denumirea autorităților competente la care este înregistrat prestatorul de servicii de plată.

(4) Atributele menționate la alineatul (3) nu afectează interoperabilitatea și recunoașterea certificatelor calificate pentru sigiliile electronice sau pentru autentificarea site-urilor internet.

[1] Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

Articolul 35

Securitatea sesiunilor de comunicare

(1) Prestatorii de servicii de plată care oferă servicii de administrare cont, prestatorii de servicii de plată care emit instrumente de plată pe bază de card, prestatorii de servicii de informare cu privire la conturi și prestatorii de servicii de inițiere a plății se asigură că, atunci când se face schimb de date prin internet, între părțile care comunică sunt aplicate procese de criptare sigură pe durata întregii sesiuni de comunicare, pentru a proteja confidențialitatea și integritatea datelor, cu ajutorul unor tehnici de criptare solide și recunoscute pe scară largă.

(2) Prestatorii de servicii de plată care emit instrumente de plată pe bază de card, prestatorii de servicii de informare cu privire la conturi și prestatorii de servicii de inițiere a plății mențin o durată cât mai scurtă posibil a sesiunilor în care se asigură accesul și care sunt oferite de prestatorii de servicii de plată care oferă servicii de administrare cont și încheie în mod activ astfel de sesiuni de îndată ce acțiunea solicitată a fost realizată.

(3) Atunci când mențin sesiuni de rețea paralele cu prestatorul de servicii de plată care oferă servicii de administrare cont, prestatorii de servicii de informare cu privire la conturi și prestatorii de servicii de inițiere a plății se asigură că sesiunile respective sunt legate în condiții de siguranță de sesiunile relevante stabilite cu utilizatorul (utilizatorii) serviciilor de plată, pentru a se evita riscul ca orice mesaj sau informație comunicată între aceștia să fie transmisă unei destinații greșite.

(4) Prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății și prestatorii de servicii de plată care emit instrumente de plată pe bază de card împreună cu prestatorul de servicii de plată care oferă servicii de administrare cont indică trimiteri explicite la fiecare dintre următoarele elemente:

(a) utilizatorul sau utilizatorii serviciilor de plată și sesiunile de comunicare corespunzătoare, pentru a face distincția între mai multe cereri din partea aceluiași utilizator (acelorași utilizatori) al (ai) serviciilor de plată;

(b) pentru serviciile de inițiere a plății, operațiunea de plată inițiată identificată în mod unic;

(c) pentru confirmarea disponibilității fondurilor, cererea identificată în mod unic referitoare la suma necesară pentru executarea operațiunii de plată pe bază de card.

(5) Prestatorii de servicii de plată care oferă servicii de administrare cont, prestatorii de servicii de informare cu privire la conturi, prestatorii de servicii de inițiere a plății și prestatorii de servicii de plată care emit instrumente de plată pe bază de card se asigură că, în cazul în care comunică elemente de securitate personalizate și coduri de autentificare, acestea nu pot fi citite, direct sau indirect, de către niciun membru al personalului, în niciun moment.

În cazul pierderii caracterului confidențial al elementelor de securitate personalizate atunci când se află în sfera lor de competență, prestatorii în cauză informează fără întârziere în acest sens utilizatorul serviciilor de plată aferente acestora și emitentul elementelor de securitate personalizate.

Articolul 36

Schimburi de date

(1) Prestatorii de servicii de plată care oferă servicii de administrare cont respectă fiecare dintre următoarele cerințe:

(a) aceștia furnizează prestatorilor serviciilor de informare cu privire la conturi aceleași informații provenind de la conturile de plată desemnate și de la operațiunile de plată aferente ca și cele puse la dispoziția utilizatorului serviciilor de plată atunci când acesta solicită acces direct la informațiile despre cont, cu condiția ca informațiile respective să nu includă date sensibile privind plățile;

(b) aceștia furnizează prestatorilor de servicii de inițiere a plății, imediat după primirea ordinului de plată, aceleași informații cu privire la inițierea și executarea operațiunii de plată ca și cele furnizate sau puse la dispoziția utilizatorului serviciilor de plată în cazul în care operațiunea este inițiată în mod direct de către acesta din urmă;

(c) aceștia informează imediat, la cerere, prestatorii de servicii de plată, printr-o confirmare într-un format simplu de tipul „da” sau „nu”, dacă suma necesară pentru executarea unei operațiuni de plată este disponibilă în contul de plăți al plătitorului.

(2) În cazul unui eveniment sau al unei erori neprevăzute care survine în timpul procesului de identificare sau de autentificare ori în momentul schimbului de informații, prestatorul de servicii de plată care oferă servicii de administrare cont transmite un mesaj de notificare prestatorului de servicii de inițiere a plății sau prestatorului de servicii de informare cu privire la conturi și prestatorului de servicii de plată care emite instrumente de plată pe bază de card, în care explică din ce cauză a survenit evenimentul sau eroarea neprevăzută.

În cazul în care prestatorul de servicii de plată care oferă servicii de administrare cont furnizează o interfață specifică în conformitate cu articolul 32, interfața pune la dispoziție mesajele de notificare referitoare la evenimente sau erori neprevăzute care trebuie comunicate de către orice prestator de servicii de plată ce detectează evenimentul sau eroarea celorlalți prestatori de servicii de plată care participă la sesiunea de comunicare.

(3) Prestatorii de servicii de informare cu privire la conturi trebuie să dispună de mecanisme adecvate și eficace care să împiedice accesul la alte informații decât cele provenind de la conturile de plată desemnate și de la operațiunile de plată aferente, în conformitate cu consimțământul explicit al utilizatorului.

(4) Prestatorii de servicii de inițiere a plății furnizează prestatorilor de servicii de plată care oferă servicii de administrare cont aceleași informații ca și cele solicitate de utilizatorul serviciilor de plată atunci când inițiază operațiunea de plată în mod direct.

(5) Prestatorii de servicii de informare cu privire la conturi sunt în măsură să acceseze informații provenind de la conturile de plată desemnate și de la operațiunile de plată aferente deținute de prestatorii de servicii de plată care oferă servicii de administrare cont, pentru executarea serviciului de informare cu privire la conturi, în oricare dintre următoarele circumstanțe:

(a) ori de câte ori utilizatorul serviciilor de plată solicită astfel de informații în mod activ;

(b) în cazul în care utilizatorul serviciilor de plată nu solicită astfel de informații în mod activ, nu mai mult de patru ori într-o perioadă de 24 de ore, cu excepția cazului în care prestatorul de servicii de informare cu privire la conturi și prestatorul de servicii de plată care oferă servicii de administrare cont au convenit asupra unei frecvențe mai ridicate, cu consimțământul utilizatorului serviciilor de plată.

CAPITOLUL VI

DISPOZIȚII FINALE

Articolul 37

Revizuire

Fără a aduce atingere articolului 98 alineatul (5) din Directiva (UE) 2015/2366, ABE revizuiește până la 14 martie 2021 ratele fraudelor menționate în anexa la prezentul regulament, precum și derogările acordate în temeiul articolului 33 alineatul (6) în ceea ce privește interfețele specifice și, dacă este cazul, transmite Comisiei proiectul de actualizare a acestora, în conformitate cu articolul 10 din Regulamentul (UE) nr. 1093/2010.

Articolul 38

Intrare în vigoare

(1) Prezentul regulament intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Prezentul regulament se aplică de la 14 septembrie 2019.

(3) Cu toate acestea, articolul 30 alineatele (3) și (5) se aplică de la 14 martie 2019.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 noiembrie 2017.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

ANEXĂ

	Rata de referință a fraudei (%) pentru:	
ETV (valoarea pragului de derogare)	Plățile electronice la distanță pe bază de card	Operațiunile electronice la distanță de transfer de credit
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015